



SDN-μSense

Project No. 833955

Project acronym: SDN-microSENSE

Project title:

SDN - microgrid reSilient Electrical eNergy SystEm

Deliverable D5.2

SS-IDPS System

Programme: H2020-SU-DS-2018

Start date of project: 01.05.2019

Duration: 36 months

Editor: ATOS

Due date of deliverable: 31/10/2020

Actual submission date: 30/10/2020



Deliverable Description:

Deliverable Name	SS-IDPS System
Deliverable Number	D5.2
Work Package	WP 5
Associated Task	T5.2
Covered Period	M6
Due Date	M18
Completion Date	M18
Submission Date	30/10/2020
Deliverable Lead Partner	ATOS
Deliverable Author(s)	Rubén Trapero
Version	1.3

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

CHANGE CONTROL
DOCUMENT HISTORY

Version	Date	Change History	Author(s)	Organisation
0.1	15/06/2020	Initial ToC	Ruben Trapero	ATOS
0.2	7/8/2020	Section 3.2, Section 4	Jose Antonio Lopez Montero	TECN
0.3	13/8/2020	Section 1	Ruben Trapero	ATOS
0.4	15/09/2020	Section 2.2, Section 2.3, Section 2.4	Yannis Spyridis (OINF), Panagiotis Radoglou-Grammatikis (UOWM), Elisavet Grigoriou (SID)	UOWM, OINF, SID
0.5	16/09/2020	Annex I, Annex II, Annex III	Yannis Spyridis (OINF), Panagiotis Radoglou-Grammatikis (UOWM), Elisavet Grigoriou (SID)	UOWM, OINF, SID
0.6	16/09/2020	Section 3.3	Ruben Trapero	ATOS
0.7	17/09/2020	Section 3.2	Iñaki Angulo	TECN
0.8	17/09/2020	Section 2.1	Iñaki Angulo (TECN) Sofianna Menesidou (UBI)	TECN, UBI
0.8a	17/09/2020	Section 4	All	All
0.9	17/09/2020	Executive Summary, Conclusions, list of acronyms	Ruben Trapero	ATOS
1.0	30/09/2020	Version ready for reviews	Ruben Trapero	ATOS

1.1	09/10/2020	Industrial and academic reviews addressed	Ruben Trapero	ATOS
1.2	16/10/2020	SAB review completed	Dave Raggett	ERCIM
1.3	29/10/2020	QM and TM review addressed	Ruben Trapero (ATOS), Iñaki Angulo (TECN). Panagiotis Radoglou-Grammatikis (UOWM)	ATOS, TECN, UOWM

DISTRIBUTION LIST

Date	Issue	Group
28/10/2020	Revision	ERCIM, CERTH, SID, SAB, TM, QM
29/10/2020	Acceptance	ERCIM, CERTH, SID, SAB, TM, QM
30/10/2020	Submission	ATOS

SAB APPROVAL

NAME	INSTITUTION	DATE
Dr. Dave Raggett	ERCIM	16/10/2020

Academic and Industrial partner revision

NAME	INSTITUTION	DATE
Anastasis Drosou	Academic partner: CERTH	08/10/2020
Anastasios Lytos	Industrial partner: SID	08/10/2020

Quality and Technical manager revision

NAME	INSTITUTION	DATE
Dimos Ioannidis	CERTH	26/10/2020
Anastasios Drosou	CERTH	26/10/2020

Table of contents

Table of contents	4
Table of figures	6
Table of tables	6
Acronyms	7
Executive Summary.....	8
1 Introduction	9
1.1 Purpose of this Document	9
1.2 Structure of this Document.....	9
1.3 Relation to other Tasks and Deliverables	10
1.4 Requirements analysis.....	10
2 Main protocols in the Electrical Power and Energy System domain	12
2.1 IEC 61850	12
2.1.1 Description	12
2.1.2 Main attacks	13
2.1.3 Attacking tools.....	14
2.1.4 Attacks detection	15
2.2 IEC 60870-5-101/104	15
2.2.1 Description	15
2.2.2 Main attacks	17
2.2.3 Attacking Tools	18
2.2.4 Attacks detection	18
2.3 Modbus.....	20
2.3.1 Description	20
2.3.2 Main attacks	21
2.3.3 Attacking tools.....	22
2.3.4 Attacks detection	23
2.4 DNP3.....	23
2.4.1 Description	23
2.4.2 Attacking tools.....	25
2.4.3 Attacks detection	25
3 Main detection tools.....	27

3.1	Enhanced Suricata for EPES	27
3.1.1	Input data	29
3.1.2	Internals of the tool	29
3.1.3	Deployment.....	29
3.1.4	Output: connection to XL-SIEM, logs and taxonomy	30
3.2	SBT-Aware.....	31
3.2.1	Input data	32
3.2.2	Internals of the tool	33
3.2.2.1	SCL interpreter module	34
3.2.2.2	Pluggable detection engine module	37
3.2.2.3	Pluggable report launcher module	37
3.2.3	Deployment.....	37
3.2.3.1	SCL interpreter	37
3.2.3.2	Report launcher	38
3.2.3.3	Tools integration.....	38
3.2.4	Output: connection to XL-SIEM, logs and taxonomy	38
3.3	SDN-IDPS: Nightwatch	39
3.3.1	Input data from the SDN controller	40
3.3.2	Internals of the tool	40
3.3.3	Deployment.....	41
3.3.4	Output: connection to XL-SIEM, logs and taxonomy	41
4	Unit Testing and validation	43
4.1	Modbus/TCP Unit Tests – Suricata	43
4.2	IEC104 Unit Tests – Suricata.....	55
4.3	DNP3 Unit Tests – Suricata	62
4.4	IEC 61850 Unit Tests – STB-Aware	71
5	Innovation Summary	75
6	Conclusions	83
7	References	84
	Annex I: IEC104 Suricata Signature/Specification Rules.....	86
	Annex II: Modbus/TCP Suricata Signature/Specification Rules.....	96
	Annex III: DNP3 Suricata Signature/Specification Rules	100

Table of figures

Figure 1. T5.2 components within WP5 architecture	9
Figure 2. Links between D5.2 and the rest of deliverables and WPs.....	10
Figure 3. Security requirements, threats, and possible attacks [IEC62351].	13
Figure 4. Modbus/TCP frame information [PLIATSIOS20]	20
Figure 5. Suricata output using JSON format	28
Figure 6. Suricata internals.....	29
Figure 7. SBT-Aware tool, including modules, I/O data and relevant actors	34
Figure 8. Defence in Depth for devices and for an IEC 61850 substation.....	35
Figure 9. Architecture of Nightwatch in SDN-microSENSE.....	41
Figure 10. Activation of the Modbus/TCP keywords testcase Modbus_Suricata_01.....	44
Figure 11. Pcap for modbus/function/readCoils attack for test case Modbus_Suricata_01	44
Figure 12. Activation of the Modbus/TCP keywords for test case Modbus_Suricata_02	46
Figure 13. Pcap for modbus/function/writeSingleCoils attack for test case Modbus_Suricata_02	47
Figure 14. Activation of Modbus/TCP keywords for test case Modbus_Suricata_03	49
Figure 15. Pcap for modbus/function/readInputRegister attack for test case Modbus_Suricata_03	49
Figure 16. Activation of Modbus/TCP keywords for test case Modbus_Suricata_04	51
Figure 17. Pcap for modbus/function/writeSingleRegister attack for Modbus_Suricata_04	52
Figure 18. Activation of Modbus/TCP keywords for test case Modbus_Suricata_05	54
Figure 19. Pcap for modbus/function/readDiscreteInput attack for test case Modbus_Suricata_05.....	54
Figure 20. Pcap for UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_01	56
Figure 21. Pcap file of UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_02	58
Figure 22. Pcap file of UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_03	60
Figure 23. Pcap file of UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_04	62
Figure 24. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_01	63
Figure 25. Pcap of [Pliatsios20] for test case DNP3_Suricata_01	64
Figure 26. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_02	65
Figure 27. Pcap of [Pliatsios20] for test case DNP3_Suricata_02	66
Figure 28. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_03	67
Figure 29. Pcap of [Pliatsios20] for test case DNP3_Suricata_03	68
Figure 30. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_04	69
Figure 31. Pcap of [Pliatsios20] for test case DNP3_Suricata_04	70
Figure 32. scliCrawler output (XML containing CDATA for MMS)	72
Figure 33. Extract from scliCrawler output for bay 1 CID file.....	73
Figure 34. LUA script to add substation specific information	74
Figure 35. Alert launched when checking the state	74

Table of tables

Table 1. Standard IEC104 data types	16
Table 2. Description for Suricata logs	30
Table 3. Description for the Generic Threat Discovery log	38
Table 4 Description of the SBT Cybersecurity events log.....	39

Table 5. Description for the threat discovery log	41
Table 6. Summary of protocols attacks and tools involved	75

Acronyms

Acronym	Explanation
ADU	Application Data Unit
APCI	Application Protocol Control Information
APDU	Application Protocol Data Unit
CASDU	Common Address of ASDU
COT	Cause of Transmission
DiD	Defense in Depth
DNP3	Distributed Network Protocol Version 3.0
DoS	Denial of Service
EPA	Enhanced Performance Architecture
EPDS	Energy Protection and Detection System
EPES	Electrical Power and Energy System
FR	Functional Requirement
GOOSE	Generic Object-Oriented Substation Events
GR	General Requirement
GSSE	Generic Substation State Events
IDCM	Intrusion Detection and Classification Module
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
ISO	Open Systems Interconnection
MiTM	Man-In-The-Middle
MMS	Manufacturing Messaging Specification
NSE	Nmap Scripting Engine
PDU	Protocol Data Unit
RTU	Remote terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCD	Substation Configuration Description
SCL	System Control Language
SDN	Software Defined Network
SIEM	Security Information and Event Manager
SMV	Sampled Measured Values
UC	Use Case
UR	User Requirement
VSQ	Variable Structure Qualifier

WAF	Web Application Firewalls
WAN	Wide Area Networks

Executive Summary

This deliverable is the second document of Work Package 5 (WP5) of SDN-microSENSE. WP5 focuses on cybersecurity protection in the EPES domain, including components for the monitoring of EPES infrastructures, detection of cyber incidents associated to application protocols commonly used EPES networks (T5.1), the development of components for detecting cyber incidents linked to these protocols (T5.2, T5.3, T5.4), and threat intelligence sharing capabilities within EPES (T5.4).

The content of this deliverable is focused on the results of task T5.2, describing the main threats associated to the most popular protocols used in the EPES domain, including not just the insights of those protocols but also the techniques to detect attacks associated to those threats. This document continues with the work carried out in T5.1 and reported in D5.1, which was focused on the incident detection as part of the XL-EDPS module. More specifically, this document details those components that interconnects to the XL-EDPS, acting as detectors of some of the attacks described in this document. This document is complemented with D5.3 (the output from T5.3) which details the detection of some of the attacks described in this deliverable with AI based detection mechanisms, and D5.4 (the output from T5.4), which details the detection of privacy related incidents.

More specifically, this document is structured in two parts. The **1st part describes the attacks, tools and detection mechanisms** associated to the protocols IEC61850, IEC60870-5-101/104, Modbus and DNP3, extending the introduction included in D5.1 with more details related to mechanisms to detect the incidents described.

The **2nd part of the deliverable details the three main tools** that implement the detection techniques described in the first part of the document: **Nightwatch as an SDN-based IDPS, and SBT Aware and Suricata as rule-based IDPSs**. The attacks detected by these tools depends on their capabilities and the protocols that are able to monitor.

1.1 Purpose of this Document

[illegible]

Figure 1. T5.2 components within WP5 architecture

This document is structured as follows:

- Section 2 is focused on the detailed description of the communication and industrial protocols widely used in EPES operations and their associated threats
- Section 3 details IDPS detectors developed in T5.2 capable of detecting the incidents described in Section 2.
- Section 4 details the unit testing to validate the mechanisms described in Section 2.
- Section 5 summarizes the main innovations developed in this task.

¹ <https://suricata-ids.org/>

² <https://www.cyberlens.eu/nightwatch/>

- Section 6 concludes the document.

1.3 Relation to other Tasks and Deliverables

The following tasks and deliverables are related to the current report:

- D2.2 [SDN22], where the requirements of the SDN-microSENSE platform are elicited
- D2.3 [SDN23] that describes the SDN-microSENSE architecture
- D2.4 [SDN24] that describes the validation methodology and the list of threats and attacks associated to every pilot and use case
- D3.3 [SDN33], where the output from the honeypots developed in WP3 are described and used as input for the Nightwatch component described in Section 3.1.
- D5.1 [SDN51], where the XL-EPDS is described, detailing the interfaces available at the XL-SIEM for receiving events produced by T5.2 detectors. The communication protocols deeply described in this document were also introduced in D5.1.
- D5.3 [SDN53], that details the machine learning based detectors that allows to detect the cyber-incidents described in Section 2.

Those three deliverables are the ones that are directly related, although there are additional ones that also, to some extent, related, such as D5.4 [SDN54] and D5.5 [SDN55]

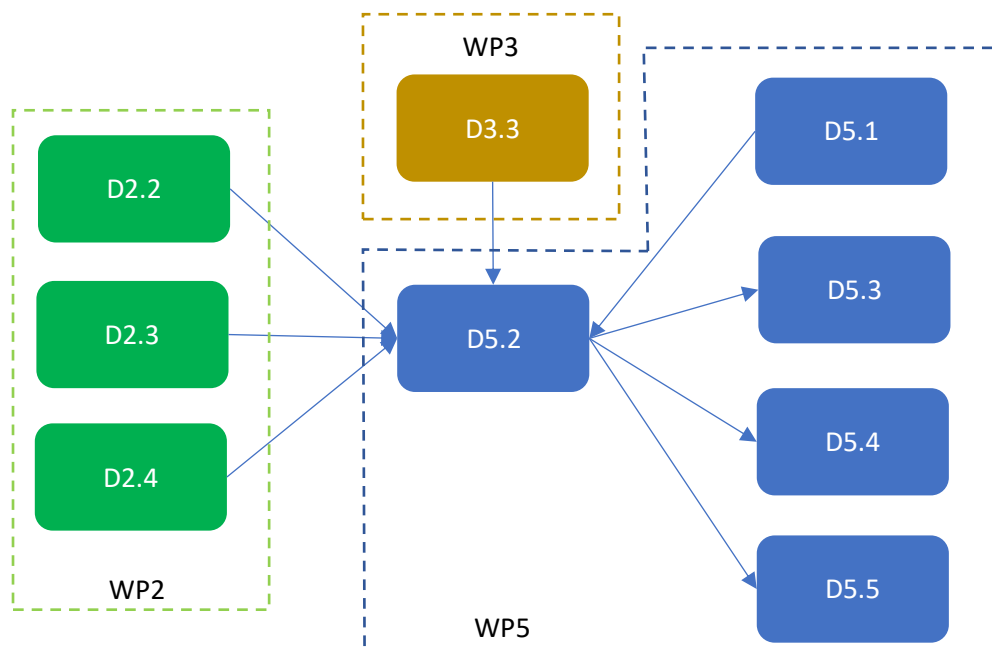


Figure 2. Links between D5.2 and the rest of deliverables and WPs

1.4 Requirements analysis

The following requirements elicited from D2.2 are covered by the components described in this document.

Functional Requirements General Requirements
FR-GR-05, related to the ability to provide network flow metrics from network data
FR-GR-12, related to the collection of security events

Functional Requirements User Requirements
FR-UR-03 to 13 related to the detection of cyberattacks associated to different types of protocols FR-UR-16, related to the discrimination of various types of cyberattacks
Functional Requirements Use Case Requirements
FR-UC1-01 to 03, which cover cyber-attacks to SCADAs logical interface under the Use Case 1 FR-UC1-04 to 07, which cover cyber-attacks to the Station Bus network under the Use Case 1 FR-UC1-08 to 11, which cover cyber-attacks against the process control bus FR-UC3-01, which cover the defence against coordinated attacks scenarios in the Islanding Use Case 3.
Non-Functional requirements
All non-functional requirements refined in Table 12 of D2.2 are covered by this deliverable

The following sections describe the results of this task. The deliverable is structured in two main parts. The first part, covered by Section 2, describe in detail the main communication and industrial protocols commonly used in the EPES domain, focused from the cybersecurity point of view, indicating their weak points from a cybersecurity perspective, the main attacks threatening these protocols and the techniques to detect them.

The second part, covered by Section 3, details the technologies developed or adapted by SDN-microSENSE partners for detecting the attacks described in Section 2. In this part it is described how the mechanisms detailed in Section 2 are implemented and incorporated to these tools. As part of WP7 activities these tools will be integrated in the SDN-microSENSE platform and interconnected to the XL-SIEM derived from Task 5.1.

The final part of the document describes other aspects related to the results obtained in Task 5.2, such as the unit testing carried out (described in Section 4) and the innovation summary described in Section 5.

2 Main protocols in the Electrical Power and Energy System domain

This section extends the description included in Section 4 of deliverable D5.1, related to the detection of the attacks described there. The following subsections detail the insights of the main protocols in the EPES domain, and the strategies to monitor them and detect incidents associated with these protocols.

2.1 IEC 61850

2.1.1 Description

As described in deliverable D5.1 [SDN51], the objective of the IEC 61850 was the definition of an international standard for the automation of the control, protection and measurement functions of a substation. IEC 61850 is used for interactions with field equipment, including protective relaying, substation automation, distribution automation, power quality, distributed energy resources, substation to control centre, and other power industry operational functions. It also includes profiles to meet the ultra-fast response times of protective relaying and for the sampling of measured values.

The IEC 61850 stack consists of four types of messages:

- Manufacturing Messaging Specification (MMS). It is the client-server communication that takes place between the servers (the protection and control devices) and the SCADA and GATEWAY acting as clients. The protocol used in this exchange use the MMS protocol (Manufacturing Message Specification) that is depicted in the standard ISO 9506. This protocol was developed for industrial automation, and it is one of the first protocols that identify data with hierarchies of names. The communication is based on the OSI layered model over TCP/IP. A TCP channel is created between each client and each server. Over this channel, the client can read data, force settings, request commands or receive spontaneous reporting. A SCADA system will keep open as many TCP/IP channels as servers it is monitoring [IEC61850].
- Generic Substation State Events (GSSE) and Generic Object-Oriented Substation Events (GOOSE). Fast and reliable system-wide distribution of data based on a publisher-subscriber model. This model is used for real-time transmission of critical events (GOOSE messages).
- Sampled Measured Values (SMV) model for multicast measurement values. This model is used to provide rapid communication of measurement, protection and control values. It works through Ethernet (Layer 2 OSI) following a publisher-subscriber model.

Elaborated by the IEC Technical Committee 57 (IEC TC57), IEC 61850 did not consider initially cybersecurity aspects in its definitions. Because of this, communication protocols (MMS, GOOSE, GSSE, SMV) have rarely incorporated any security measures, including security against inadvertent errors, power system equipment malfunctions, communications equipment failures, or deliberate sabotage [IEC62351]. The IEC 62351 (Power systems management and associated information exchange - Data and communications security), incorporates cybersecurity capabilities in the IEC TC57 electrical protocols [IECTC57]. The different security objectives include authentication in the transfer of data through digital signatures, guaranteeing only authenticated access, eavesdropping prevention, spoofing prevention, or intrusion detection.

2.1.2 Main attacks

The Figure 3 references to the IEC 62351-1 specification and presents a set of cyberattacks that are likely to occur in an electrical environment. Furthermore, it provides a relationship between cyberattacks and threats, depending on whether they threaten the confidentiality, integrity, availability or non-repudiation of an IED.

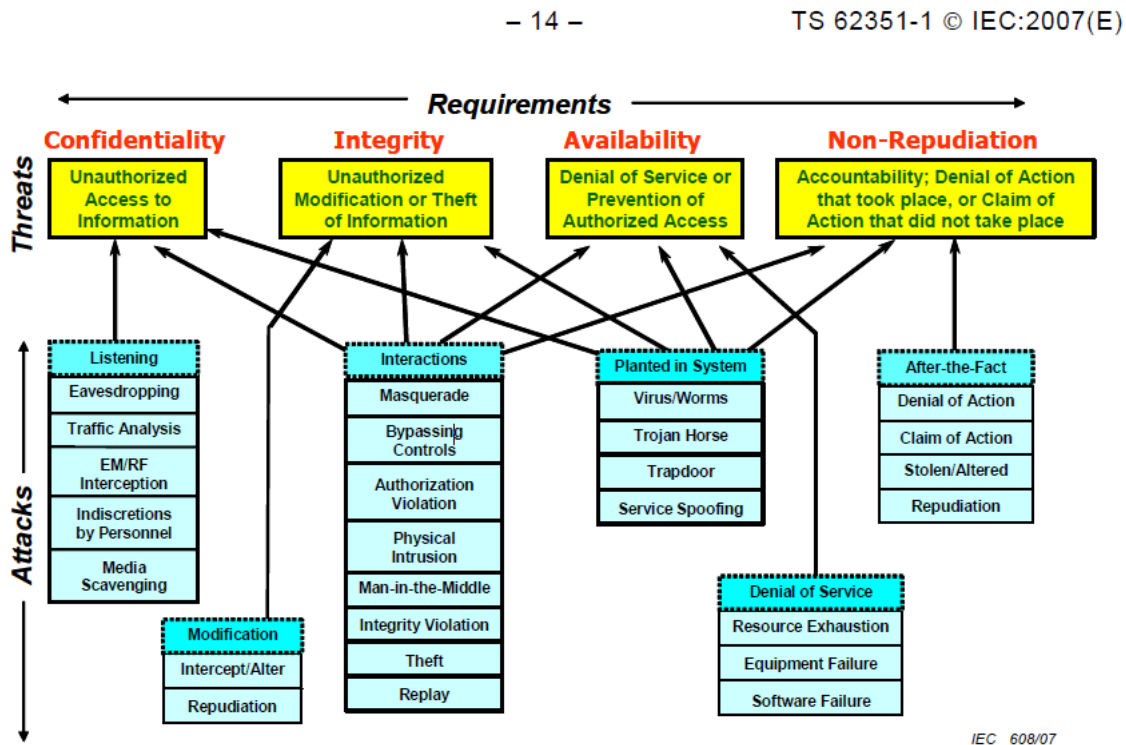


Figure 3. Security requirements, threats, and possible attacks [IEC62351].

The most typical attacks to an IED are the following:

- **Deny of Service (DOS).** The most common is to saturate the communication channels. However, it can also be accomplished by injecting invalid firmware or configuration or by inserting a malicious program to stop internal daemons.
- Access to the IED for **theft of information**.
- **Identity Fraud.** Take the control of an IED to generate unauthorised actions in the electrical components of a substation (for example to generate a blackout), provide wrong information to the SCADA of the control room, or to get access to other EIDs.
- **Message injection.** A MiTM attack that intercept authorised messages from the control room and replay them to make the IED behave anomalously.

Most of these attacks use a specific mechanism to achieve their malicious purpose, these attack mechanisms are categorized by CAPEC³ and the attacks listed above belong to the following categories:

³ <https://capec.mitre.org/data/definitions/1000.html>

- **Abuse Existing Functionality**
- **Engage in Deceptive Interactions**
- **Manipulate Data Structures**
- **Inject Unexpected Items**

Among the three IEC 61850 protocols, one is devoted to inter-IED high-speed information exchange: GOOSE (Generic Object-Oriented Substation Event). To meet IEC 61850 standard requirements its end-to-end transfer time must be less than 4ms. This time-critical specification explains GOOSE implementation as an Ethernet Link layer-based protocol (mapped on ISO/IEC 8802-3): GOOSE messages are broadcasted over the Ethernet network, IEDs that need a specific-GOOSE message content must have been subscribed to it at configuration time of the substation. To ensure reliability of such communications, message publication follows a periodical mechanism: in stable conditions, the same information is published within a standard period T_0 . When a data item changes, its new value is sent at a higher frequency, then publication rhythm progressively slows down back to stable conditions. Regarding the cybersecurity tools, an attacking computer is connected to the high-speed real-time network and launches **false data injection** and **spoofing GOOSE attacks** [Kabir16].

2.1.3 Attacking tools

Strictly speaking, an IEC 61850 attack would be an attack to specific protocols i.e. MMS, GOOSE, PTP, HSR, sending messages that the IEC 61850 components would eventually understand. Therefore, it can be made only by a specific component which is able to spoof a real device or to inject IEC 61850 messages. For example, for a MITM successful attack, the real components (source and destination) must rely on the malicious software/component in the middle. Therefore, as a first step, conventional attacks (DoS for the service and ARP Spoofing for the client) must be launched. Once the control is taken, the second step is a malware injecting/modifying messages into the IEC 61850 communication channels.

The cybersecurity tools include an attack generation station and a network analyzer. Usually starting from the highest level which is the operating system we will use Kali Linux which includes all the required tools and services to help successfully simulate an attack against IEC 61850 Protocol. Moreover, we can use the Kali Linux built in and famous network analyzer which is Wireshark.

In the following list, the most common attacking tools are described:

- **Metasploit**⁴. Based on the "exploit" concept, this tool contains code which can circumvent security measurements and break into the system. It is a commercial product, but a free version is available.
- **W3af**⁵. Open Source framework for scanning Web Applications. It detects vulnerabilities such as SQL injection, cross-site scripting, application errors and PHP misconfigurations
- **Nmap**⁶. This tool looks for open ports in a system or entire network
- **Hydra**⁷. This application is designed for brute force attacks even for multiple protocols. It has both command line and graphic interfaces.

⁴ <https://www.metasploit.com/>

⁵ <http://w3af.org/>

⁶ <https://nmap.org/>

⁷ <https://github.com/vanhauser-thc/thc-hydra>

- **Wafw00f**⁸. This software detects whether a component has WAF (Web Application Firewalls) or not
- **Ettercap**⁹. A network sniffer which allows filters to exploit only the desired vulnerabilities. It allows attacks such as spoofing, MITM or DoS. It has both command line and graphic interfaces.
- **Siege**¹⁰. This application is designed for load testing in servers, but it is usually used in Denial of Service attacks by hackers.
- **Slowloris**¹¹. Application for performing DoS. It keeps the connections opened for multiple and simultaneous invocations.
- **hping3**¹². Among other functionalities, it allows to send thousands of packets per second, even simulating different source addresses. It allows perform DoS not only of the targeted device, but the complete network as well.

Note: Although IEC 61850 does not include any HTTP-based protocol, some tools listed above exploit it. This is the reason why some of these tools are available in the previous list.

2.1.4 Attacks detection

One of the most important mechanisms to detect the aforementioned attacks is with Intrusion Detection Systems, which are based on the identification of signatures associated to the attacks to detect. The IDS usually lie in the same network as the system which is being attacked.

As any IDS, the **Error! Reference source not found.** described in **Error! Reference source not found.** detects the attacks described in **Error! Reference source not found.**, however, after a successful attack, valid IEC 61850 messages are present in the Ethernet network. Therefore, it is more difficult to detect malicious messages unless the IDS can understand the application protocols, the substation (electric and network) topology, as well as its configuration. The **Error! Reference source not found.**, described in section **Error! Reference source not found.**, adds extra information concerning substation components (named logical and physical devices in IEC 61850). This way, the **Error! Reference source not found.** is more robust because it also detects not allowed operations for the specific substation.

Another possible solution is with the usage of a SIEM, used to collect all required logs and add the policies and rules required to detect such attacks.

Finally, a combination of a honeypot and a SIEM could be the best solution to catch an attack before it makes real damage to the infrastructure. The honeypot imitates the function of the real infrastructure and it provides the time for the SIEM to catch the actual attack before the attacker understand that the system which is focusing is not the real one.

2.2 IEC 60870-5-101/104

2.2.1 Description

IEC-60870-5-104 [IEC60870-104] also called for short IEC104, is an international standard released in 2000 by IEC and it is often used in electrical industries in Europe. Its application layer is based on IEC101. IEC104 enables the communication between the control station and the substation using

⁸ <https://github.com/EnableSecurity/wafw00f>

⁹ <https://www.ettercap-project.org/>

¹⁰ <https://linux.die.net/man/1/siege>

¹¹ <https://github.com/gkbrk/slowloris>

¹² <https://tools.kali.org/information-gathering/hping3>

TCP/IP. Its advantage is that it enables communication using a standard network, which allows simultaneous data transmission between several devices and services.

The messages that are sent by IEC101 use one of the two directions of the communication, (i) control direction from the control station to the RTU transported using data types with TypeIDs begging with “C_”, or (ii) monitor direction from RTU to the control station and these are transported using data types with TypeIDs begging with “M_”. The standard IEC104 data types are presented in Table 1.

An IEC104 packet is called Application Protocol Data Unit (APDU), and it contains a header called Application Protocol Control Information (APCI).

There are three types of filed formats, (i) I-format to perform numbered information transfer and consist additionally the Application Service Data Unit (ASDU) that determines the type of function they carry i.e. the TypeID, (ii) S-format to perform numbered supervisory functions, and (iii) U-format to perform unnumbered control functions, which are built from the APCI.

All the ASDU structures include a common header to identify the following, (i) Type Identification (TI) identifies the ASDU and then its format and its content, (ii) Variable Structure Qualifier (VSQ) describes how the information objects are organized, (iii) Cause of Transmission (COT) includes the reason for sending the ASDU and one byte with an identifier of the control centre, (iv) Common Address of ASDU (CASDU) used to identify the data in the system and (v) Information objects include the content of the requested service or the notified information.

Table 1. Standard IEC104 data types

3	M_DP_NA_1	Double point information
5	M_ST_NA_1	Step position information
7	M_BO_NA_1	Bit string of 32 bit
9	M_ME_NA_1	Measured value, normalized value
11	M_ME_NB_1	Measured value, scaled value
13	M_ME_NC_1	Measured value, short floating point value
15	M_IT_NA_1	Integrated totals
20	M_SP_NA_1	Packed single-point information with status change detection
21	M_ME_ND_1	Measured value, normalized value without quality descriptor
45	C_SC_NA_1	Single command
46	C_DC_NA_1	Double command
47	C_RC_NA_1	Regulating step command
48	C_SE_NA_1	Setpoint command, normalized value
49	C_SE_NB_1	Setpoint command, scaled value
50	C_SE_NC_1	Setpoint command, short floating point value
51	C_BO_NA_1	Bit string 32 bit
70	M_EI_NA_1	End of initialization
100	C_IC_NA_1	(General-) Interrogation command
101	C_CI_NA_1	Counter interrogation command
102	C_RD_NA_1	Read command
103	C_CS_NA_1	Clock synchronization command
104	C_TS_NB_1	(IEC 101) Test command

105	C_RP_NC_1	Reset process command
106	C_CD_NA_1	(IEC 101) Delay acquisition command
110	P_ME_NA_1	Parameter of measured value, normalized value
111	P_ME_NB_1	Parameter of measured value, scaled value
112	P_ME_NC_1	Parameter of measured value, short floating point value
113	P_AC_NA_1	Parameter activation
120	F_FR_NA_1	File ready
121	F_SR_NA_1	Section ready
122	F_SC_NA_1	Call directory, select file, call file, call section
123	F_LS_NA_1	Last section, last segment
124	F_AF_NA_1	Ack file, Ack section
125	F_SG_NA_1	Segment
126	F_DR_TA_1	Directory
127	F_SC_NB_1	QueryLog – Request archive file

The TypeIDs described above, it is possible to parse traffic containing the most commonly used functions.

2.2.2 Main attacks

With recent malware developed to abuse the lack of security mechanisms in IEC104, it is important to include real-time monitoring capabilities for this protocol. By making this parser available, the target is to share a practical solution for packet inspection, which will enable research with respect to monitoring and intrusion detection of the IEC104 based on the SDN-microSENSE user requirements defined in D2.1 are the following:

- (1) Attempt to identify IEC104 ICS protocol.
- (2) IEC104 DoS attack that sends continuously malicious IEC104 packets to the target system.
- (3) Malicious IEC104 commands. Various kinds of IEC104 commands are executed to the target system.

In particular, the following attacks can be directly performed against IEC-104.

- **M_SP_NA_1_DoS:** It is a packet flooding attack. The M_SP_NA_1 is a Single-point information without time tag command in the Monitor Direction. The specific cyberattack sends continually to the target system M_SP_NA_1 packets. The aim is to generate a possible malfunction to the MTU, confuse the system operator or even disrupt the operation of MTU. The configured PLC transmits M_SP_NA_1 command to MTU per second.
- **C_SE_NA_1_DoS:** It is a packet flooding attack. The C_SE_NA_1 is a Set-point Command with normalized value in the Control Direction. This cyberattack floods the target with C_SE_NA_1 packets. The aim is to generate a possible malfunction to the MTU, confuse the system operator or even disrupt the operation of MTU. The configured PLC transmits C_SE_NA_1 command to MTU per second.
- **C_SC_NA_1_DoS:** It is a packet flooding attack. The C_SC_NA_1 command is Single command in the Control Direction. Similarly, this attack sends continuously to the target system C_SC_NA_1_packets. The aim is to generate a possible malfunction to the MTU, confuse the

system operator or even disrupt the operation of MTU. The configured PLC transmits C_SC_NA_1 command to MTU per second.

- **C_SE_NA_1:** The C_SE_NA_1 is a Set-point Command with normalized value in the Control Direction. This cyberattack constitutes an unauthorised access, transmitting to the target system C_SE_NA_1 packets. An authorized client sends a Control command to a Server using the C_SE_NA_1. The unauthorized client is created by modifying the static IP of the authorized client, in order not to be recognized as part of the recognized network.
- **C_CI_NA_1:** The C_CI_NA_1 is a Counter Interrogation command in the Control Direction. This cyberattack sends unauthorised C_CI_NA_1 packets to the target system. It's an unauthorized access attack. Normally, an unauthorized user should not be able to communicate with PLC. However, IEC104 does not provide any authentication mechanism. To emulate this attack, the IP address of the attacker is modified appropriately, in order not to be considered as a member of the network.
- **C_SC_NA_1:** The C_SC_NA_1 command is Single command in the Control Direction. This cyberattack is another unauthorised access attempt related to IEC-104, transmitting C_SC_NA_1 packets to the target. An authorized client sends a Control command to a Server using the C_SC_NA_1. The unauthorized client is created by modifying the static IP of the authorized client, in order not to be recognized as part of the recognized network.
- **C_CI_NA_1_DoS:** It is a packet flooding attack. The C_CI_NA_1 is a Counter Interrogation command in the Control Direction. This cyberattacks constitutes a DoS related to IEC-104, transmitting continuously C_CI_NA_1 packets to the target system. The aim is to generate a possible malfunction to the MTU, confuse the system operator or even disrupt the operation of MTU. The configured PLC transmits C_CI_NA_1 command to MTU per second.

2.2.3 Attacking Tools

As penetration testing tool, Scapy¹³ was used in order to test and assess the vulnerabilities of IEC104:

Any cyber infrastructure is an integral part of a network. For the networking aspect of pentesting and other security assessment tasks such as Nmap, tcpdump, arppoof, there are numerous tools available, but one tool that stands out is Scapy. The most important thing is that it can also be used as a library in the Python programs that allow the pentester to generate its own tool according to the demand. Scapy is a powerful interactive packet manipulation tool written in Python. It helps us to analyze packets, to build, send and slice.

2.2.4 Attacks detection

The tools that are used were the Suricata and "SID iec104 rules generator" (SIREN). Suricata is used to detect IEC104-related cyberattacks in the sense of Task 5.2 / D5.2. The SIREN is able to load a pcap file with normal traffic, identify the packets and their formats i.e. i-format, u-format, s-format and create a file with IEC104 rules for Suricata, using Scapy. Recent studies have demonstrated the efficacy of Suricata to detect effectively cyberattacks against IEC104. Some remarkable cases are listed in [Radoglou-Grammatikis19] and [Yang17].

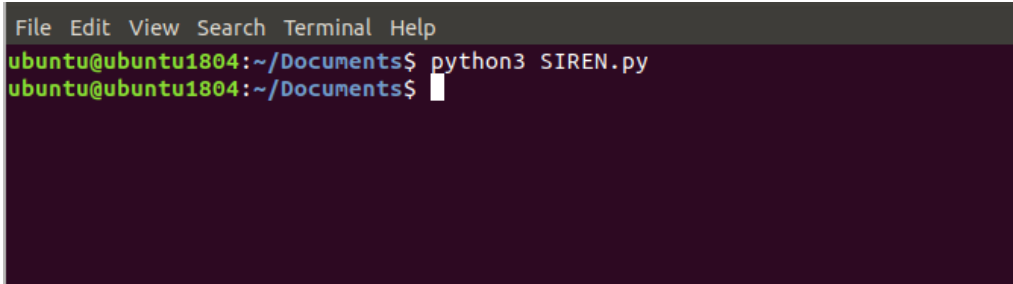
¹³ <https://github.com/Feanaur/Scapy-Pentest>

SIREN (SID iec104 rules generator)

STEP1: Define the pcap file

```
from scapy.all import *
packets = rdpcap("/home/ubuntu/Documents/server3.pcap")
```

STEP2: Run the SIREN python script.



```
File Edit View Search Terminal Help
ubuntu@ubuntu1804:~/Documents$ python3 SIREN.py
ubuntu@ubuntu1804:~/Documents$
```

STEP3: Open the “IEC104_Rules.txt” file with the identified rules.



```
Open IEC104_RULES.txt Save
alert tcp any [1024:] <=> any 2404 ( msg:"PROTOCOL-SCADA IEC 104 C_IC_NA_1";flow:established; content:"[60]",depth 1; content:"[64]",within 1,distance 5;
reference:Slidroco_Holdings_IEC104_Rules; classtype:protocol-command-decode; sid:52204; rev:1;)
alert tcp any [1024:] <=> any 2404 ( msg:"PROTOCOL-SCADA IEC 104 C_SC_NA_1";flow:established; content:"[60]",depth 1; content:"[20]",within 1,distance 5;
reference:Slidroco_Holdings_IEC104_Rules; classtype:protocol-command-decode; sid:52205; rev:1;)
```

STEP4: Validate that only these rules exist to the pcap file.

No.	Time	Source	Destination	Protocol	Length	Info
1873	6523.555683	27	25	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2
1893	6585.829059	27	25	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2
1921	6687.144463	27	25	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2
1945	6767.297679	27	25	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2
2025	7174.390983	27	25	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2
2053	7270.694107	27	25	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2
2084	7362.984954	27	25	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2
94	355.082542	27	25	104asdu	82	<- I (0,2) ASDU=1 C_SC_NA_1 Act IOA=2
198	685.079356	27	25	104asdu	82	<- I (0,2) ASDU=1 C_SC_NA_1 Act IOA=2
1217	4315.087227	27	25	104asdu	82	<- I (0,2) ASDU=1 C_SC_NA_1 Act IOA=2
85	345.046558	20	25	104asdu	70	<- I (1,14) ASDU=1 C_IC_NA_1 Act IOA=0
919	3315.050551	20	25	104asdu	70	<- I (10,142) ASDU=1 C_IC_NA_1 Act IOA=0
1019	3645.047663	20	25	104asdu	70	<- I (11,160) ASDU=1 C_IC_NA_1 Act IOA=0
1117	3975.051567	20	25	104asdu	70	<- I (12,177) ASDU=1 C_IC_NA_1 Act IOA=0
1209	4305.047648	20	25	104asdu	70	<- I (13,193) ASDU=1 C_IC_NA_1 Act IOA=0
1314	4635.047669	20	25	104asdu	70	<- I (14,212) ASDU=1 C_IC_NA_1 Act IOA=0
1411	4965.047379	20	25	104asdu	70	<- I (15,228) ASDU=1 C_IC_NA_1 Act IOA=0
1508	5295.047985	20	25	104asdu	70	<- I (16,246) ASDU=1 C_IC_NA_1 Act IOA=0
1597	5625.047832	20	25	104asdu	70	<- I (17,261) ASDU=1 C_IC_NA_1 Act IOA=0
1701	5955.050180	20	25	104asdu	70	<- I (18,279) ASDU=1 C_IC_NA_1 Act IOA=0
1801	6285.047567	20	25	104asdu	70	<- I (19,296) ASDU=1 C_IC_NA_1 Act IOA=0
190	675.046144	20	25	104asdu	70	<- I (2,31) ASDU=1 C_IC_NA_1 Act IOA=0

In the context of D5.2, Suricata and SIREN were used to implement the respective unit tests related to the detection tools provided by Task 5.2/D5.2. Unique IEC104 rules were found for this reason and provided by Annex1. In this respect, Suricata checked the applicability and validity of the rules and described in Section 4 (Unit Tests).

The following example present an alert message of Suricata regarding the detection of a IEC104 cyberattack. This message is sent to the XL-SIEM agent, which undertakes to normalise it, thus producing the respective security alert.

```
{"timestamp":"2020-04-28T21:24:59.491102+0300","flow_id":375306941721969,"pcap_cnt":6956,"event_type":"alert","src_ip":"X.X.X.28","src_port":XXX9,"dest_ip":"X.X.X.21","dest_port":XXX4,"proto":"TCP","flow":{"pkts_toserver":6,"pkts_tocl
```

```
ient":3,"bytes_toserver":426,"bytes_toclient":228,"start":"2020-04-28T21:24:49.355697+0300"},"alert":{"action":"allowed","gid":1,"signature_id":52171,"rev":1,"signature":"PROTOCOL-SCADA IEC 104 C_SC_NA_1","category":"Generic Protocol Command Decode","severity":3}}
```

2.3 Modbus

2.3.1 Description

Modbus is an industrial communication protocol utilised widely by SCADA systems in the energy sector due to its simplicity, easy deployment and open specifications. Figure 4 depicts the reference structure of Modbus, which is provided through two versions a) serial communication (Modbus/RTU) and b) TCP/IP (Modbus/TCP). In particular, the general Modbus frame is called Application Data Unit (ADU), which in turn consists of a) the Protocol Data Unit (PDU), b) Addressing and c) Error Checking. PDU encloses the primary information of the Modbus packets, including the function code and the respective data [PLIATSIOS20]. Each function code defines a different functionality. The whitepaper [Modbus15] summarises and details the available Modbus function codes and their necessary data. It is noteworthy that each manufacturer and programmer has the capability to develop its own Modbus function codes. On the other side, the addressing and error checking functionalities rely on the Modbus version (i.e., a) Modbus/RTU or b) Modbus/TCP). In the Modbus RTU version, the master and each slave are characterised by unique IDs while the error checking is achieved through Cyclic Redundancy Check (CRC). On the other hand, in the Modbus/TCP version, the Slave ID field is replaced by the Modbus Application Protocol (MBAP) header, which in turn includes a) the Transaction Identifier, b) the Protocol Identifier, c) Length and d) Unit Identifier. The protocol identifier is always equal to zero for the current Modbus services, and other values are reserved for potential extensions. Length indicates the size of the remaining field, including Unit ID, Function Code and Data. The Unit ID is used for serial connecting to a Modbus device which does not use the Modbus/TCP version. Finally, the error checking functionality was replaced by the corresponding mechanisms of TCP/IP. It is worth mentioning that based on the SDN-microSENSE user requirements and the technical specification defined in D2.2 and D2.3, respectively, D5.2 focuses mainly on Modbus/TCP.

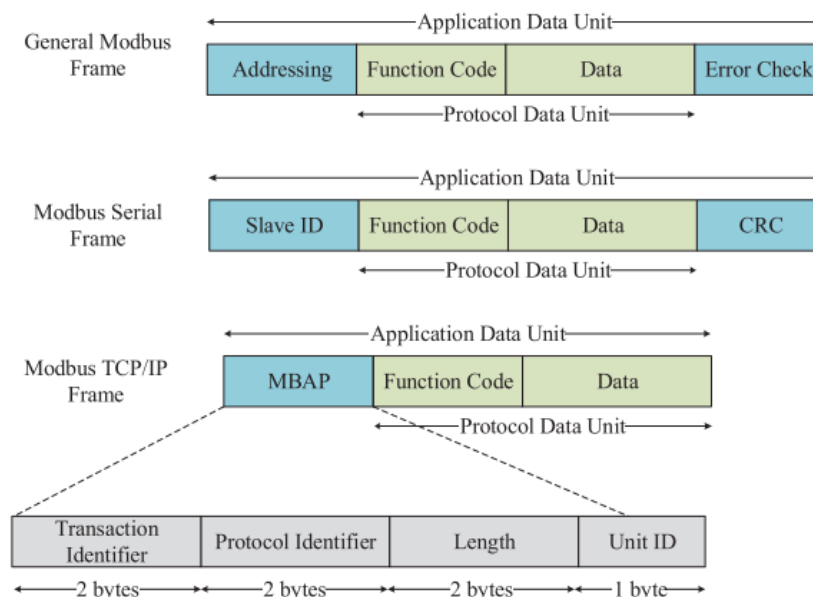


Figure 4. Modbus/TCP frame information [PLIATSIOS20]

2.3.2 Main attacks

Modbus/RTU and Modbus/TCP are characterised by severe security issues since they were not constructed having cybersecurity in mind. In particular, they do not include sufficient authentication and access control rules, thus allowing a plethora of unauthorised access and MiTM attacks. P. Huitsing et al. in [Huitsing08] summarise and describe the various attacks against Modbus RTU and Modbus TCP. Based on the SDN-microSENSE user requirements defined in D2.1, WP5 focuses mainly on the following Modbus/TCP cyberattacks.

- **modbus/function/readInputRegister (DoS):** This Modbus/TCP attack sends continuously a plethora of Modbus/TCP packets with the function code 04 (Modbus Read Input Register packet) to the target system, thus aiming to corrupt its availability.
- **modbus/function/writeSingleCoils:** This unauthorised access Modbus/TCP attack takes full advantage of the lack of authentication and authorisation mechanisms by changing the status of single coil either to ON or OFF through a Modbus/TCP packet with the function code 05.
- **modbus/scanner/getfunc:** This reconnaissance Modbus/TCP attack enumerates all Modbus/TCP function codes supported by the target system. Usually, it constitutes the first step when a cyberattacker tries to exploit the vulnerabilities of the Modbus/TCP protocol. Based on the outcome, the cyberattacker can proceed to unauthorised access, Man-in-The-Middle (MiTM) or Denial of Service (DoS) attacks targeting the corresponding Modbus/TCP services (Modbus/TCP function codes).
- **modbus/dos/writeSingleRegister:** This DoS Modbus/TCP attack transmits continuously Modbus/TCP packets with the function code 06 to the target system. The goal of the cyberattacker is to affect the availability of the target. The particular Modbus/TCP function code is used to write a single register in the TCP server Modbus device (e.g., slave device).
- **modbus/function/readDiscreteInputs (DoS):** This DoS Modbus/TCP cyberattacks sends a plethora of Modbus/TCP packets with the function code 02. The specific function code is utilised to read the status of the discrete inputs of a Modbus/TCP server. As in the previous case, the cyberattack aims to disrupt the availability of the Modbus/TCP server.
- **modbus/function/readHoldingRegister (DoS):** This Modbus/TCP cyberattack also targets the availability of a Modbus/TCP device by sending multiple Modbus/TCP packets with the function code 03. This function code is used to read the content of a holding register.
- **modbus/function/readCoils (DoS):** As in the previous cases, this Modbus/TCP cyberattack is another DoS attack, which exploits in this time the function code 01. The attacker sends continuously to the target system a plethora of Modbus/TCP packets with the function code 01 that read the status of a single coil.
- **modbus/function/readInputRegister:** This unauthorised access Modbus/TCP cyberattack aims to violate the confidentiality of a Modbus/TCP input register by reading its content. Since Modbus/TCP does not include any authentication or authorisation mechanism, the cyberattackers have the capability to execute such cyberattacks in order to read or change the content of the various Modbus/TCP registers without the necessary permissions.

- **modbus/function/writeSingleRegister:** This unauthorised access Modbus/TCP cyberattack targets both the confidentiality and integrity of a Modbus/TCP single register by sending a Modbus/TCP packet with the function code 06, thus changing its content.
- **modbus/dos/writeSingleCoils:** This DoS Modbus/TCP cyberattack is another DoS attack, which uses the Modbus/TCP packets with the function code 05. The specific function code is used to change the value of a single coil to ON or OFF.
- **modbus/function/readDiscreteInput:** This Modbus/TCP unauthorised access cyberattack violates the confidentiality of a Modbus/TCP device by reading the content of multiple discrete inputs. It uses Modbus/TCP packets with the function code 02.
- **modbus/scanner/uid:** This Modbus/TCP reconnaissance cyberattack enumerates the slave IDs supported by the target system. As in the case of modbus/scanner/getfunc, it usually constitutes the first step for other cyberattacks targeting Modbus/TCP. Based on the available slave IDs given by this cyberattack, next, the cyber attacker can adapt and specify the following cyberattacks (e.g., unauthorised access cyberattacks).
- **modbus/function/readCoils:** This Modbus/TCP unauthorised access cyberattack accesses the content of a single coil. To this end, a Modbus/TCP packet with the function code 01 is utilised.
- **modbus/function/readHoldingRegister:** It constitutes the most usual unauthorised access attack against Modbus/TCP targeting the content of a holding register via a Modbus/TCP packet with the function code 03.

2.3.3 Attacking tools

Several penetration testing tools have been developed in order to test and assess the vulnerabilities of Modbus/TCP. The most widely used of them are summarised below.

- **SMOD:** SMOD [Radoglou-Grammatikis20+1] is a pen-testing tool devoted to Modbus RTU and Modbus/TCP, including multiple Modbus-related cyberattacks. It relies on Python and Scapy. Its functional environment is very similar to Metasploit.
- **UOWM SMOD:** UOWM SMOD is an extension of the aforementioned SMOD tool developed by UOWM [Radoglou-Grammatikis20+1], incorporating more experimental Modbus/TCP-related cyberattacks, such as a) teardrop, b) port pool exhaustion, c) response delay and d) baseline response delay.
- **Metasploit:** Metasploit¹⁴ includes several modules devoted to Modbus, such as a) modbus_findunitid, b) modbusdetect, c) modbus_zip and d) modbusclient. The first one transmits a Modbus/TCP packet with the function code 04 (Read Input Registers) and returns the Unit ID of the Modbus endpoint. The second module (modbusdetect) detects whether Modbus is used by the target system. Next, modbuszip extracts from a pcap file a ZIP file which was transmitted via Modbus. Finally, modbusclient enables the penetration tester or the cyberattacker to read and write appropriate data via Modbus.
- **mbtget:** mbtget¹⁵ is a Modbus/TCP client written in Perl which enables a plethora of Modbus/TCP transactions.

¹⁴ <https://www.rapid7.com/db/?q=modbus&type=metasploit>

¹⁵ <https://nmap.org/nsedoc/scripts/modbus-discover.html>

- **Nmap NSE (modbus-discover):** This script (modbus-discover) of the NMAP NSE¹⁶ enumerates which slave IDs are supported by the target system or network and displays information about their vendor and firmware.
- **Modbus/TCP Fuzzer:** The Modbus/TCP Fuzzer was developed by A. Voyiatzis et al. [Voyiatzis15] Modbus/TCP Fuzzer includes Modbus/TCP-related reconnaissance attacks and performs relevant fuzzing action, thus revealing potential bugs and vulnerabilities of the Modbus/TCP application. It is not available publicly.
- **CAS Modbus Scanner:** CAS Modbus Scanner¹⁷ can detect and identify whether the assets of a network use the Modbus/TCP service. It is also capable of retrieving and displaying the values of coils, input and holding registers.
- **TCP Modbus Hacker:** TCP Modbus Hacker is a Java application, which was developed by S. Bhatia et al. [PLIATSIOS200] and it can read and write input and holding registers as well as coils, thus executing the respective unauthorised access and DoS attacks. It is not available publicly.
- **ModScan:** ModScan [PLIATSIOS201] identifies whether the assets of a network utilise Modbus/TCP.

In the context of D5.2, SMOD and UOWM SMOD were used to implement the respective unit tests related to the detection tools provided by Task 5.2/D5.2.

2.3.4 Attacks detection

In the context of Task 5.2/D5.2, Suricata is used to detect Modbus/TCP-related cyberattacks presented above. To this end, particular signature and specification Modbus-related rules were identified and provided by Annex 2. The applicability and validity of the particular rules were tested using Suricata in section 4. Suricata is analysed further in subsection 3.2. . Its is noteworthy, that recent papers have confirmed the effectiveness of Suricata against Modbus/TCP cyberattacks. Some notable papers are provided by K.Wong et al. in [Wong17] and O. N. Nyasore et al. in [Nyasore20]. The following example presents an alert message of Suricata regarding the detection of a modbus/function/readCoils cyberattack. This message is sent to the XL-SIEM agent, which undertakes to normalise it, thus producing the respective security alert.

```
{"timestamp":"2020-03-25T13:12:22.707663+0200","flow_id":"1409353732485049","pcap_cnt":6775,"event_type":"alert","src_ip":"XX.XX.XX.6","src_port":XXX8,"dest_ip":"XX.XX.XX.9","dest_port":XXX,"proto":"TCP","tx_id":0,"alert":{"action":"all owed","gid":1,"signature_id":2,"rev":0,"signature":"Modbus\\TCP Alert - Not Allowed Moudbus\\TCP Function Code","category":"","severity":3,"app_proto":"modbus","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_to server":284,"bytes_toclient":216,"start":"2020-03-25T13:12:22.683961+0200"}}
```

2.4 DNP3

2.4.1 Description

Distributed Network Protocol Version 3.0 (DNP3) constitutes an open industrial protocol that was established in the 1990s and defines communications between master devices, RTUs and a number of IEDs. The key incentive of its development was the interoperability among different systems in various

¹⁶ <https://nmap.org/nsedoc/scripts/modbus-discover.html>

¹⁷ <https://store.chipkin.com/products/tools/cas-modbus-scanner>

types of industries. Ever since its distribution, DNP3 has been widely adopted in Critical Infrastructures (CIs), including EPES, especially in the US. DNP3 was specifically designed targeting SCADA applications and thus involves the acquisition of information and the exchange of control commands among distinct computer devices. In contrast to general IT protocols, DNP3 is used to transmit relatively smaller data packets in a robust way that arrive in well-defined sequences, rendering it appropriate for SCADA control. Notable features of DNP3 include the detailed specification of data objects and a comprehensive certification system.

The following system topologies are supported by DNP3:

- a) Master – slave: Direct one-on-one communication between a master and a slave station.
- b) Multi-drop: One master station communicates with several slaves.
- c) Hierarchical: An intermediate slave can act as master station for different slave devices.
- d) Multiple master: Several master stations communicate with one slave.

The DNP3 protocol is based on the three-layer Enhanced Performance Architecture (EPA) model which was defined by the IEC and constitutes a sub-set of the Open Systems Interconnection (OSI) model [Clarke04]. When examined with respect to the OSI model, DNP3 is composed of the following three layers:

- a) **Application layer:** This layer is responsible for combining the application service data with the application protocol control information and creating the application protocol data unit (APDU). All the necessary commands and generic data types required for controlling the various entities in the system are defined in this layer.
- b) **Transport layer:** Often referred to as pseudo-transport, this layer is responsible for segmenting the APDU from the application layer into several data link frames, inserting a single-byte function code that indicates the position of the frame in the message.
- c) **Data link layer:** This layer manages the logical link between the communicating devices. A control byte is added here, specifying the purpose of the data link frame, and the status of the logical link. The data link layer provides addressing services for data while offering techniques for multiplexing, data fragmentation, error checking, link control and prioritisation.

Besides the above, DNP3 can also be encapsulated into Ethernet packets and used over TCP/IP, enabling SCADA communications in local or Wide Area Networks (WANs). More information about the technical details of DNP3 is provided in [Pliatsios20].

As with several industrial protocols, DNP3 is a standard that was not designed with integrated cyber-security mechanisms [0IN4]. Comprehensive analysis on the protocol has identified several attacks that target weaknesses and exploit vulnerabilities in DNP3, raising important security issues when using it in an industrial environment [East09, Igbe17]. Although there are several categories into which DNP3 attacks can be classified, those that directly target the protocol specifications are of greater concern, since they can be directed at every SCADA system that uses the DNP3 standard, irrespective of specific implementation. Key targets of potential attacks are usually master stations, outstation devices as well as communication paths. The main attacks that threaten the security of the protocol involve intercepting, interrupting, modifying, and fabricating messages encapsulated in DNP3 packets [Igbe17]. Centered on the SDN-microSENSE requirements, the following DNP3 attacks are assessed:

- **DNP3 Enumerate:** This reconnaissance attack aims to discover which DNP3 services and functional codes are used by the target system. It is implemented via the Nmap NSE.
- **DNP3 Info:** This attack constitutes another reconnaissance attempt, aggregating various DNP3 diagnostic information related the DNP3 usage. It can be executed via the Nmap NSE.
- **DNP3 Disable Unsolicited Messages Attack:** This attack targets an outstation device, establishing a connection with it while acting as a master station. The false master then transmits a packet carrying the DNP3 function code “21” which requests to disable all the unsolicited messages on the target. A successful conduction of this attack renders the outstation device unable to send alarm messages to the actual master station in cases of critical failure in the system.
- **DNP3 Cold Restart Message Attack:** In a similar manner to the previous attack, the intruding device acts as the master station and sends a DNP3 packet that includes the “Cold Restart” function code to the target outstation. When the target receives this message, it initiates a complete restart and sends back a reply with the time window available before the restart. This attack renders the outstation unavailable for a period of time and has the risk of resulting in an inconsistent device restoration after restarting.
- **DNP3 Warm Restart Message Attack:** This attack is quite similar to the “Cold Restart Message”, but aims to trigger a partial restart, re-initiating a DNP3 service on the target outstation. This attack is of particular concern, since it could be executed several consecutive times, resulting in a denial-of-service attack, since the outstation will not be able to send events or receive control command packets, causing disruptions in the industrial procedure.

2.4.2 Attacking tools

This subsection outlines the key penetration testing tools utilised to examine the weaknesses of the DNP3 protocol and evaluate the effectiveness of the developed attack detectors. The following tools were used for this purpose:

- **Nmap Scripting Engine (NSE):** NSE constitutes a substantial and versatile feature of Nmap, offering the possibility to develop scripts that allow the automation of various network processes. It was designed with vulnerability detection mechanisms in mind, but also provides the capability of incorporating custom scripts that exploit vulnerabilities and thus can be used for penetration testing purposes as well. Two specific Nmap scripts were utilised, targeting the reconnaissance attacks described in the above subsection, namely the “DNP3 enumerate” and the “DNP3 info”.
- **OpenDNP3:** Open DNP3 is not a pent-testing tool but emulates the DNP3 service. It can be used appropriately to emulate various DNP3 cyberattacks.
- **Scapy:** Scapy constitutes a network packet manipulation tool and programming library, which gives the necessary interfaces in order to capture, parse, analyse and construct network packets. Therefore, Scapy can be used in order to perform various DNP3 attacks, such as DNP3 Disable Unsolicited Messages Attack, DNP3 Cold Restart Message Attack and DNP3 Warm Restart Message Attack.

2.4.3 Attacks detection

The attacks described above exploit weaknesses inherent to the design of the DNP3 protocol and can result in critical incidents if they are not detected early and addressed effectively [Radoglou-Grammatikis20]. In the context of Task 5.2/D5.2, Suricata is adopted to detect DNP3-related

cyberattacks. To this end, specific signature and specification DNP3 rules (available in Annex 2) were specified and tested. The “msg” label of each DNP3 specification/signature rule denotes details related to the corresponding DNP3 cyberattack. Suricata is analysed in subsection 3.2. As in the aforementioned protocols the efficacy of Suricata against DNP3-related cyberattacks has been presented by recent papers [Wong17]. A security log exported by Suricata regarding the DNP3 Disable Unsolicited Messages Attack is presented below. This message is transmitted to the XL-SIEM agent, which undertakes to produce the respective, normalised security event.

```
{"timestamp":"2017-02-14T01:28:54.950977+0200","flow_id":706430872485681,"pcap_cnt":1428,"event_type":"alert","src_ip":"XX.XX.XX.197","src_port":XXXX,"dest_ip":"XX.XX.XX.198","dest_port":XXXX,"proto":"TCP","alert":{"action":"allowed","gid":1,"signature_id":1111203,"rev":1,"signature":"SCADA_IDS: DNP3 - Unsolicited Response Storm","category":"Attempted Denial of Service"},"severity":2},"flow":{"pkts_toserver":2,"pkts_toclient":2,"bytes_toserver":140,"bytes_toclient":157,"start":"2017-02-14T01:28:54.950065+0200"}}
```

3 Main detection tools

The techniques described in Section 2 are supported by underlying technologies that allows their deployment in real infrastructures. To this end, the state of the art of technologies for the detection of cyber incidents, and more specifically IDPSs, is mostly taken by proprietary commercial solutions, typically integrated in bigger solutions that includes additional capabilities(i.e., SIEM or SOC). Such is the case of Cisco IOS IPS¹⁸, Real Secure Network from IBM¹⁹ or McAfee Network Security Platform²⁰. The open source community counts with several alternatives for IDPS, such as Kismet²¹ or Prelude OSS²². However, the most popular and considered as de facto standard in IDPSs technologies is Snort²³. Snort is a rule based IDPSs that analyses traffic either in real time or from precaptured network packets, detecting incidents and triggering alerts in different possible formats. The support from the cyber security solution is very consolidated, with rules that are updated daily and the possibility to update them automatically. An evolution of Snort is Suricata, which improves Snort on the support for multithreading processing, increasing performance. Suricata uses the same rules format as Snort does, which guarantee the support of the community. Therefore, Suricata has been chosen as the best option to include the detection mechanisms described in Section 2. As a result, these technologies results in a set of Suricata rules as listed in the Annexes of this document. Section 3.1 describes Suricata, how it works and how it is integrated with the XL-SIEM. Section 3.2 describes the Tecnalia's SBT Aware, which is also based on Suricata rules. Finally, Section 3.3 describes the Nightwatch IDPS, which is a CLS proprietary solution for detecting cyber incidents using SDN information.

3.1 Enhanced Suricata for EPES

Suricata is a real time intrusion detection (IDS) that can also act as an inline intrusion detection (IPS), network security monitoring (NSM) and is capable of processing network traffic files (pcap) offline. Suricata is open source and publicly available.

Suricata analyses network traffic, either in real time sniffing directly from the network, or offline through a network capture file. It supports multi-threading processing, optimizing the CPU usage. It is also capable of detecting the protocol of the network traffic automatically for IP, TCP, UDP and ICMP. I can also detect incidents associated to other specific application protocols such as FTP, HTTP, TLS and SMB, and it can be extended to support additional protocols, as it has been done in SDN-microSENSE.

Suricata works with rules. The network traffic is analysed by Suricata, parsed and compared with a set of predefined rules. The rules to be compared can be configured in order to optimize the detection and performance. Suricata rules (also known as signatures) consists of three main parts:

- The action, represents the action to be taken when the rule matches.
- The header, represents general information related to the rule, such as IP addresses to match, the direction of the rule or the ports.

¹⁸ <https://www.cisco.com/c/en/us/products/security/ios-intrusion-prevention-system-ips/index.html>

¹⁹ <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=DD&subtype=SM&htmlfid=897/ENUS5765-ISS>

²⁰ <https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html>

²¹ <https://www.kismetwireless.net/>

²² <https://www.prelude-siem.org/>

²³ <https://www.snort.org/>

- The rule options, which are specific fields that can be specified in the rule for a more accurate matching.

For example, for the following rule:

```
alert tcp $HOME_NET 502 -> $EXTERNAL_NET any (msg:"PROTOCOL-SCADA Modbus function scan";
flow:established,to_client,no_stream; content:"|00 00|"; depth:2; offset:2; byte_test:1,&,128,7;
content:"|01|"; depth:1; offset:8; detection_filter:track by_dst, count 3, seconds 10;
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf;
classtype:protocol-command-decode; sid:29314; rev:2;)
```

- The action is “alert”
- The header is “tcp \$HOME_NET 502 -> \$EXTERNAL_NET any”, being:
 - tcp: the protocol.
 - \$HOME_NET: The IP address (or subnet) of the home network that is monitored. The value of this variable is configured in the Suricata configuration file.
 - 502: The port for the source of the packet.
 - \$EXTERNAL_NET: The IP address (or subnet) of the destination of the packet. The values of this variable are configured in the Suricata configuration file.
 - Any: The port of the destination of the packet. In this case this rule applies to any port.
- The rule options are “msg:”PROTOCOL-SCADA Modbus function scan”; flow:established,to_client,no_stream; content:”|00 00|”; depth:2; offset:2; byte_test:1,&,128,7; content:”|01|”; depth:1; offset:8; detection_filter:track by_dst, count 3, seconds 10; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:29314; rev:2;”

Suricata as output as output supports several standard formats such as JSON, XML, CSV among others.

```
{
  "timestamp": "2020-08-28T14:59:18.033009+0000",
  "flow_id": 813102196305589,
  "in_iface": "enp2s0",
  "event_type": "alert",
  "src_ip": "xxx.xxx.x.9",
  "src_port": "xxx",
  "dest_ip": "xxx.xx.xxx.8",
  "dest_port": "xxx",
  "proto": "006",
  "metadata": {
    "flowbits": {
      "exe.no.referer",
      "ET.http.binary"
    }
  },
  "tx_id": 1,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2018959,
    "rev": 4,
    "signature": "ET POLICY PE EXE or DLL Windows file download HTTP",
    "category": "Potential Corporate Privacy Violation",
    "severity": 1,
    "metadata": {
      "updated_at": {
        "2017_02_01"
      },
      "created_at": {
        "2014_08_19"
      },
      "former_category": {
        "POLICY"
      }
    }
  }
},
  "timestamp": 1
```

Figure 5. Suricata output using JSON format

3.1.1 Input data

Suricata receives network traffic directly from the network interface that is defined in the Suricata configuration. Additionally, Suricata can also analyse traffic contained in pcap files.

3.1.2 Internals of the tool

Suricata is conceptually a simple framework, as depicted in next figure. Network traffic is captured. This traffic is decoded, reading the different parts of the packets. Depending on the type of traffic, several decoders can be applied. Once decoded packets are passed through the active rules. If any rule matches (one or more than one) an event (or more than one in case more than one matches) is reported as output. Suricata outputs are logged a text file.

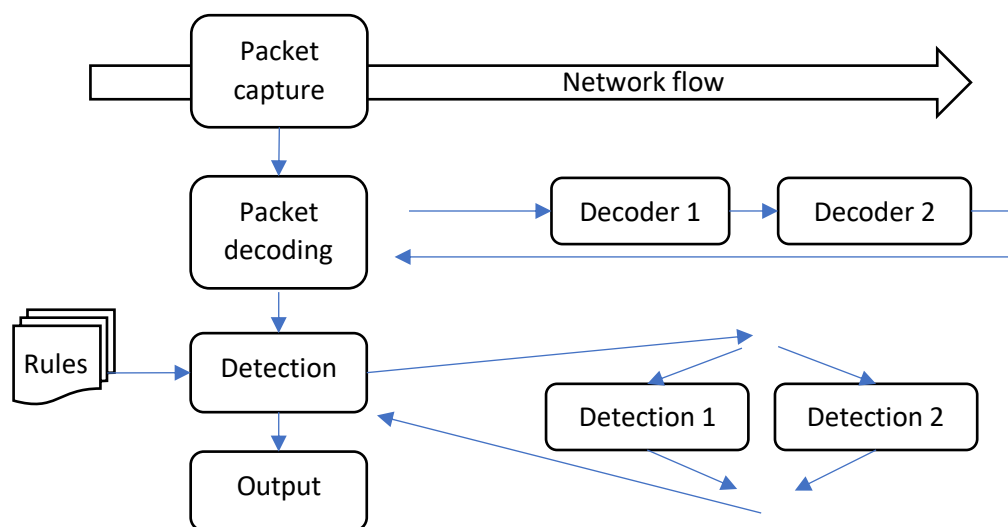


Figure 6. Suricata internals

3.1.3 Deployment

Suricata can be found in many different Linux distributions directly from their respective packet managers. Suricata can also be downloaded and compiled directly from the Suricata home page.

The Suricata configuration file is called `suricata.yaml` and can be typically found under `/etc/suricata/`. This file contains many different options. The main ones are the following:

- Address-groups: Contains the range of IP addresses to take into account for monitoring network packets. The two main variables are `HOME_NET` and `EXTERNAL_NET`. `HOME_NET` specifies the source IP or subnet that is taken into account when monitoring. For example,

`HOME_NET: "XX.XX.XX.XX/24"` indicates that only the packets with origin in this IP or range or IPs is used to apply the Suricata rules

`EXTERNAL_NET` indicates the remote IP or subnet taken into account to apply Suricata rules. It can also be used combinations of both and logic operators. For example,

`EXTERNAL_NET: "!HOME_NET"` includes all the IPs that are not inside the `HOME_NET` set.

- Port-groups: Similar to address-groups, there are a set of variables that allows to specify custom port numbers for HTTP, SSH, etc.
- Default-rule-path: defines the rule to the rule files
- Rule-files: indicates the name of the files containing the rules. Rules are written in different files. Lines commented (using #) are ignored.
- Outputs: indicates options for the different types of output that Suricata produces. All of them are plain text options. The different is in the format (normal text, json, etc), more (alert-debig) or less verbose (i.e., fast.log), pcap logs, etc.
- Af-packet, indicates the interfaces to monitor. For example, "interface: eth0" tells Suricata to sniff traffic in the eth0 interface

There are many more options that can be checked directly from the Suricata documentation.

3.1.4 Output: connection to XL-SIEM, logs and taxonomy

As it was mentioned before, Suricata produces output in plain text and written in different log files. As mentioned in Deliverable D5.1, the XL-EPDS receives logs from the different detectors (such as Suricata), through rsyslog. Therefore, it is necessary to configure rsyslog appropriately to send all events written by Suricata in its output log files (i.e., fast.log) to the XL-SIEM agent at the XL-EPDS. The following is an example of rsyslog configuration that send fast.log and eve.json logs (both produced by Suricata) to the XL-SIEM agent:

```
$ModLoad imfile
$InputFileName /var/log/suricata/fast.log
$InputFileTag suricata_fastlog
$InputFileStateFile fast.log
$InputFileSeverity alert
$InputFileFacility local6
$InputRunFileMonitor
local6.*@@XX.XX.XX.XX:xx
$InputFilePollInterval 1

$ModLoad imfile
$InputFileName /var/log/suricata/eve.json
$InputFileTag suricata_evelog
$InputFileStateFile eve.json
$InputFileSeverity alert
$InputFileFacility local7
$InputRunFileMonitor
local7.*@@ XX.XX.XX.XX:xx
$InputFilePollInterval 1
```

The following table describe the format of the logs created by Suricata and exported to the XL-SIEM agent through rsyslog.

Table 2. Description for Suricata logs

Log name	Suricata log (general taxonomy)		
Log description	This log represents an anomaly detected by Suricata. Suricata can detect a myriad of anomalies. The structure of the logs is generic enough to be interpreted by the XL-SIEM as the same type of log.		
Important fields	Field type	Possible values	Field description

Timestamp	String	Free text representing a date	Timestamp when the incident appeared (Aug 22 07:38:41 in the example below)
Incident description	String	Free text	Text describing the incident (MODBUS port 502 access in the example below)
Incident id	int	Undetermined	Unique identifier used by the XL-SIEM to know the type of incident (19700 in the example below)
Priority	int	0-5	Level of importance of the incident detected (3 in the example below)
Protocol	String	{TCP, UDP}	Type of protocol where the incident has been detected (TCP in the example below)
Source IP	String	String representing a valid ipv4 or ipv6 IP	IP address of the machine originating the anomaly (XX.XX.XX.XX in the example below)
Source Port	int	Any valid port	Port of the machine originating the anomaly (xx in the example below)
Destination IP	String	String representing a valid ipv4 or ipv6 IP	IP address of the machine targeted by the incident (YY.YY.YY.YY in the example below)
Destination Port	int	Any valid port	Port of the machine targeted by the incident (yy in the example below)
Example	Aug 22 07:38:41 ubuntu suricata[19700]: [1:1:0] MODBUS port 502 access [Classification: (null)] [Priority: 3] {TCP} XX.XX.XX.XX:xx -> YY.YY.YY.YY:yy		

A new set of rules has been created for Suricata to cover the requirements of SDN-microSENSE. These rules are listed in Annexes I, II and III. Additionally, the information related to the attacks and the detection of the incidents associated to EPES related protocols have been described in Section 2.

3.2 SBT-Aware

Most detection tools are generalist, designed to find predefined patterns such as frequency of messages, well-known malware packets, source and destination of the messages or the content of each packet itself. These tools also allow plugging modules for different protocols, offering a better understanding of the analysed data, such as the protocol action (read, write, reset...) or data model/schema understanding. However, the semantics of the data transmitted cannot be inferred. The SBT-Aware tool adds the latest feature for primary and secondary substations, taking into account not only the protocols defined in the IEC 61850 standard (see Section 2.1), but the substation topology as well.

SBT-Aware is composed by three modules. The first one is the SCL interpreter which extracts data from any SCL file and delivers it to the detection engine. The second is the detection engine which analyses

messages at real time, whereas the third module sends the reports, alarms, detected attacks, etc. to any system or human.

After the installation of the tool and the configuration of the electric substation configuration (IEC 61850) to protect, the detection engine will be capable to detect generic attacks such as deny of service, ARP spoofing, known protocol bugs exploitation, alert to IED conversations or MMS connections, as well as detecting undesired (deliberated or not) accesses to any device and requests for existing but unused data.

The innovation of the STB-Aware solution lies in the use of the IEC 61850 configuration files to generate the detection rules that will be used by an IDS, Suricata in our case. As it was explained in section 3.2.1, these files contain relevant information about the substation topology (electrical and communication), the IEDs deployed (IP address, data model, published services, ...) and data they publish and receive (reports and GOOSEs). STB-Aware processes IEC 61850 configuration files and transform its information into a set of rules that allow detecting any activity inside the substation that does not correspond to what is specified in the configuration files.

Two are the main advantages of STB-Aware: the **automatic generation of the detection rules**, and the **instantiation of the rules to a particular substation**. Modern solutions incorporate industrial protocol-based rules, which means that they can detect and process messages of this protocol. However, they are not able to interpret nothing about the equipment that has sent the message or the destination one. Rules generated by STB-Aware can contain information about the functionality of the devices that are involved in the communication.

This approach has been validated in a lab environment using a Suricata installed in Tecnalia's Cybersecurity Lab and an attack tool developed for this purpose. We have deployed the detection rules generated by the SCL-Crawler in the Suricata and executed an identity fraud attack against a real IED installed the lab. The second unit test, 61850_IED_Sniffing, included in section 4.4 explain how the Suricata detects an MMS message, that tries to request for a control switch, that is not configured, and therefore not present in the sclCrawler output file.

The following subsections describe in detail the main aspects of the SBT-Aware solution.

3.2.1 Input data

The needed information for running this tool is the following:

- SCL file(s). One or more XML documents which complies with the IEC 61850-6 specification. They are used to define the substation (electric, communications and devices) using SCL files, as follows:
 - SCD (Substation Configuration Description) file. It is the complete substation configuration, which contains the substation details. This file also contains the substation electric topology, the communications topology and the IEDs along with their functionality. Notice that in most cases the SCD file is not available or provided by the DSO.
 - CID (Configured IED Description) file. It contains the IED configuration (network and functionality) and is used to upload the configuration to the IED for the substation where it is installed. When the SCD file is not present, the tool can import several CID

files (one per IED) in order to extract the substation data, although in this case, some global information, such as the electric topology is missing.

- Rules file(s). This is a sort of rules files whose data model is understood by the detection engine. There are three kind of rules files:
 - Generic rules. They are rules for general purpose, written or imported by the cybersecurity team that describe when communication alarms or events must be launched. These rules include scripts to detect invalid connections, undesired or malware traffic, invalid ports or protocols, message flooding, etc.
 - Substation rules. It is the SCL interpreter output, which formats the allowed accesses to IEDs and their data into the detection engine data model.
 - Enhanced SBT rules. The cybersecurity team can enrich the substation rules, adding some extra information that is not present in the SCL. For example, the IED has several disconnectors, but only three of them (XSWI1, XSWI2 and XSWI3) are used. Therefore, any attempt to access XSWI4 can launch an alarm. It has the same data model as the substation rules file.
- Ethernet traffic. The detection engine listens to the Ethernet channel. There can be many communication, configuration or substation protocols (HTTP, MMS, ARP, DHCP, DNS, GOOSE, SOAP, NTP...) which can be allowed or not.
- Reporting data. In order to report alarms, this inner model allows sending alarms and events to any system in the required data format.

Note: As the SBT-Aware can use different detection and reporting tools, the rules and the reporting data format have been omitted in the present deliverable.

3.2.2 Internals of the tool

Although, as any detection tool, SBT-Aware is intended to be used in production, it can also be used at substation engineering stage. The overall system is depicted in the Figure 7, where the software modules are represented in blue, whereas the yellow files are input data created outside the tool, the green files are substation related data used for a better attack detection and the orange files contains alarms, events and alerts to be delivered to any report launcher.

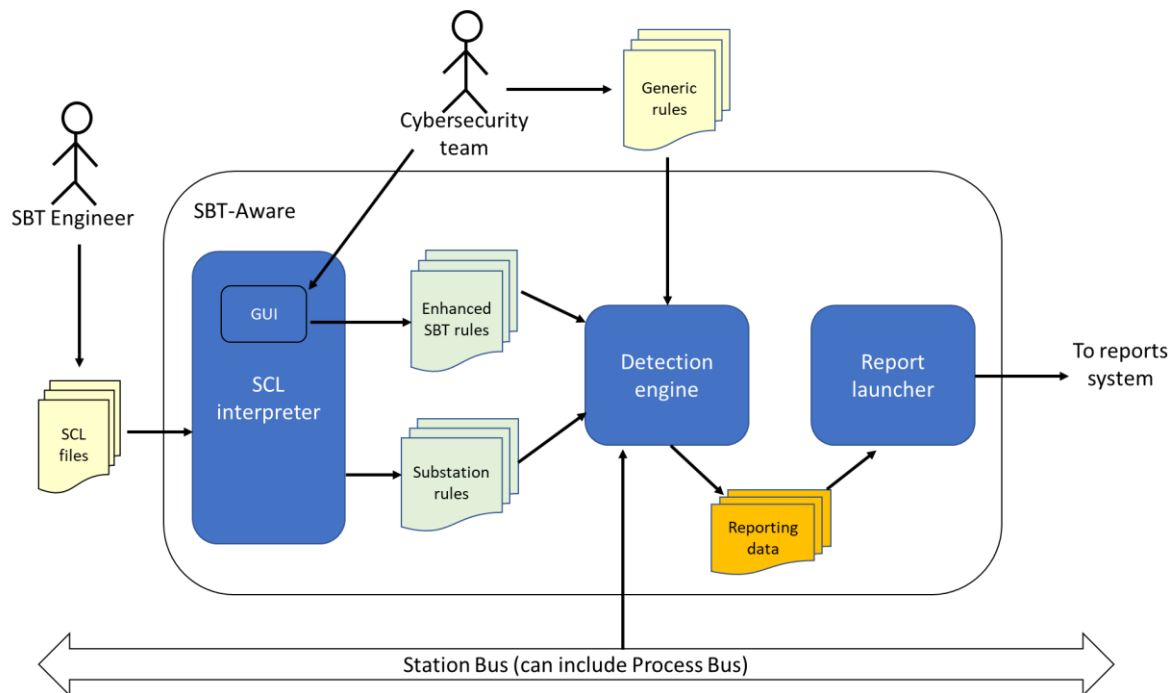


Figure 7. SBT-Aware tool, including modules, I/O data and relevant actors

In the Figure 7, two actors are involved. The SBT engineer is responsible for designing and configuring the substation, who composes the SCD file (or write one CID file per IED). The cybersecurity team creates generic rules (attack patterns) with all the data relevant to any IT/OT system. The SBT-Aware has a graphic interface in order to enhance/enrich the substation operation that can be used by the cybersecurity team with the help of the SBT engineer to generate rules that cannot be extracted from the SCL files according to the IEC 61850-6 specification.

3.2.2.1 SCL interpreter module

The SCL interpreter is an XML parser, which processes IEC 61850 (-6, -7.2, -7.3 and -7.4) SCL files and data models, for extracting devices, nodes, objects and attributes, among other general information, from any SCL file. It is an offline module whose objective is just adding information to the IDS system installed in the substation.

If we consider the cybersecurity as an onion layer defence system (DiD), where the substation processes (devices operation) are in the inner layer, when the attackers circumvented the outer layers (communications, firewalls, access control) they could operate the controls (feeders, taps, disconnectors, switches...) straightforward. In Figure 8, the classic DiD for breaking into a device is translated to its corresponding IEC 61850 substation. If the user can listen to the messages within the station bus and manages to associate (MMS association or ARP spoofing) to an IED, the attackers can send messages.

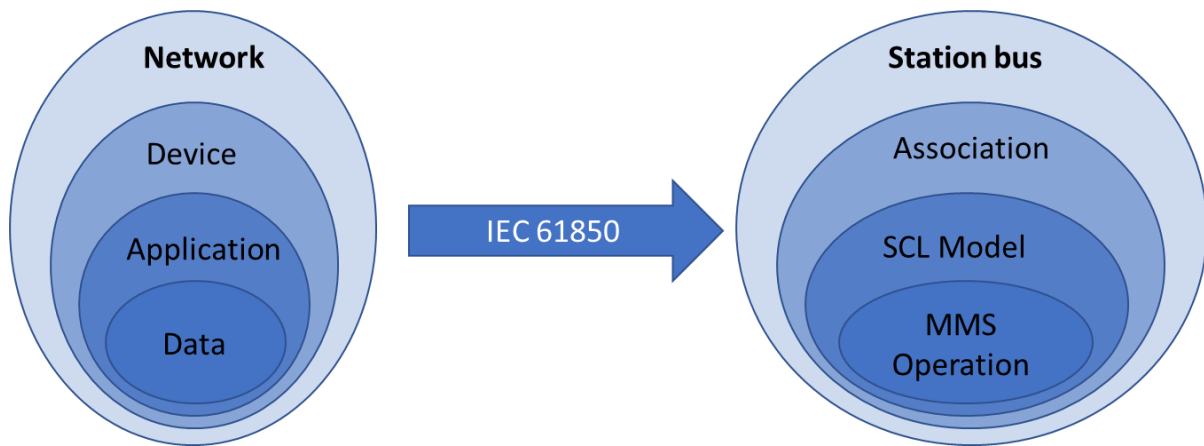


Figure 8. Defence in Depth for devices and for an IEC 61850 substation

Conventional IDS can easily detect attacks for spoofing IEDs, as well as normative MMS association or reports subscription attempts (association layer). By means of the SCL interpreter output, the IDS is fed by the substation data model and therefore can detect if the operations comply with it. The main advantage of the SCL interpreter module is that the IDS is customized to the substation to protect.

3.2.2.1.1 SCL rules extraction process

Input data: One SCL file or several CID files

Output data: Substation rules file

Process/daemon: sclCrawler

The sclCrawler is a standalone application which navigates through SCL files and extract useful information for allowed information, data flow and communications. The XML navigation is divided into 4 steps:

1. Communication extraction. The first step looks for any communication device connected to a network. It looks for all elements (IEDs) in each communication node and extracts its IP configuration. To do so, the <Communication.Subnetwork.ConnectedAP> elements are retrieved. The result of this process will serve the IDS to know the networks and the IPs in each network.
2. IED services extraction. The IEC 61850 services available for each IED is extracted from here (model navigation, dataset configurations, reports, GOOSEs and files). Notice that some services, although available in the SCL file, they are not recommendable its use in operation (e.g. get data object definitions). In such case, the logical nodes curtailment process should mark these services as alarms. This information is in the <IED.Services> elements.
3. Extract MMS (logical devices and logical nodes). In this step, the access to the logical nodes are retrieved for each IED. This information is the features, protections or functionalities that each IED provides, allocated in the <IED.AccessPoint.Server.LDevice.LN and LN0 nodes> elements. When CID files are provided, more nodes than finally used in substation could be identified that should be deleted in the logical nodes curtailment process.
4. Extract data objects and attributes. In MMS request, the attributes to read or write are associated to objects and accessed by its functional constraint. To obtain a list of allowed request, the previous <IED.AccessPoint.Server.LDevice.LN and LN0 nodes> elements are

mapped to <DataTypeTemplates.LNodeType> elements along with Data Object types (recursive elements) and Data Attributes. When a logical node is deleted, all its attributes should also be deleted.

The output is a single file (substation rules file), which is an XML document containing the following information:

- <ipaddresses> element, with a list of all IPs identified by its IED name.
- <services> element, with a list of IED names and their allowed services.
 - <reportSettingsService> element, a special service for reports
 - <gseSettingsService> element, a special service for reports
- <LNnodesObj> element with a list of read/write objects and attributes for MMS operations

Each element in the output file has been assigned a default severity for each operation. However, commands and associations have higher severity than request for information.

3.2.2.1.2 Priority/Severity assignation process

Input data: Substation rules file

Output data: Substation rules file (modified)

Process/daemon: guiCrawler

Although seven levels of severity have been defined for the substation rules (0 – no severity, 1 – trace, 2 – information, 3 – advice, 4 – high, 5 – severe, 6 – fatal), only 1-5 are used. The level 0 is like deleting the rule, that is, when detected at operation time, do not report anything in any case, therefore it can be deleted straightforward. The level 6 is reserved to operations that could damage the substation, mainly provoked by a coordinated attack to several points of the substation and even to the control centre.

The guiCrawler is a graphic interface to modify the default severity assigned automatically by the sclCrawler in a smart way, grouping logical nodes or functional constraints to modify complete sets in once. It also allows the user to deal some IEDs separately, that could be helpful to distinguish IEDs connected to different voltage levels.

3.2.2.1.3 Logical Nodes curtailment process

Input data: Substation rules file

Output data: Enhanced SBT rules file

Process/daemon: guiCrawler

When several CID files are provided the sclCrawler output collects the whole functionality of the IEDs, which is not only unnecessary in its deployment in the substation, but an attempt to access to an unused logical node is considered as an attack or a wrong configuration of the invoker. One option is preserving these nodes and mark them as 4/5 severity upon an attempt to access by means of the Priority/Severity assignation process.

The second option is reserved **if and only if** the IDS is able to alert when a MMS request tries to access a non-defined logical node in its configuration rules. In this case, the guiCrawler also allows deleting unused nodes.

3.2.2.2 Pluggable detection engine module

The SBT-Aware is designed to feed IDS with substation specific information. This means that the application can use any IDS for attacks detection, whose integration details are explained in the deployment (see 0). The IDS selected for the SDN-microSENSE is **Suricata** (Section 3.1).

In the SDN-microSENSE, sclCrawler will be used to generate rules. These rules are evaluated against the network traffic and an alert is sent when this traffic not fit the existing configuration in the SCL files. So, these detection rules are customized for that specific substation.

These alerts will be sent to XL SIEM by Report Launcher.

3.2.2.3 Pluggable report launcher module

The main goal of this library is to register appropriately the different alarms found by the detection engine. For alarm registration, a logging library has been specifically developed for the project. The library provides methods for managing the alarms generated by the detection engine, abstracting the caller of the intern logic of each event. Once the detection engine detects an action that shall be recorded for later analysis it calls the library to store it conveniently. The purpose of using this library is to decouple from the detection engine application's source code the details of event/alarm management and, specifically, where those alarms are stored. With this approach future event publishing capabilities and storing locations (Databases, MQTT sending, etc) could be easily integrated. Alarm information is stored into a string with a JSON format to be processed and analysed later by the appropriated tools. The JSON format has been selected for events because its usage is widespread among other detection solutions.

3.2.3 Deployment

The deployment of the AWT-Aware consist in the installation of the three modules and connecting the pluggable modules (detection engine and report launcher), which need some extra actions to integrate (plug) them.

3.2.3.1 SCL interpreter

This module is a multiplatform standalone application developed in Java, therefore its deployment consists only in the JRE/JDK installation and the tool configuration. This is done by the following steps:

1. Install JVM (Java Virtual Machine)
 - Go to <https://www.oracle.com> and navigate to Java resources
 - The application was developed with Java 8, so download the latest stable Java version compatible with Java 8 (currently, the latest version is Java 14 which can be used). When downloading, select the OS where the program will be run.
 - Once downloaded, click on the installable archive, and follow the steps to install the JVM. No extra features are needed; the default settings are enough for the application.
2. Copy the Java Archives sclCrawler.jar and guiCrawler.jar to a specific location (e.g. /home/sdn/sbtaware)
3. Run the program. Move to the selected location in step 2 and run the command line:
 - Command line: `java -jar sclCrawler.jar [-all] <rules> <scl_file>`

- where:
 - i. `-all` [Optional] if Data Objects and Data Attributes must be also retrieved. If missing, only up to Logical Nodes are retrieved.
 - ii. `<rules>` One output file containing the object and attributes for the provided SCL file
 - iii. `<scl_file>` The SCL file to parse.
- Examples:
 - i. `java -jar sclCrawler.jar -all rules.out L1.cid`
 - ii. `java -jar sclCrawler.jar rules.out substation.scd`
- By default, the format of the output data is written for Suricata. If other IDS were installed, the JVM property IDS should be changed for the selected one. Example of command line for Snort (notice that the `-D` option do not require the space for the key to modify):
 - i. `java -DIDS="Snort" -jar sclCrawler.jar rules.out substation.scd`
- 4. [Optional] Add extra information. If the cybersecurity staff wanted to adjust extra rules:
 - They can do it straightforward in the output rules file,
 - or they can use the graphical view for this purpose:
 - i. Run the command line `java -jar guiCrawler.jar`
 - ii. Open the rules file to modify/delete items

The SBT engineer must know that the substation will be monitored. This way, whenever the substation changes, or some IED is installed, replaced or removed, or some IED configuration is updated, may make the rules obsolete and the IDS will not work properly. In this case, the cybersecurity team must be advised that a change was made in the substation and the rules must be regenerated, just by running step 3 and optionally 4.

3.2.3.2 Report launcher

For setting up this reporter launcher library, it is as easy as executing *"make all"* and the library is built. The library includes Unit Testing, which is also compiled using *"make all"* and can be individually compiled using *"make test"*.

Once the library is compiled, it can be included in any C file as usual (*#include "log.h"*) and its methods can be called.

3.2.3.3 Tools integration

Whenever an event or alarm is detected, the message is formatted properly by the Report Launcher and sent to the XL-SIEM, as described in section 4.3.1 of deliverable D5.1 XL-SIEM System.

3.2.4 Output: connection to XL-SIEM, logs and taxonomy

The following tables details the information contained in the events to submit from this detector to the XL-SIEM.

Table 3. Description for the Generic Threat Discovery log

Log name	Generic Threat Discovery
Log description	This log record is reserved for communication anomalies detected by the detection engine

Important fields	Field type	Possible values	Field description
TSMMSG	UTC Time		Timestamp when the message was recorded
TSLAUNCH	UTC Time		Timestamp when the anomaly was detected as suspicious
SEVERITY	Integer	0..7	Higher value means higher severity
PAYLOAD	String		Original message or formatted message if the message is a known-pattern (e.g. ARP Spoofing)
IPFROM	String	IPv4 or IPv6	Source of the message
IPTO	String	IPv4 or IPv6	Message destination

Table 4 Description of the SBT Cybersecurity events log

Log name	SBT Cybersecurity events		
Log description	This log record gathers any message which should not be present according to the substation electric topology or its current state		
Important fields	Field type	Possible values	Field description
TSMMSG	UTC Time		Timestamp when the message was recorded
TSLAUNCH	UTC Time		Timestamp when the anomaly was detected as suspicious
SEVERITY	Integer	0..7	Higher value means higher severity
PAYLOAD	String		Original message (if desired)
PROTOCOL	String	MMS, GOOSE, REPORT	If the message that launched this event was a GOOSE, a MMS request/response or a report (rcb, urcb)
NODE	String		The LNode/constraint/dataset requested
IPFROM	String	IPv4, IPv6 or MAC	Source of the message (MAC for GOOSE)
IPTO	String	IPv4, IPv6 or MAC	Message destination (MAC for GOOSE)

3.3 SDN-IDPS: Nightwatch

Nightwatch is an Intrusion Detection and Classification Module (IDCM) for advanced and novel threats to EPES. As an IDCM, Nightwatch uses artificial intelligence technologies to determine the likelihood that an EPES has been compromised. It supports low-computational analysis and machine learning techniques for resource constrained devices common in EPES environments. Nightwatch is specifically developed to interface with and gather raw network data related SDN-controllers to elicit indicators of compromise. It is using information derived from the SDN-controller to determine whether the SDN components are under cyber-attack. Additionally, Nightwatch can determine the type of the attack and likelihood that an SDN component has been compromised. It can detect novel attacks and known attacks. For example, regarding high level attack categories, Nightwatch is able to detect DoS attacks against specific SDN components; malware compromise of controllers and or specific APIs; or malicious use of an SDN controller.

Nightwatch will be able to consume data from XL-SIEM using the XL-SIEM's RabbitMQ message broker. Nightwatch will use the RabbitMQ to read events from XL-SIEM agents as inputs for its intrusion detection analysis. Security-related events from XL-SIEM will enable Nightwatch to augment its intrusion detection process with additional information on the security posture of the system.

The resulting analysis of Nightwatch based on input from the SDN-controller and the XL-SIEM agents will be made available to the XL-SIEM for a consolidated analysis of the security of the EPES system.

3.3.1 Input data from the SDN controller

In SDN-microSENSE, Nightwatch is receiving inputs from two sources. The SDN-controllers (via controller API and network SPAN port) and the XL-SIEM. The interaction between Nightwatch and XL-SIEM is further described in D3.3 EPES Honeypots and D5.1 XL-SIEM System. The present deliverable is focussed on the interaction of Nightwatch with the SDN-controllers.

The communication between Nightwatch and the SDN-controller is made through the SDN-controller's RYU interface for collecting controller telemetry that provides context for network-based threat detection. The RYU Controller provides software components with application program interfaces (APIs) that make it easy for developers to create new network management and control applications. Nightwatch will make use of the RYU's APIs to gather network-related data that can be used for data analytics and where applicable aid in security assessment via correlation with raw network data collected via the network segment SPAN port. Nightwatch will gather network-related information using Representational State Transfer (REST) based queries from the RYU's northbound interface. The network information will include the network topology of the SDN switches, available network ports, and statistical information related to the available network ports. The network-based information will enable Nightwatch to elicit the nature of threats targeting SDN components, such as malware, service, or resource disruption. Nightwatch's network SPAN interface collections effectively give the module full visibility of the network segment in which it is situated and provides the module with the ability to filter specific communication related to SDN controllers in a dynamic manner with needed prior configuration. Nightwatch specifically applies connection-orientated analysis of raw network data to provide rich and contextual network telemetry data to its detection engine.

3.3.2 Internals of the tool

The architectural components of Nightwatch are shown in Figure 9. The main component of Nightwatch is the SDN Threat Detection Engine. The Network Probe contains a network sensor for collecting and forwarding network data telemetry from the SDN-Controller to the SDN Threat Detection engine. The Datastream Service of the Threat Detection Engine receives input from the Network probes. The function of the Datastream Service is used to structure the information received by the Network probes into a format that can be consumed by the Anomaly Sensor Service.

The Anomaly Sensor Service is divided into two components, the Threat models, and the Heuristic Analysers. The Threat models use a range of ML algorithms specifically developed and trained to detect attack vector that can disrupt, degrade or deny SDN controller functionality and control. The Threat models are dynamically trained in a continuous online manner with data sent and received by SDN controller(s) and its connectivity peers, against a set of principal detection use cases by which the models feature context are designed. The Heuristic Analyzers validate Threat model output to determine the context of anomaly detections, and correlate information across Threat models with additional analytics processes to determine the likelihood and type of network-based attack. The

Heuristic Analyser are developed to detect novel threats or new variants of known threats. They use several techniques such as decomposing specific network patterns and evaluate it based on the system's functionality. If a certain percentage of the network pattern matches information from the Threat models, the behavior is marked as an anomaly.

After the security assessment is completed, the SDN Threat detection Engine outputs a threat summary, which is consumed by the XL-SIEM. The threat summary contains all the anomalies detected by the Anomaly Sensor Service that can result in the compromise of SDN components.

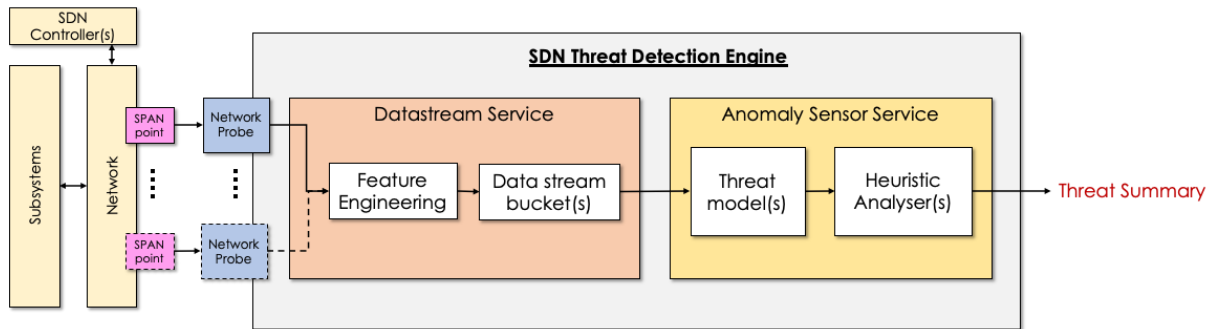


Figure 9. Architecture of Nightwatch in SDN-microSENSE

3.3.3 Deployment

Nightwatch will be made available as a container-based application that will be deployable in a cloud-native manner. Cloud-native applications take full advantage of the cloud service model. They provide better orchestration and management of resources in dynamic environments than traditional deployment practises.

Regarding data collection, Nightwatch module requires network connectivity to a SPAN or passive monitoring interface tap in which consume to consume SDN network telemetry. It will generate anomaly output events/logs that are then forwarded to remote RESTful or streaming APIs. Nightwatch can also receive data via its streaming API interface using a publisher/subscriber model (e.g., KAFKA, MQTT).

3.3.4 Output: connection to XL-SIEM, logs and taxonomy

Nightwatch produces one type of log related to threat detection, which contains various possible attack classifications and meta-data.

Table 5. Description for the threat discovery log

Log name	Threat discovery		
Log description	A log record containing the records of the anomaly detection		
Important fields	Field type	Possible values	Field description
attack_vector	string	OpenFlow Packet-In Flood	The vector used to execute the attack
attack_type	string	Denial of Service	The type of attack
timestamp	string	1600105625	Epoch for the time of the anomaly alert

window_start	string	1600105623	Epoch for the start of the detection window
window_stop	string	1600105624	Epoch for the end of the detection window

4 Unit Testing and validation

4.1 Modbus/TCP Unit Tests – Suricata

This subsection aims to test the efficacy of the Suricata specification rules presented in subsection 2.3.4) against Modbus/TCP cyberattacks. In particular, custom Suricata specification rules were constructed, thereby determining the normal Modbus/TCP behaviour of a use case and detecting potential malicious/anomalous Modbus/TCP commands. Based on subsection 2.3.2, the following unit tests verify that Suricata can detect a) modbus/function/writeSingleCoils, b) modbus/function/readInputRegister, c) modbus/function/writeSingleRegister, d) modbus/function/readDiscreteInput and e) modbus/function/readCoils Modbus/TCP related cyberattacks. The aforementioned cyberattacks described in subsection 2.3.2 will be addressed by the machine and deep learning solutions of Task 5.3/D5.3.

Test Case ID	Modbus_Suricata_01	Component	Suricata (Sensor of XL-SIEM)
Description	This unit test intends to detect potential malicious or anomalous Modbus/TCP commands, utilising custom Suricata Modbus/TCP specification rules. These Modbus/TCP specification rules define the normal Modbus/TCP behaviour of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4), where only the Function Code 03 (0x03 - Read Holding Registers) is allowed. First, the configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to recognise normally the Modbus/TCP keywords. Next, a specific specification rule, which defines the aforementioned Modbus/TCP normal behaviour is defined and stored in the configuration file (/etc/Suricata/rules/suricata.rules), which includes all specification rules of Suricata. Then, the cyberattack modbus/function/readCoils presented in subsection 2.3.2 is emulated, capturing in parallel the Modbus/TCP network traffic in a pcap file. Finally, the pcap file is parsed suitably by Suricata, detecting successfully the relevant attack.		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	High
Prepared by	UOWM	Tested by	UOWM
Pre-condition(s)	-		
Test steps			
1	The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to recognise normally the Modbus/TCP keywords. In particular, in the /etc/suricata/suricata.yaml file, the lines related to the Modbus keywords were uncommented, as showed in the following figure.		

```

927 modbus:
928   # How many unreplied Modbus requests are considered a flood.
929   # If the limit is reached, app-layer-event:modbus.flooded; will match.
930   #request-flood: 500
931
932   enabled: yes
933   detection-ports:
934     dp: 502
935   # According to MODBUS Messaging on TCP/IP Implementation Guide V1.0b, it
936   # is recommended to keep the TCP connection opened with a remote device
937   # and not to open and close it for each MODBUS/TCP transaction. In that
938   # case, it is important to set the depth of the stream reassembling as
939   # unlimited (stream.reassembly.depth: 0)
940
941   # Stream reassembly size for modbus. By default track it completely.
942   stream-depth: 0

```

Figure 10. Activation of the Modbus/TCP keywords testcase Modbus_Suricata_01

- 2 The following Suricata specification rule was used in order to detect any Modbus/TCP command, which is not relevant to the Modbus/TCP network traffic characteristics of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4). The specific rule defines that only Modbus/TCP Function Code 03 (0x03 - Read Holding Registers) is allowed.

```

alert modbus any any -> any 502 (modbus: function !3; msg:"Modbus/TCP Alert - Not Allowed
Moudbus/TCP Function Code"; sid: 2;)

```

- 3 Then, the cyberattack modbus/function/readCoils is performed in an emulated environment, which follows the Modbus/TCP network traffic characteristics of the Alkyonis PV Power Station. For this purpose, the UOWM Smold was utilised [Radoglou-Grammatikis20+1]. In parallel, the network traffic related to the attack is captured and stored via Wireshark in a pcap file named malicious_pcap.pcap.

- 4 The pcap (malicious_pcap.pcap) is parsed by Suricata offline, utilising the following command.
- ```

sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap

```

#### Input data

A pcap file (malicious\_pcap.pcap) related to the modbus/function/readCoils attack. The following figure shows a sample of this pcap file. In particular, this pcap file (malicious\_pcap.pcap) includes 20 Modbus/TCP packets related to the modbus/function/readCoils attack and 100 Modbus/TCP packets related to Modbus/TCP Function Code 03 (0x03 - Read Holding Registers).

| No. | Time       | Source | Destination | Protocol  | Length | Info                                            |
|-----|------------|--------|-------------|-----------|--------|-------------------------------------------------|
| 28  | 171.143459 | 6      | 17          | Modbus... | 78     | Query: Trans: 2; Unit: 1, Func: 1;              |
| 29  | 171.147156 | 17     | 6           | TCP       | 66     | 502 -> 59352 [ACK] Seq=1 Ack=13 Win=29056 Len=  |
| 30  | 171.147202 | 6      | 54          | Modbus... | 78     | Query: Trans: 2; Unit: 1, Func: 1;              |
| 31  | 171.147377 | 6      | 8           | TCP       | 74     | 35854 -> 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1  |
| 32  | 171.148273 | 17     | 6           | Modbus... | 76     | Response: Trans: 2; Unit: 1, Func: 1;           |
| 33  | 171.148278 | 6      | 17          | TCP       | 66     | 59352 -> 502 [ACK] Seq=13 Ack=11 Win=64256 Len= |
| 34  | 171.148294 | 54     | 6           | TCP       | 66     | 502 -> 43250 [ACK] Seq=1 Ack=13 Win=65152 Len=  |
| 35  | 171.149677 | 54     | 6           | Modbus... | 76     | Response: Trans: 2; Unit: 1, Func: 1;           |
| 36  | 171.149682 | 6      | 54          | TCP       | 66     | 43250 -> 502 [ACK] Seq=13 Ack=11 Win=64256 Len= |
| 37  | 171.149698 | 8      | 6           | TCP       | 74     | 502 -> 35854 [SYN, ACK] Seq=0 Ack=1 Win=28960   |
| 38  | 171.149710 | 6      | 8           | TCP       | 66     | 35854 -> 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0  |
| 39  | 171.163219 | 6      | 15          | TCP       | 74     | 36772 -> 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1  |
| 40  | 171.164444 | 6      | 9           | TCP       | 74     | 41058 -> 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1  |

Figure 11. Pcap for modbus/function/readCoils attack for test case Modbus\_Suricata\_01

#### Result

The modbus/function/readCoils attack was detected successfully by Suricata. The detection results are stored in the eve.json file. An example of the corresponding alerts generated by Suricata is provided below.

```

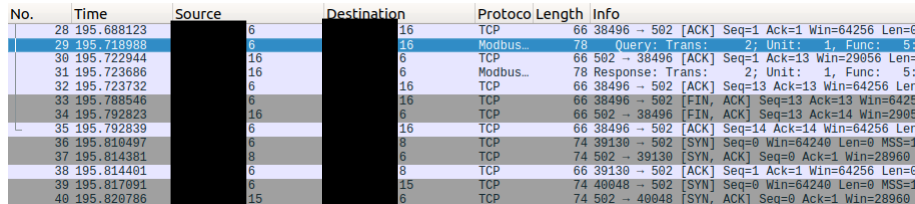
{"timestamp": "2020-03-
25T13:12:22.707663+0200", "flow_id": "1409353732485049", "pcap_cnt": "6775", "event_type":

```

|                  | <div>"alert","src_ip":"YY.YY.YY.YY","src_port":yy,"dest_ip":"XX.XX.XX.XX","dest_port":xx,"proto" : "TCP","tx_id":0,"alert":{"action":"`allowed","gid":1,"signature_id":2,"rev":0,"signature": "Modbus\\TCP Alert - Not Allowed Moudbus\\TCP Function Code","category":"","severity":3},"app_proto":"modbus","flow":{"pkts_toserver":4,"pkts_t oclient":3,"bytes_toserver":284,"bytes_toclient":216,"start":"2020-03- 25T13:12:22.683961+0200"}}}</div> <p>Before analysing the detection results, some necessary terms need to be defined. First, True Positives (TP) denotes the number of the correct classifications that detect the cyberattacks as intrusions. True Negatives (TN) implies the number of the correct classifications that recognise the normal network packets as normal. On the other side, False Negative (FN) denotes the number of incorrect classifications that detect the malicious behaviours as normal. Finally, False Positive (FP) indicates the number of mistaken classifications where the normal behaviours are recognised as malicious. Based on these terms, the following metrics are defined.</p> $Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{20 + 100}{20 + 100 + 0 + 0} = 1$ $True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{20}{20 + 0} = 1$ $True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{120}{120 + 0} = 1$ $False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 120} = 0$ $F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 20}{2 \times 20 + 0 + 0} = 1$ <p>Therefore, based on these metrics, the following evaluation results are presented</p> <table><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></table> <p>Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of unknown attacks or without the appropriate specification rules, then the detection results can present FP and FN.</p> | Accuracy | TPR | TNR | FPR | F1 | 1 | 1 | 1 | 0 | 0 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----|-----|-----|----|---|---|---|---|---|
| Accuracy         | TPR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | TNR      | FPR | F1  |     |    |   |   |   |   |   |
| 1                | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 1        | 0   | 0   |     |    |   |   |   |   |   |
| Test Case Result | Achieved                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |          |     |     |     |    |   |   |   |   |   |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                 |                  |                              |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------------------------|
| <b>Test Case ID</b> | Modbus_Suricata_02                                                                                                                                                                                                                                                                                                                                                                              | <b>Component</b> | Suricata (Sensor of XL-SIEM) |
| <b>Description</b>  | This unit test aims to detect a modbus/function/writeSingleCoils presented in subsection 2.3.2. To this end, as in the previous unit test, Suricata was used determining the respective Modbus/TCP specification rules based on the Modbus/TCP network traffic characteristics of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4), where only the Function Code 03 (0x03 - |                  |                              |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
|                  | <p>Read Holding Registers) is permitted. Although the same Suricata specification rule was used in the previous unit test, this unit test intends to verify the applicability of Suricata to detect modbus/function/writeSingleCoils cyberattacks.</p> <p>First, the configuration file of Suricata (/etc/suricata/suricata.yaml) was edited to activate the Modbus/TCP keywords. Then, a particular specification rule, which determines the Modbus/TCP normal behavioural characteristics of the Alkyonis PV Power Station is defined and stored in the configuration file (/etc/Suricata/rules/suricata.rules). Next, the cyberattack modbus/function/writeSingleCoils is emulated, storing in parallel the Modbus/TCP network traffic in a pcap file. Finally, the pcap file is processed appropriately by Suricata, recognising successfully the relevant attack.</p>                                                                                                                                                                                                                                                                                     |           |      |
| Spec ID          | SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Priority  | High |
| Prepared by      | UOWM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Tested by | UOWM |
| Pre-condition(s) | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |      |
| Test steps       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |      |
| 1                | <p>The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to activate the Modbus/TCP keywords. In particular, in the /etc/suricata/suricata.yaml file, the rows relevant to the Modbus/TCP keywords were activated, as depicted in the following figure.</p> <div><pre>927 modbus: 928     # How many unreplied Modbus requests are considered a flood. 929     # If the limit is reached, app-layer-event:modbus.flooded; will match. 930     #request-flood: 500 931 932     enabled: yes 933     detection-ports: 934       dp: 502 935     # According to MODBUS Messaging on TCP/IP Implementation Guide V1.0b, it 936     # is recommended to keep the TCP connection opened with a remote device 937     # and not to open and close it for each MODBUS/TCP transaction. In that 938     # case, it is important to set the depth of the stream reassembling as 939     # unlimited (stream.reassembly.depth: 0) 940 941     # Stream reassembly size for modbus. By default track it completely. 942     stream-depth: 0</pre></div> <p>Figure 12. Activation of the Modbus/TCP keywords for test case Modbus_Suricata_02</p> |           |      |
| 2                | <p>As in the previous case, the below Suricata specification rules was utilised in order to recognise any Modbus/TCP command, which is not relevant to the Modbus/TCP network traffic characteristics of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4). The particular rule determines that only Modbus/TCP Function Code 03 (0x03 - Read Holding Registers) is allowed.</p> <pre>alert modbus any any -&gt; any 502 (modbus: function !3; msg:"Modbus/TCP Alert - Not Allowed Moudbus/TCP Function Code"; sid: 2;)</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |           |      |
| 3                | <p>Then, the cyberattack modbus/function/readCoils is executed in an emulated environment, which follows the Modbus/TCP network traffic characteristics of the Alkyonis PV Power Station. For this purpose, the UOWM Smod was utilised [Radoglou-Grammatikis20+1]. In parallel, the</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |      |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | network traffic relevant to the attack is captured through Wireshark in a pcap file named malicious_pcap.pcap.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 4                 | The pcap (malicious_pcap.pcap) is analysed by Suricata offline, using the following command.<br><code>sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Input data</b> | <p>A pcap file (malicious_pcap.pcap) related to the modbus/function/writeSingleCoils attack. The following figure depicts a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes 30 Modbus/TCP packets related to the modbus/function/writeSingleCoils attack and 150 Modbus/TCP packets related to Modbus/TCP Function Code 03 (0x03 - Read Holding Registers).</p>  <p>Figure 13. Pcap for modbus/function/writeSingleCoils attack for test case Modbus_Suricata_02</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Result</b>     | <p>The modbus/function/writeSingleCoils attack was recognised successfully by Suricata. The detection results are stored in the eve.json file. An example of the corresponding alerts generated by Suricata is provided below.</p> <pre>{   "timestamp": "2020-03-25T15:14:15.615226+0200",   "flow_id": "821675984101679",   "pcap_cnt": "1042",   "event_type": "alert",   "src_ip": "XX.XX.XX.XX",   "src_port": "xx",   "dest_ip": "YY.YY.YY.YY",   "dest_port": "yy",   "proto": "TCP",   "tx_id": "0",   "alert": {     "action": "allowed",     "gid": "1",     "signature_id": "2",     "rev": "0",     "signature": "Modbus/TCP Alert - Not Allowed Moudbus/TCP Function Code",     "category": "",     "severity": "3",     "app_proto": "modbus",     "flow": {       "pkts_toserver": "4",       "pkts_toclient": "3",       "bytes_toserver": "284",       "bytes_toclient": "218",       "start": "2020-03-25T15:14:15.598319+0200"     }   } }</pre> <p>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</p> $Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{30 + 150}{30 + 150 + 0 + 0} = 1$ $True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{30}{30 + 0} = 1$ $True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{150}{150 + 0} = 1$ $False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 150} = 0$ $F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 30}{2 \times 30 + 0 + 0} = 1$ <p>Therefore, based on these metrics, the following evaluation results are presented</p> |



|                         | Accuracy                                                                                                                                                                                                                                                                                                                                         | TPR | TNR | FPR | F1 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|-----|----|
|                         | 1                                                                                                                                                                                                                                                                                                                                                | 1   | 1   | 0   | 0  |
|                         | <p>Since the appropriate specification rules were defined properly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection outcome is accurate completely. Nevertheless, in the case of zero-day attacks or without the sufficient rules, then the detection results can present FP and FN.</p> |     |     |     |    |
| <b>Test Case Result</b> | Achieved                                                                                                                                                                                                                                                                                                                                         |     |     |     |    |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |           |                              |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------|
| Test Case ID     | Modbus_Suricata_03                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Component | Suricata (Sensor of XL-SIEM) |
| Description      | <p>This unit test aims at detecting a modbus/function/readInputRegister (presented in subsection 2.3.2). Suricata was utilised, defining the corresponding Modbus/TCP specification rules according to the normal Modbus/TCP network traffic behaviour of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4), where only the Function Code 03 (0x03 - Read Holding Registers) is allowed. Although the same Suricata specification rule was applied in the previous unit tests, this unit test intends to check the applicability and validity of Suricata to recognise modbus/function/readInputRegister.</p> <p>First, the configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to activate the Modbus/TCP keywords. Following, a specific specification rule, which determines the Modbus/TCP normal behavioural characteristics of the Alkyonis PV Power Station is defined in the configuration file (/etc/Suricata/rules/suricata.rules). Subsequently, the cyberattack modbus/function/readInputRegister is emulated, storing the Modbus/TCP network traffic in a pcap file. Finally, the pcap file is parsed by Suricata, recognising the aforementioned attack.</p> |           |                              |
| Spec ID          | SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Priority  | High                         |
| Prepared by      | UOWM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Tested by | UOWM                         |
| Pre-condition(s) | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |                              |
| Test steps       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |           |                              |
| 1                | The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to uncomment the Modbus/TCP keywords. Specifically, in the /etc/suricata/suricata.yaml file, the lines related to the Modbus/TCP keywords were uncommented, as illustrated in the following figure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |                              |

```

927 modbus:
928 # How many unreplied Modbus requests are considered a flood.
929 # If the limit is reached, app-layer-event:modbus.flooded; will match.
930 #request-flood: 500
931
932 enabled: yes
933 detection-ports:
934 | dp: 502
935 # According to MODBUS Messaging on TCP/IP Implementation Guide V1.0b, it
936 # is recommended to keep the TCP connection opened with a remote device
937 # and not to open and close it for each MODBUS/TCP transaction. In that
938 # case, it is important to set the depth of the stream reassembling as
939 # unlimited (stream.reassembly.depth: 0)
940
941 # Stream reassembly size for modbus. By default track it completely.
942 stream-depth: 0

```

Figure 14. Activation of Modbus/TCP keywords for test case Modbus\_Suricata\_03

- 2 As in the previous case, the following Suricata specification rule was used to detect Modbus/TCP commands, which is not relevant to the Modbus/TCP network traffic characteristics of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4). The particular rule determines that only Modbus/TCP Function Code 03 (0x03 - Read Holding Registers) is allowed.  
alert modbus any any -> any 502 (modbus: function !3; msg:"Modbus/TCP Alert - Not Allowed Moudbus/TCP Function Code"; sid: 2;)

- 3 Then, the cyberattack modbus/function/readInputRegister is performed in an emulated environment, which adopts the Modbus/TCP network traffic characteristics of the Alkyonis PV Power Station. The UOWM Smod was utilised [Radoglou-Grammatikis20+1] for the execution of the cyberattack. In parallel, the network traffic related to the attack is captured through Wireshark in a pcap file called malicious\_pcap.pcap.

- 4 The pcap (malicious\_pcap.pcap) is processed by Suricata offline, using the following command.  
sudo suricata -c /etc/suricata/suricata.yaml -r malicious\_pcap.pcap

**Input data** A pcap file (malicious\_pcap.pcap) related to the modbus/function/readInputRegister attack. The following figure depicts a sample of this pcap file. In particular, this pcap file (malicious\_pcap.pcap) includes 20 Modbus/TCP packets related to the modbus/function/readInputRegister attack and 100 Modbus/TCP packets related to Modbus/TCP Function Code 03 (0x03 - Read Holding Registers).

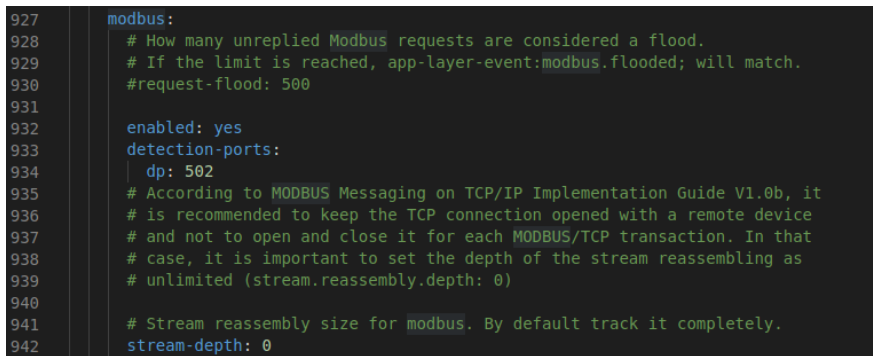
| No. | Time      | Source | Destination | Protocol  | Length | Info                                                 |
|-----|-----------|--------|-------------|-----------|--------|------------------------------------------------------|
| 16  | 73.173458 | 3      | 6           | TCP       | 74     | 502 → 55940 [SYN, ACK] Seq=0 Ack=1 Win=28960         |
| 17  | 73.173482 | 6      | 3           | TCP       | 66     | 55940 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0        |
| 18  | 73.182526 | 6      | 3           | Modbus... | 78     | Query: Trans: 2; Unit: 1, Func: 4;                   |
| 19  | 73.182848 | 3      | 6           | TCP       | 66     | 502 → 55940 [ACK] Seq=1 Ack=13 Win=29056 Len=0       |
| 20  | 73.183647 | 3      | 6           | Modbus... | 77     | Response: Trans: 2; Unit: 1, Func: 4;                |
| 21  | 73.183656 | 6      | 3           | TCP       | 66     | 55940 → 502 [ACK] Seq=13 Ack=12 Win=64256 Len=0      |
| 22  | 73.253298 | 6      | 3           | TCP       | 66     | 55940 → 502 [FIN, ACK] Seq=13 Ack=12 Win=64256 Len=0 |
| 23  | 73.255141 | 3      | 6           | TCP       | 66     | 502 → 55940 [FIN, ACK] Seq=12 Ack=14 Win=29056 Len=0 |
| 24  | 73.255177 | 6      | 3           | TCP       | 66     | 55940 → 502 [ACK] Seq=14 Ack=13 Win=64256 Len=0      |
| 25  | 73.255622 | 6      | 15          | TCP       | 74     | 53738 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1        |
| 26  | 73.259455 | 15     | 6           | TCP       | 74     | 502 → 53738 [SYN, ACK] Seq=0 Ack=1 Win=28960         |
| 27  | 73.259519 | 6      | 15          | TCP       | 66     | 53738 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0        |
| 28  | 73.276467 | 6      | 15          | Modbus    | 78     | Query: Trans: 2; Unit: 1, Func: 4;                   |

Figure 15. Pcap for modbus/function/readInputRegister attack for test case Modbus\_Suricata\_03

**Result** The modbus/function/readInputRegister attack was detected successfully by Suricata. The detection results are stored in the eve.json file. An example of the corresponding alerts produced by Suricata is presented below.

|                  | <p>{<br/>"timestamp":"2020-03-26T17:10:54.018282+0200",<br/>"flow_id":1497422194612871,<br/>"pcap_cnt":1023,<br/>"event_type":<br/>"alert",<br/>"src_ip":"XX.XX.XX.XX",<br/>"src_port":xx,<br/>"dest_ip":"YY.YY.YY.YY",<br/>"dest_port":yy,<br/>"proto":<br/>"TCP",<br/>"tx_id":0,<br/>"alert":{"action":"allowed",<br/>"gid":1,<br/>"signature_id":2,<br/>"rev":0,<br/>"signature":"M odbus\TCP Alert - Not Allowed Moudbus\TCP Function Code",<br/>"category":"","severity":3},<br/>"app_proto":"modbus",<br/>"flow":{"pkts_toserver":4,<br/>"pkts_t oclient":3,<br/>"bytes_toserver":284,<br/>"bytes_toclient":217,<br/>"start":"2020-03-26T17:10:53.989831+0200"}}}</p> <p>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</p> $Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{20 + 100}{20 + 100 + 0 + 0} = 1$ $True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{20}{20 + 0} = 1$ $True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{120}{120 + 0} = 1$ $False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 120} = 0$ $F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 20}{2 \times 20 + 0 + 0} = 1$ <p>Therefore, based on these metrics, the following evaluation results are presented</p> <table><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></table> <p>Given the appropriate specification rules were determined properly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks or without the suitable specification rules, then the detection results could present FP and FN.</p> | Accuracy | TPR | TNR | FPR | F1 | 1 | 1 | 1 | 0 | 0 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----|-----|-----|----|---|---|---|---|---|
| Accuracy         | TPR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | TNR      | FPR | F1  |     |    |   |   |   |   |   |
| 1                | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 1        | 0   | 0   |     |    |   |   |   |   |   |
| Test Case Result | Achieved                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |          |     |     |     |    |   |   |   |   |   |

| Test Case ID       | Modbus_Suricata_04                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Component | Suricata (Sensor of XL-SIEM) |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------|
| <b>Description</b> | This unit test intends to detect a modbus/function/writeSingleRegister (presented in subsection 2.3.2). Suricata is used, determining the respective Modbus/TCP specification rules based on the normal Modbus/TCP network traffic behavioural characteristics of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4), where only the Function Code 03 (0x03 - Read Holding Registers) is permitted. Although the same Suricata specification rule was used in the previous unit tests, this unit test intends to check the applicability and validity of Suricata to recognise modbus/function/writeSingleRegister. |           |                              |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
|                  | The configuration file of Suricata (/etc/suricata/suricata.yaml) was edited to uncomment the Modbus/TCP keywords (commented by default). Following, a particular specification rule, which defines the Modbus/TCP normal behavioural characteristics of the Alkyonis PV Power Station is determined in the configuration file (/etc/Suricata/rules/suricata.rules). Subsequently, the cyberattack modbus/function/writeSingleRegister is performed, capturing the Modbus/TCP network traffic in a pcap file. Finally, the pcap file is processed by Suricata, detecting the aforementioned attack. |           |      |
| Spec ID          | SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Priority  | High |
| Prepared by      | UOWM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Tested by | UOWM |
| Pre-condition(s) | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |           |      |
| Test steps       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |
| 1                | <p>The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to uncomment the Modbus/TCP keywords. Specifically, in the /etc/suricata/suricata.yaml file, the lines related to the Modbus/TCP keywords were uncommented, as illustrated in the following figure.</p>  <p>Figure 16. Activation of Modbus/TCP keywords for test case Modbus_Suricata_04</p>                                                                                                                                |           |      |
| 2                | <p>As in the previous unit test, the below Suricata specification rule was applied to detect Modbus/TCP commands that are not related to the Modbus/TCP network traffic of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4). The specific rule defines that only Modbus/TCP Function Code 03 (0x03 - Read Holding Registers) is allowed.</p> <pre>alert modbus any any -&gt; any 502 (modbus: function !3; msg:"Modbus/TCP Alert - Not Allowed Moudbus/TCP Function Code"; sid: 2;)</pre>                                                                                      |           |      |
| 3                | <p>Next, the cyberattack modbus/function/writeSingleRegister is emulated, adopting the Modbus/TCP network traffic of the Alkyonis PV Power Station. The UOWM Smod was used [Radoglou-Grammatikis20+1] for the execution of the cyberattack. Simultaneously, the network traffic related to the attack is captured through Wireshark in a pcap file called malicious_pcap.pcap.</p>                                                                                                                                                                                                                 |           |      |
| 4                | <p>The pcap (malicious_pcap.pcap) is parsed by Suricata offline, utilising the following command.</p> <pre>sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap</pre>                                                                                                                                                                                                                                                                                                                                                                                                               |           |      |

| Input data | <p>A pcap file (malicious_pcap.pcap) related to the modbus/function/writeSingleRegister attack. The following figure depicts a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes 30 Modbus/TCP packets related to the modbus/function/writeSingleRegister attack and 150 Modbus/TCP packets related to Modbus/TCP Function Code 03 (0x03 - Read Holding Registers).</p> <table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>70</td><td>163.438576</td><td>6</td><td>54</td><td>TCP</td><td>66</td><td>49834 → 502 [ACK] Seq=14 Ack=14 Win=64256 Len=0</td></tr><tr><td>71</td><td>163.440239</td><td>6</td><td>9</td><td>Modbus...</td><td>78</td><td>Query: Trans: 2; Unit: 1, Func: 6;</td></tr><tr><td>72</td><td>163.441990</td><td>9</td><td>6</td><td>TCP</td><td>66</td><td>502 → 47640 [ACK] Seq=1 Ack=13 Win=65152 Len=0</td></tr><tr><td>73</td><td>163.442093</td><td>9</td><td>6</td><td>Modbus...</td><td>78</td><td>Response: Trans: 2; Unit: 1, Func: 6;</td></tr><tr><td>74</td><td>163.442810</td><td>6</td><td>9</td><td>TCP</td><td>66</td><td>47640 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0</td></tr><tr><td>75</td><td>163.448454</td><td>6</td><td>15</td><td>TCP</td><td>74</td><td>43358 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1</td></tr><tr><td>76</td><td>163.452381</td><td>15</td><td>6</td><td>TCP</td><td>74</td><td>502 → 43358 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0</td></tr><tr><td>77</td><td>163.452436</td><td>6</td><td>15</td><td>TCP</td><td>66</td><td>43358 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0</td></tr><tr><td>78</td><td>163.455864</td><td>6</td><td>15</td><td>Modbus...</td><td>78</td><td>Query: Trans: 2; Unit: 1, Func: 6;</td></tr><tr><td>79</td><td>163.459051</td><td>6</td><td>6</td><td>TCP</td><td>66</td><td>502 → 43358 [ACK] Seq=1 Ack=13 Win=29056 Len=0</td></tr><tr><td>80</td><td>163.459064</td><td>15</td><td>6</td><td>Modbus...</td><td>78</td><td>Response: Trans: 2; Unit: 1, Func: 6;</td></tr><tr><td>81</td><td>163.459071</td><td>6</td><td>15</td><td>TCP</td><td>66</td><td>43358 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0</td></tr><tr><td>82</td><td>163.460865</td><td>6</td><td>3</td><td>TCP</td><td>74</td><td>46998 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1</td></tr></tbody></table> | No.      | Time        | Source    | Destination | Protocol                                           | Length | Info | 70 | 163.438576 | 6 | 54 | TCP | 66 | 49834 → 502 [ACK] Seq=14 Ack=14 Win=64256 Len=0 | 71 | 163.440239 | 6 | 9 | Modbus... | 78 | Query: Trans: 2; Unit: 1, Func: 6; | 72 | 163.441990 | 9 | 6 | TCP | 66 | 502 → 47640 [ACK] Seq=1 Ack=13 Win=65152 Len=0 | 73 | 163.442093 | 9 | 6 | Modbus... | 78 | Response: Trans: 2; Unit: 1, Func: 6; | 74 | 163.442810 | 6 | 9 | TCP | 66 | 47640 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0 | 75 | 163.448454 | 6 | 15 | TCP | 74 | 43358 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1 | 76 | 163.452381 | 15 | 6 | TCP | 74 | 502 → 43358 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 | 77 | 163.452436 | 6 | 15 | TCP | 66 | 43358 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0 | 78 | 163.455864 | 6 | 15 | Modbus... | 78 | Query: Trans: 2; Unit: 1, Func: 6; | 79 | 163.459051 | 6 | 6 | TCP | 66 | 502 → 43358 [ACK] Seq=1 Ack=13 Win=29056 Len=0 | 80 | 163.459064 | 15 | 6 | Modbus... | 78 | Response: Trans: 2; Unit: 1, Func: 6; | 81 | 163.459071 | 6 | 15 | TCP | 66 | 43358 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0 | 82 | 163.460865 | 6 | 3 | TCP | 74 | 46998 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1 |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------------|-----------|-------------|----------------------------------------------------|--------|------|----|------------|---|----|-----|----|-------------------------------------------------|----|------------|---|---|-----------|----|------------------------------------|----|------------|---|---|-----|----|------------------------------------------------|----|------------|---|---|-----------|----|---------------------------------------|----|------------|---|---|-----|----|-------------------------------------------------|----|------------|---|----|-----|----|-----------------------------------------------|----|------------|----|---|-----|----|----------------------------------------------------|----|------------|---|----|-----|----|-----------------------------------------------|----|------------|---|----|-----------|----|------------------------------------|----|------------|---|---|-----|----|------------------------------------------------|----|------------|----|---|-----------|----|---------------------------------------|----|------------|---|----|-----|----|-------------------------------------------------|----|------------|---|---|-----|----|-----------------------------------------------|
| No.        | Time                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Source   | Destination | Protocol  | Length      | Info                                               |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 70         | 163.438576                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 54          | TCP       | 66          | 49834 → 502 [ACK] Seq=14 Ack=14 Win=64256 Len=0    |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 71         | 163.440239                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 9           | Modbus... | 78          | Query: Trans: 2; Unit: 1, Func: 6;                 |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 72         | 163.441990                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 9        | 6           | TCP       | 66          | 502 → 47640 [ACK] Seq=1 Ack=13 Win=65152 Len=0     |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 73         | 163.442093                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 9        | 6           | Modbus... | 78          | Response: Trans: 2; Unit: 1, Func: 6;              |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 74         | 163.442810                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 9           | TCP       | 66          | 47640 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0    |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 75         | 163.448454                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 15          | TCP       | 74          | 43358 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1      |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 76         | 163.452381                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 15       | 6           | TCP       | 74          | 502 → 43358 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 77         | 163.452436                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 15          | TCP       | 66          | 43358 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0      |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 78         | 163.455864                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 15          | Modbus... | 78          | Query: Trans: 2; Unit: 1, Func: 6;                 |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 79         | 163.459051                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 6           | TCP       | 66          | 502 → 43358 [ACK] Seq=1 Ack=13 Win=29056 Len=0     |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 80         | 163.459064                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 15       | 6           | Modbus... | 78          | Response: Trans: 2; Unit: 1, Func: 6;              |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 81         | 163.459071                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 15          | TCP       | 66          | 43358 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0    |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 82         | 163.460865                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 6        | 3           | TCP       | 74          | 46998 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1      |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
|            | <p>Figure 17. Pcap for modbus/function/writeSingleRegister attack for Modbus_Suricata_04</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |             |           |             |                                                    |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| Result     | <p>The modbus/function/writeSingleRegister attack was recognised by Suricata. The detection results are stored in the eve.json file. An example of the corresponding alerts generated by Suricata is presented below.</p> <pre>{"timestamp":"2020-03-25T18:02:10.710063+0200","flow_id":"967791431795084","pcap_cnt":1388,"event_type":"alert","src_ip":"XX.XX.XX.XX","src_port":xx,"dest_ip":"YY.YY.YY.YY","dest_port":yy,"protocol":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2,"rev":0,"signature":"Modbus\\TCP Alert - Not Allowed Moudbus\\TCP Function Code","category":"","severity":3,"app_proto":"modbus","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":284,"bytes_toclient":218,"start":"2020-03-25T18:02:10.672140+0200"}}</pre> <p>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</p> $Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{30 + 150}{30 + 150 + 0 + 0} = 1$ $True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{30}{30 + 0} = 1$ $True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{150}{150 + 0} = 1$ $False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 150} = 0$ $F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 30}{2 \times 30 + 0 + 0} = 1$ <p>Therefore, based on these metrics, the following evaluation results are presented</p> <table><thead><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr></thead><tbody><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></tbody></table> <p>Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Accuracy | TPR         | TNR       | FPR         | F1                                                 | 1      | 1    | 1  | 0          | 0 |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| Accuracy   | TPR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | TNR      | FPR         | F1        |             |                                                    |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |
| 1          | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 1        | 0           | 0         |             |                                                    |        |      |    |            |   |    |     |    |                                                 |    |            |   |   |           |    |                                    |    |            |   |   |     |    |                                                |    |            |   |   |           |    |                                       |    |            |   |   |     |    |                                                 |    |            |   |    |     |    |                                               |    |            |    |   |     |    |                                                    |    |            |   |    |     |    |                                               |    |            |   |    |           |    |                                    |    |            |   |   |     |    |                                                |    |            |    |   |           |    |                                       |    |            |   |    |     |    |                                                 |    |            |   |   |     |    |                                               |

|                         |                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | detection results are accurate completely. However, in the case of zero-day attacks or without the appropriate specification rules, then the detection results could present FP and FN. |
| <b>Test Case Result</b> | Achieved                                                                                                                                                                                |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                  |                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------------------------|
| <b>Test Case ID</b>     | Modbus_Suricata_05                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Component</b> | Suricata (Sensor of XL-SIEM) |
| <b>Description</b>      | <p>This unit test intends to detect a modbus/function/readDiscreteInput (presented in subsection 2.3.2). Suricata is applied, specifying the appropriate Modbus/TCP specification rules according to the normal Modbus/TCP network traffic of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4), where only the Function Code 03 (0x03 - Read Holding Registers) is used. Although the same Suricata specification rule was utilised in the previous unit tests, this unit test aims at validating that Suricata can recognise modbus/function/readDiscreteInput attacks.</p> <p>The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to activate the Modbus/TCP keywords (commented by default). Next, a specification rule defining the Modbus/TCP normal behaviour of the Alkyonis PV Power Station is defined in the configuration file (/etc/Suricata/rules/suricata.rules). Next, the cyberattack modbus/function/readDiscreteInput is emulated, capturing and storing the Modbus/TCP network traffic in a pcap file. Finally, the pcap file is parsed by Suricata, recognising the aforementioned attack.</p> |                  |                              |
| <b>Spec ID</b>          | SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Priority</b>  | High                         |
| <b>Prepared by</b>      | UOWM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Tested by</b> | UOWM                         |
| <b>Pre-condition(s)</b> | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                  |                              |
| <b>Test steps</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                  |                              |

- 1 The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to uncomment the Modbus/TCP keywords. More precisely, in the /etc/suricata/suricata.yaml file, the rows of the Modbus/TCP keywords were activated, as depicted in the following figure.

```

927 modbus:
928 # How many unreplied Modbus requests are considered a flood.
929 # If the limit is reached, app-layer-event:modbus.flooded; will match.
930 #request-flood: 500
931
932 enabled: yes
933 detection-ports:
934 dp: 502
935 # According to MODBUS Messaging on TCP/IP Implementation Guide V1.0b, it
936 # is recommended to keep the TCP connection opened with a remote device
937 # and not to open and close it for each MODBUS/TCP transaction. In that
938 # case, it is important to set the depth of the stream reassembling as
939 # unlimited (stream.reassembly.depth: 0)
940
941 # Stream reassembly size for modbus. By default track it completely.
942 stream-depth: 0

```

Figure 18. Activation of Modbus/TCP keywords for test case Modbus\_Suricata\_05

- 2 As in the previous unit test, the following Suricata specification rule was used to recognise the Modbus/TCP commands that are not relevant to the Modbus/TCP network traffic of the Alkyonis PV Power Station (SDN-microSENSE Pilot 5 based on D2.4). The particular rule specifies that only Modbus/TCP Function Code 03 (0x03 - Read Holding Registers) is allowed.

```

alert modbus any any -> any 502 (modbus: function !3; msg:"Modbus/TCP Alert - Not Allowed
Moudbus/TCP Function Code"; sid: 2;)

```

- 3 Next, the cyberattack modbus/function/readDiscreteInput is emulated, adopting the Modbus/TCP network traffic of the Alkyonis PV Power Station. The UOWM Smod was used [Radoglou-Grammatikis20+1] for the execution of the cyberattack. Simultaneously, the network traffic related to the attack is captured through Wireshark in a pcap file called malicious\_pcap.pcap.

- 4 The pcap (malicious\_pcap.pcap) is parsed by Suricata offline, utilising the following command.
- ```

sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap

```

Input data

A pcap file (malicious_pcap.pcap) relevant to the modbus/function/readDiscreteInput attack. The following figure illustrates a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes 40 Modbus/TCP packets related to the modbus/function/writeSingleRegister attack and 150 Modbus/TCP packets related to Modbus/TCP Function Code 03 (0x03 - Read Holding Registers).

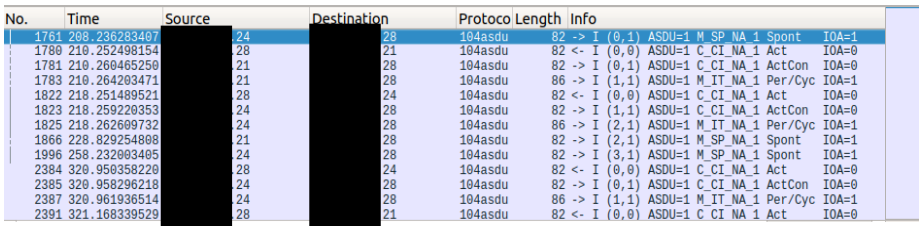
No.	Time	Source	Destination	Protocol	Length	Info
10	110.808321	17	6	TCP	66	502 -> 60192 [ACK] Seq=1 Ack=13 Win=29056 Len=
11	110.808334	17	6	Modbus...	76	Response: Trans: 2; Unit: 1, Func: 2;
12	110.808340	6	17	TCP	66	60192 -> 502 [ACK] Seq=13 Ack=11 Win=64256 Len=
13	110.827899	6	17	TCP	66	60192 -> 502 [FIN, ACK] Seq=13 Ack=11 Win=64256 Len=
14	110.832972	17	6	TCP	66	502 -> 60192 [FIN, ACK] Seq=11 Ack=14 Win=29056 Len=
15	110.833093	6	17	TCP	66	60192 -> 502 [ACK] Seq=14 Ack=12 Win=64256 Len=
16	110.840558	6	16	TCP	74	44536 -> 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1
17	110.843866	16	6	TCP	74	502 -> 44536 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
18	110.843885	6	16	TCP	66	44536 -> 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0
19	110.845570	6	16	Modbus...	78	Query: Trans: 2; Unit: 1, Func: 2;
20	110.848728	16	6	TCP	66	502 -> 44536 [ACK] Seq=1 Ack=13 Win=29056 Len=
21	110.848740	16	6	Modbus...	76	Response: Trans: 2; Unit: 1, Func: 2;
22	110.848748	6	16	TCP	66	44536 -> 502 [ACK] Seq=13 Ack=11 Win=64256 Len=

Figure 19. Pcap for modbus/function/readDiscreteInput attack for test case Modbus_Suricata_05

Result	<p>The modbus/function/readDiscreteInput attack was detected normally by Suricata. The detection results are stored in the eve.json file. An example of the respective alerts produced by Suricata is depicted below.</p> <pre>{"timestamp":"2020-03-26T14:13:25.346664+0200","flow_id":586922789774764,"pcap_cnt":1999,"event_type":"alert","src_ip":"XX.XX.XX.XX","src_port":xx,"dest_ip":"YY.YY.YY.YY","dest_port":yy,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2,"rev":0,"signature":"Modbus\\TCP Alert - Not Allowed Moudbus\\TCP Function Code","category":"","severity":3},"app_proto":"modbus","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":284,"bytes_toclient":216,"start":"2020-03-26T14:13:25.337324+0200"}}</pre>									
	<p>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</p>									
	$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{40 + 150}{40 + 150 + 0 + 0} = 1$									
	$True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{40}{40 + 0} = 1$									
	$True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{150}{150 + 0} = 1$									
$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 150} = 0$										
$F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 40}{2 \times 40 + 0 + 0} = 1$										
<p>Therefore, based on these metrics, the following evaluation results are presented</p>										
<table><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></table>	Accuracy	TPR	TNR	FPR	F1	1	1	1	0	0
Accuracy	TPR	TNR	FPR	F1						
1	1	1	0	0						
<p>Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks or without the appropriate specification rules, then the detection results could present FP and FN.</p>										
Test Case Result	Achieved									

4.2 IEC104 Unit Tests – Suricata

The goal of this subsection is to verify the effectiveness of the Suricata specification rules presented in subsection 2.2.4) against IEC 60870-5-104 cyberattacks. In particular, both predefined and custom Suricata specification rules were constructed that can detect the following cyberattacks, C_CI_NA_1, C_SE_NA_1 and C_SC_NA_1. The remaining cyberattacks, namely M_SP_NA_1_DoS, C_SE_NA_1_DoS, C_SC_NA_1_DoS and C_CI_NA_1_DoS will be adopted by the ML solutions of Task 5.3/D5.3.

Test Case ID	IEC104_Suricata_01	Component	Suricata (Sensor of XL-SIEM)
Description	<p>This unit test intends to detect the C_CI_NA_1 cyberattack presented in subsection 2.2.2. To this end, on the one hand, a particular Suricata IEC 60870-5-104-related specification rule is used from subsection 2.2.4 and Annex 3. On the other hand, a malicious IEC 60870-5-104-related network traffic data (pcap file) from the UOWM IEC 60870-5-104 intrusion detection dataset is adopted.</p> <p>First, a particular specification rule related to C_CI_NA_1 is defined and stored in the configuration file (/etc/Suricata/rules/suricata.rules), which contains all specification rules of Suricata. Finally, the pcap file of the UOWM IEC 60870-5-104 intrusion detection dataset is parsed suitably by Suricata, detecting successfully the relevant attack.</p>		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	High
Prepared by	SID	Tested by	SID
Pre-condition(s)	-		
Test steps			
1	<p>The following Suricata specification rule was used to detect the C_CI_NA_1 attack presented in subsection 2.2.2.</p> <pre>alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 counter interrogation command"; flow:established; content:" 68 "; content:" 65 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41075; rev:4;)</pre>		
2	<p>The pcap (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset is parsed by Suricata offline, utilising the following command.</p> <pre>sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap</pre>		
Input data	<p>A pcap file (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset. The following figure depicts a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes 50 C_CI_NA_1 packets and 150 normal IEC 60870-5-104 packets.</p>  <p>Figure 20. Pcap for UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_01</p>		

Result	<p>The C_CI_NA_1 was recognised successfully by Suricata. The detection results are stored in the eve.json file. The corresponding alert generated by Suricata is provided below.</p> <pre>{ "timestamp": "2020-04-26T13:40:29.040698+0300", "flow_id": 1057454856209836, "pcap_cnt": 2391, "event_type": "alert", "src_ip": "XX.XX.XX.XX", "src_port": XX, "dest_ip": "YY.YY.YY.YY", "dest_port": YY, "proto": "TCP", "alert": { "action": "allowed", "gid": 1, "signature_id": 41075, "rev": 4, "signature": "PROTOCOL-SCADA IEC 104 counter interrogation command", "category": "Generic Protocol Command Decode", "severity": 3 }, "flow": { "pkts_toserver": 5, "pkts_toclient": 2, "bytes_toserver": 360, "bytes_toclient": 146, "start": "2020-04-26T13:40:18.984492+0300" } }</pre> <p>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</p> $Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{50 + 150}{50 + 150 + 0 + 0} = 1$ $True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{50}{50 + 0} = 1$ $True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{150}{150 + 0} = 1$ $False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 150} = 0$ $F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 50}{2 \times 50 + 0 + 0} = 1$ <p>Therefore, based on these metrics, the following evaluation results are presented</p> <table><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></table> <p>Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks or without the appropriate specification rules, then the detection results could present FP and FN.</p>	Accuracy	TPR	TNR	FPR	F1	1	1	1	0	0
Accuracy	TPR	TNR	FPR	F1							
1	1	1	0	0							
Test Case Result	Achieved										

Test Case ID	IEC104_Suricata_02	Component	Suricata (Sensor of XL-SIEM)
Description	<p>This unit test aims to recognise the C_SE_NA_1 cyberattack presented in subsection 2.2.2. To this end, a specific Suricata IEC 60870-5-104-related specification rule is applied from subsection 2.2.4 and Annex 3. On the other side, a malicious IEC 60870-5-104-related network traffic data (pcap file) from the UOWM IEC 60870-5-104 intrusion detection dataset is used.</p>		

	First, a particular specification rule related to C_SE_NA_1 is defined and stored in the configuration file (/etc/Suricata/rules/suricata.rules), which includes all specification rules of Suricata. Finally, the pcap file of the UOWM IEC 60870-5-104 intrusion detection dataset is processed appropriately by Suricata, recognising successfully the relevant attack.																																																																																																				
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	High																																																																																																		
Prepared by	SID	Tested by	SID																																																																																																		
Pre-condition(s)	-																																																																																																				
Test steps																																																																																																					
1	The following Suricata specification rule was utilised in order to recognise the C_SE_NA_1 attack described in subsection 2.2.2. alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SE_NA_1"; flow:established; content:" 68 "; depth:1; content:" 30 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52174; rev:1;)																																																																																																				
2	The pcap (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset is analysed by Suricata, using the following command. sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap																																																																																																				
Input data	A pcap file (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset. The following figure illustrates a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes 20 C_SE_NA_1_1 packets and 100 normal IEC 60870-5-104 packets. <table><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>363</td><td>173.528439886</td><td>28</td><td>21</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]</td></tr><tr><td>364</td><td>173.537667515</td><td>21</td><td>28</td><td>104asdu</td><td>84</td><td>-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2</td></tr><tr><td>366</td><td>173.753571402</td><td>28</td><td>24</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]</td></tr><tr><td>367</td><td>173.765175353</td><td>24</td><td>28</td><td>104asdu</td><td>84</td><td>-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2</td></tr><tr><td>391</td><td>188.012635658</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>394</td><td>188.358892445</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>669</td><td>274.556208946</td><td>28</td><td>21</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]</td></tr><tr><td>670</td><td>274.565530888</td><td>21</td><td>28</td><td>104asdu</td><td>84</td><td>-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2</td></tr><tr><td>672</td><td>274.799301910</td><td>28</td><td>24</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]</td></tr><tr><td>673</td><td>274.812216692</td><td>24</td><td>28</td><td>104asdu</td><td>84</td><td>-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2</td></tr><tr><td>700</td><td>288.050078633</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>702</td><td>288.908499321</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>946</td><td>361.095024940</td><td>28</td><td>21</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]</td></tr></table> <i>Figure 21. Pcap file of UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_02</i>			No.	Time	Source	Destination	Protocol	Length	Info	363	173.528439886	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]	364	173.537667515	21	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2	366	173.753571402	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]	367	173.765175353	24	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2	391	188.012635658	21	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1	394	188.358892445	24	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1	669	274.556208946	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]	670	274.565530888	21	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2	672	274.799301910	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]	673	274.812216692	24	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2	700	288.050078633	21	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1	702	288.908499321	24	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1	946	361.095024940	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]
No.	Time	Source	Destination	Protocol	Length	Info																																																																																															
363	173.528439886	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]																																																																																															
364	173.537667515	21	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2																																																																																															
366	173.753571402	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]																																																																																															
367	173.765175353	24	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2																																																																																															
391	188.012635658	21	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																															
394	188.358892445	24	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																															
669	274.556208946	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]																																																																																															
670	274.565530888	21	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2																																																																																															
672	274.799301910	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]																																																																																															
673	274.812216692	24	28	104asdu	84	-> I (0,1) ASDU=1 C_SE_NA_1 ActCon IOA=2																																																																																															
700	288.050078633	21	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																															
702	288.908499321	24	28	104asdu	82	-> I (1,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																															
946	361.095024940	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SE_NA_1 Act IOA=2[Mal]																																																																																															
Result	The C_SE_NA_1 was recognised successfully by Suricata. The detection results are stored in the eve.json file. The corresponding alert generated by Suricata is provided below. {"timestamp":"2020-04-27T18:15:11.108586+0300","flow_id":695148895097382,"pcap_cnt":672,"event_type":"alert","src_ip":"XX.XX.XX.XX","src_port":XX,"dest_ip":"XX.XX.XX.XX","dest_port":XX,"proto":"TCP","flow":{"pkts_toserver":5,"pkts_toclient":2,"bytes_toserver":360,"bytes_toclient":146,"start":"2020-04-27T18:15:01.086566+0300"},"alert":{"action":"allowed","gid":1,"signature_id":52174,"rev":1,"si																																																																																																				

	<div>gnature":"PROTOCOL-SCADA IEC 104 C_SE_NA_1","category":"Generic Protocol Command Decode"},"severity":3}}</div> <div>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</div> <div>$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{20 + 100}{20 + 100 + 0 + 0} = 1$</div> <div>$True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{20}{20 + 0} = 1$</div> <div>$True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{100}{100 + 0} = 1$</div> <div>$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 100} = 0$</div> <div>$F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 20}{2 \times 20 + 0 + 0} = 1$</div> <div>Therefore, based on these metrics, the following evaluation results are presented</div> <table><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></table> <div>Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks or without the appropriate specification rules, then the detection results could present FP and FN.</div>	Accuracy	TPR	TNR	FPR	F1	1	1	1	0	0
Accuracy	TPR	TNR	FPR	F1							
1	1	1	0	0							
Test Case Result	Achieved										

Test Case ID	IEC104_Suricata_03	Component	Suricata (Sensor of XL-SIEM)
Description	<p>This unit test intends to detect the C_SC_NA_1 cyberattack explained in subsection 2.2.2. A particular Suricata IEC 60870-5-104-related specification rule is utilised from subsection 2.2.4 and Annex 3. In contrast, a malicious IEC 60870-5-104-related network traffic data (pcap file) from the UOWM IEC 60870-5-104 intrusion detection dataset is used.</p> <p>First, an appropriate specification rule relevant to C_SC_NA_1 is defined in the configuration file (/etc/Suricata/rules/suricata.rules), which contains all specification rules of Suricata. Finally, the pcap file of the UOWM IEC 60870-5-104 intrusion detection dataset is parsed by Suricata, recognising successfully the relevant attack.</p>		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	High
Prepared by	SID	Tested by	SID

Pre-condition (s)	-																																																																																																		
Test steps																																																																																																			
1	<p>The following Suricata specification rule was used in to detect the C_SC_NA_1 attack described in subsection 2.2.2.</p> <pre>alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SC_NA_1"; flow:established; content:" 68 "; depth:1; content:" 2D "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52171; rev:1;)</pre>																																																																																																		
2	<p>The pcap (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset is parsed by Suricata, utilising the below command.</p> <pre>sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap</pre>																																																																																																		
Input data	<p>A pcap file (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset. The following figure illustrates a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes 30 C_SC_NA_1 packets and 100 normal IEC 60870-5-104 packets.</p> <table><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>6837</td><td>541.889618515</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>6869</td><td>543.193343742</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>6956</td><td>551.902762672</td><td>28</td><td>21</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>6957</td><td>551.913897914</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>6959</td><td>551.917968679</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2</td></tr><tr><td>6971</td><td>553.200316481</td><td>28</td><td>24</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>6972</td><td>553.211801071</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>6975</td><td>553.214674995</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2</td></tr><tr><td>7592</td><td>617.461639440</td><td>28</td><td>24</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>7593</td><td>617.467081280</td><td>28</td><td>21</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>7594</td><td>617.475703299</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>7596</td><td>617.475750126</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>7598</td><td>617.479047878</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2</td></tr></table> <p>Figure 22. Pcap file of UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_03</p>	No.	Time	Source	Destination	Protocol	Length	Info	6837	541.889618515	21	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1	6869	543.193343742	24	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1	6956	551.902762672	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	6957	551.913897914	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	6959	551.917968679	21	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2	6971	553.200316481	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	6972	553.211801071	24	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	6975	553.214674995	24	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2	7592	617.461639440	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	7593	617.467081280	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	7594	617.475703299	24	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	7596	617.475750126	21	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	7598	617.479047878	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2
No.	Time	Source	Destination	Protocol	Length	Info																																																																																													
6837	541.889618515	21	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																													
6869	543.193343742	24	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																													
6956	551.902762672	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
6957	551.913897914	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
6959	551.917968679	21	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2																																																																																													
6971	553.200316481	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
6972	553.211801071	24	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
6975	553.214674995	24	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2																																																																																													
7592	617.461639440	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
7593	617.467081280	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
7594	617.475703299	24	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
7596	617.475750126	21	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
7598	617.479047878	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2																																																																																													
Result	<p>The C_SE_NA_1 was recognised successfully by Suricata. The detection results are stored in the eve.json file. The corresponding alert generated by Suricata is provided below.</p> <pre>{"timestamp":"2020-04-28T21:24:59.491102+0300","flow_id":375306941721969,"pcap_cnt":6956,"event_type":"alert","src_ip":"XX.XX.XX.XX","src_port":XX,"dest_ip":"XX.XX.XX.XX","dest_port":XX,"proto":"TCP","flow":{"pkts_toserver":6,"pkts_toclient":3,"bytes_toserver":426,"bytes_toclient":228,"start":"2020-04-28T21:24:49.355697+0300"},"alert":{"action":"allowed","gid":1,"signature_id":52171,"rev":1,"signature":"PROTOCOL-SCADA IEC 104 C_SC_NA_1","category":"Generic Protocol Command Decode","severity":3}}</pre> <p>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</p> $Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{30 + 100}{30 + 100 + 0 + 0} = 1$																																																																																																		

	$\text{True Positive Rate (TPR)} = \frac{TP}{TP + FN} = \frac{30}{30 + 0} = 1$ $\text{True Negative Rate (TNR)} = \frac{TN}{TN + FP} = \frac{100}{100 + 0} = 1$ $\text{False Positive Rate (FPR)} = \frac{FP}{FP + TN} = \frac{0}{0 + 100} = 0$ $F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 30}{2 \times 30 + 0 + 0} = 1$ <p>Therefore, based on these metrics, the following evaluation results are presented</p> <table><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></table> <p>Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks or without the appropriate specification rules, then the detection results could present FP and FN.</p>	Accuracy	TPR	TNR	FPR	F1	1	1	1	0	0
Accuracy	TPR	TNR	FPR	F1							
1	1	1	0	0							
Test Case Result	Achieved										

Test Case ID	IEC104_Suricata_04	Component	Suricata (XL SIEM Sensor)
Description	An appropriate python script called SIREN loads a pcap file with only IEC 60870-5-104 normal traffic, thereby identifying the IEC 60970-5-104 packets' and specifying Suricata IEC 60870-5-104 specification rules that define the normal behaviour of an emulated environment. These Suricata specification rules are applied against a malicious pcap file, which includes IEC 60970-5-104 that are not contained in the initial, normal pcap file. Therefore, the Suricata specification rule identifies the IEC 60970-5-104 anomalies.		
Spec IDs	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	Medium
Prepared by	SID	Tested by	SID
Pre-condition(s)	The initial pcap file includes only normal IEC 60970-5-104 packets.		
Test steps			
1	SIREN loads a pcap file with only IEC 60870-5-104 normal traffic and exports the following IEC 60870-5-104 specification rules.		

	<pre>alert tcp any any <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_IC_NA_1"; content:" 68 ",depth 1; content:" 64 ",within 1,distance 5; reference:Sidroco_Holdings_IEC104_RULES; sid:41078; rev:1;) alert tcp any any <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SC_NA_1"; content:" 68 ",depth 1; content:" 2D ",within 1,distance 5; reference:Sidroco_Holdings_IEC104_RULES; sid:41079; rev:1;)</pre>																																																																																																		
2	The new rules are inserted into the configuration file (/etc/Suricata/rules/suricata.rules), which includes all specification rules of Suricata.																																																																																																		
3	The malicious pcap file (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset is parsed by Suricata, utilising the below command. sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap																																																																																																		
Input data	<p>A pcap file (malicious_pcap.pcap) of the UOWM IEC 60870-5-104 intrusion detection dataset. The following figure illustrates a sample of this pcap file.</p> <table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>6837</td><td>541.889610515</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>6869</td><td>543.193343742</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1</td></tr><tr><td>6956</td><td>551.902762672</td><td>28</td><td>21</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>6957</td><td>551.913897914</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>6959</td><td>551.917968679</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2</td></tr><tr><td>6971</td><td>553.200316481</td><td>28</td><td>24</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>6972</td><td>553.211801071</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>6975</td><td>553.214674995</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2</td></tr><tr><td>7592</td><td>617.461639440</td><td>28</td><td>24</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>7593</td><td>617.467081280</td><td>28</td><td>21</td><td>104asdu</td><td>82</td><td><- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2</td></tr><tr><td>7594</td><td>617.475703299</td><td>24</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>7596</td><td>617.475750126</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2</td></tr><tr><td>7598</td><td>617.479047878</td><td>21</td><td>28</td><td>104asdu</td><td>82</td><td>-> I (1,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2</td></tr></tbody></table> <p>Figure 23. Pcap file of UOWM IEC 60870-5-104 dataset for test case IEC104_Suricata_04</p>	No.	Time	Source	Destination	Protocol	Length	Info	6837	541.889610515	21	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1	6869	543.193343742	24	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1	6956	551.902762672	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	6957	551.913897914	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	6959	551.917968679	21	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2	6971	553.200316481	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	6972	553.211801071	24	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	6975	553.214674995	24	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2	7592	617.461639440	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	7593	617.467081280	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2	7594	617.475703299	24	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	7596	617.475750126	21	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2	7598	617.479047878	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2
No.	Time	Source	Destination	Protocol	Length	Info																																																																																													
6837	541.889610515	21	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																													
6869	543.193343742	24	28	104asdu	82	-> I (0,1) ASDU=1 M_SP_NA_1 Spont IOA=1																																																																																													
6956	551.902762672	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
6957	551.913897914	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
6959	551.917968679	21	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2																																																																																													
6971	553.200316481	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
6972	553.211801071	24	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
6975	553.214674995	24	28	104asdu	82	-> I (2,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2																																																																																													
7592	617.461639440	28	24	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
7593	617.467081280	28	21	104asdu	82	<- I (0,0) ASDU=1 C_SC_NA_1 Act IOA=2																																																																																													
7594	617.475703299	24	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
7596	617.475750126	21	28	104asdu	82	-> I (0,1) ASDU=1 C_SC_NA_1 ActCon IOA=2																																																																																													
7598	617.479047878	21	28	104asdu	82	-> I (1,1) ASDU=1 C_SC_NA_1 ActTerm IOA=2																																																																																													
Result	<p>The C_SE_NA_1 was recognised successfully by Suricata. The detection results are stored in the eve.json file. The corresponding alert generated by Suricata is provided below.</p> <pre>{"timestamp":"2020-04-28T21:24:59.491102+0300","flow_id":375306941721969,"pcap_cnt":6956,"event_type":"alert","src_ip":"XX.XX.XX.XX","src_port":XX,"dest_ip":"XX.XX.XX.XX","dest_port":XX,"proto":"TCP","flow":{"pkts_toserver":6,"pkts_toclient":3,"bytes_toserver":426,"bytes_toclient":228,"start":"2020-04-28T21:24:49.355697+0300"},"alert":{"action":"allowed","gid":1,"signature_id":52171,"rev":1,"signature":"PROTOCOL-SCADA IEC 104 C_SC_NA_1","category":"Generic Protocol Command Decode","severity":3}}</pre>																																																																																																		
Test Case Result	Achieved																																																																																																		

4.3 DNP3 Unit Tests – Suricata

This subsection intends to examine and verify the efficiency of the Suricata specification rules presented in subsection 2.3.4 and Annex 2 against the DNP3 cyberattacks presented in subsection 2.4.2. In particular, the following unit tests are related to the a) DNP3 Disable Unsolicited Messages Attack, b) DNP3 Cold Restart Message Attack, c) DNP3 Info and d) DNP3 enumerate. On the other side, the DNP3 Warm Restart Message Attack will be examined in Task 5.3/D5.3.

Test Case ID	DNP3_Suricata_01	Component	Suricata (Sensor of XL-SIEM)
Description	<p>This unit test intends to detect a DNP3 Disable Unsolicited Messages Attack presented in subsection 2.4.2. To this end, on the one hand, a particular Suricata DNP3-related specification rule is used from subsection 2.4.4 and Annex 2. On the other hand, the malicious DNP3-related network traffic data (pcap file) of [Pliatsios20] is adopted.</p> <p>First, the configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to consider normally the DNP3 keywords. Next, a specific specification rule related to the DNP3 Disable Unsolicited Messages Attack is defined and stored in the configuration file (/etc/Suricata/rules/suricata.rules), which contains all specification rules of Suricata. Finally, the pcap file of [Pliatsios20] is parsed suitably by Suricata, detecting successfully the relevant attack.</p>		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	High
Prepared by	OINF	Tested by	OINF
Pre-condition(s)	-		
Test steps			
1	<p>The configuration file of Suricata (/etc/suricata/suricata.yaml) was edited to consider the DNP3 keywords. In particular, in the /etc/suricata/suricata.yaml file, the rows of the DNP3 keywords were uncommented, as depicted in the following figure.</p> <div><pre>944 # DNP3 945 dnp3: 946 enabled: yes 947 detection-ports: 948 dp: 20000 949</pre></div> <p>Figure 24. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_01</p>		
2	<p>The following Suricata specification rule was used in order to detect the DNP3 Disable Unsolicited Messages Attack presented in subsection 2.4.2.</p> <pre>alert tcp \$DNP3_SERVER 20000 -> \$DNP3_CLIENT any (flow:established; content:" 82 "; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Unsolicited Response Storm"; threshold: type threshold, track by_src, count 5, seconds 10; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:1111203; rev:1; priority:2;)</pre>		
3	<p>The pcap (malicious_pcap.pcap) of [Pliatsios20] is parsed by Suricata offline, utilising the following command.</p> <pre>sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap</pre>		
Input data	A pcap file (malicious_pcap.pcap) of [Pliatsios20]. The following figure depicts a sample of this pcap file. In particular, this pcap file (malicious pcap.pcap) includes		

	<div>30 packets related to DNP3 Disable Unsolicited Messages Attack and 100 normal DNP3 packets</div> <div><table><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>1</td><td>0.000000</td><td>198</td><td>197</td><td>TCP</td><td>74</td><td>36639 → 20000 [SYN] Seq=0 Win=29200 Len=0 MSS</td></tr><tr><td>2</td><td>0.000043</td><td>197</td><td>198</td><td>TCP</td><td>74</td><td>20000 → 36639 [SYN, ACK] Seq=0 Ack=1 Win=2896</td></tr><tr><td>3</td><td>0.000294</td><td>198</td><td>197</td><td>TCP</td><td>66</td><td>36639 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len</td></tr><tr><td>4</td><td>0.000629</td><td>197</td><td>198</td><td>DNP 3.0</td><td>83</td><td>Unsolicited Response</td></tr><tr><td>5</td><td>0.000893</td><td>198</td><td>197</td><td>TCP</td><td>66</td><td>36639 → 20000 [ACK] Seq=1 Ack=18 Win=29312 Le</td></tr><tr><td>6</td><td>0.003323</td><td>198</td><td>197</td><td>DNP 3.0</td><td>93</td><td>Read, Class 0123</td></tr><tr><td>7</td><td>0.003338</td><td>197</td><td>198</td><td>TCP</td><td>66</td><td>20000 → 36639 [ACK] Seq=18 Ack=28 Win=29056 L</td></tr><tr><td>8</td><td>0.003947</td><td>198</td><td>197</td><td>DNP 3.0</td><td>81</td><td>Confirm</td></tr><tr><td>9</td><td>0.003965</td><td>197</td><td>198</td><td>TCP</td><td>66</td><td>20000 → 36639 [ACK] Seq=18 Ack=43 Win=29056 L</td></tr><tr><td>10</td><td>0.004188</td><td>197</td><td>198</td><td>DNP 3.0</td><td>358</td><td>from 10 to 1, len=255, Unconfirmed User Data</td></tr><tr><td>11</td><td>0.043865</td><td>198</td><td>197</td><td>TCP</td><td>66</td><td>36639 → 20000 [ACK] Seq=43 Ack=310 Win=30336</td></tr><tr><td>12</td><td>0.043903</td><td>197</td><td>198</td><td>DNP 3.0</td><td>106</td><td>Response</td></tr><tr><td>13</td><td>0.044150</td><td>198</td><td>197</td><td>TCP</td><td>66</td><td>36639 → 20000 [ACK] Seq=43 Ack=350 Win=30336</td></tr></table></div> <div>Figure 25. Pcap of [Platisios20] for test case DNP3_Suricata_01</div>	No.	Time	Source	Destination	Protocol	Length	Info	1	0.000000	198	197	TCP	74	36639 → 20000 [SYN] Seq=0 Win=29200 Len=0 MSS	2	0.000043	197	198	TCP	74	20000 → 36639 [SYN, ACK] Seq=0 Ack=1 Win=2896	3	0.000294	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len	4	0.000629	197	198	DNP 3.0	83	Unsolicited Response	5	0.000893	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=18 Win=29312 Le	6	0.003323	198	197	DNP 3.0	93	Read, Class 0123	7	0.003338	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=28 Win=29056 L	8	0.003947	198	197	DNP 3.0	81	Confirm	9	0.003965	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=43 Win=29056 L	10	0.004188	197	198	DNP 3.0	358	from 10 to 1, len=255, Unconfirmed User Data	11	0.043865	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=310 Win=30336	12	0.043903	197	198	DNP 3.0	106	Response	13	0.044150	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=350 Win=30336
No.	Time	Source	Destination	Protocol	Length	Info																																																																																													
1	0.000000	198	197	TCP	74	36639 → 20000 [SYN] Seq=0 Win=29200 Len=0 MSS																																																																																													
2	0.000043	197	198	TCP	74	20000 → 36639 [SYN, ACK] Seq=0 Ack=1 Win=2896																																																																																													
3	0.000294	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len																																																																																													
4	0.000629	197	198	DNP 3.0	83	Unsolicited Response																																																																																													
5	0.000893	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=18 Win=29312 Le																																																																																													
6	0.003323	198	197	DNP 3.0	93	Read, Class 0123																																																																																													
7	0.003338	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=28 Win=29056 L																																																																																													
8	0.003947	198	197	DNP 3.0	81	Confirm																																																																																													
9	0.003965	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=43 Win=29056 L																																																																																													
10	0.004188	197	198	DNP 3.0	358	from 10 to 1, len=255, Unconfirmed User Data																																																																																													
11	0.043865	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=310 Win=30336																																																																																													
12	0.043903	197	198	DNP 3.0	106	Response																																																																																													
13	0.044150	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=350 Win=30336																																																																																													
Result	<div><p>The DNP3 Disable Unsolicited Messages Attack was recognised successfully by Suricata. The detection results are stored in the eve.json file. The corresponding alert generated by Suricata is provided below.</p><pre>{ "timestamp": "2017-02-14T01:28:54.950977+0200", "flow_id": "706430872485681", "pcap_cnt": "1428", "event_type": "alert", "src_ip": "XX.XX.XX.XX", "src_port": "XX", "dest_ip": "XX.XX.XX.XX", "dest_port": "XX", "proto": "TCP", "alert": { "action": "allowed", "gid": "1", "signature_id": "1111203", "rev": "1", "signature": "SCADA_IDS: DNP3 - Unsolicited Response Storm", "category": "Attempted Denial of Service", "severity": "2", "flow": { "pkts_toserver": "2", "pkts_toclient": "2", "bytes_toserver": "140", "bytes_toclient": "157", "start": "2017-02-14T01:28:54.950065+0200" } } }</pre><p>Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.</p>$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{30 + 100}{30 + 100 + 0 + 0} = 1$$True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{30}{30 + 0} = 1$$True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{100}{100 + 0} = 1$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 100} = 0$$F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 30}{2 \times 30 + 0 + 0} = 1$<p>Therefore, based on these metrics, the following evaluation results are presented</p><table><tr><th>Accuracy</th><th>TPR</th><th>TNR</th><th>FPR</th><th>F1</th></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr></table><p>Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks or without the appropriate specification rules, then the detection results could present FP and FN.</p></div>	Accuracy	TPR	TNR	FPR	F1	1	1	1	0	0																																																																																								
Accuracy	TPR	TNR	FPR	F1																																																																																															
1	1	1	0	0																																																																																															
Test Case Result	Achieved																																																																																																		

Test Case ID	DNP3_Suricata_02	Component	Suricata (Sensor of XL-SIEM)
Description	<p>This unit test aims to recognise a DNP3 Cold Restart Message Attack described in subsection 2.4.2. To this end, a specific Suricata DNP3-related specification rule is utilised from subsection 2.4.4 and Annex 2. On the other hand, the malicious DNP3-related network traffic data (pcap file) of [Pliatsios20] is used.</p> <p>First, the configuration file of Suricata (/etc/suricata/suricata.yaml) was edited to take into account the DNP3 keywords. Then, a particular specification rule relevant to the DNP3 Cold Restart Message Attack is defined in the configuration file (/etc/Suricata/rules/suricata.rules), which comprises all specification rules of Suricata. Finally, the pcap file of [Pliatsios20] is processed appropriately by Suricata, thus detecting successfully the relevant attack.</p>		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	High
Prepared by	OINF	Tested by	OINF
Pre-condition(s)	-		
Test steps			
1	<p>The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to take into account the DNP3 keywords. In particular, in the /etc/suricata/suricata.yaml file, the lines of the DNP3 keywords were uncommented, as illustrated in the following figure.</p> <div><pre>944 # DNP3 945 dnp3: 946 enabled: yes 947 detection-ports: 948 dp: 20000 949</pre></div> <p>Figure 26. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_02</p>		
2	<p>The following Suricata specification rule was adopted to recognise the DNP3 Cold Restart Message Attack described in subsection 2.4.2.</p> <pre>alert tcp \$DNP3_CLIENT any -> \$DNP3_SERVER 20000 (msg:"SCADA_IDS: DNP3 - Cold Restart From Authorized Client"; dnp3_func:13; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112041; rev:1; priority:2;)</pre>		
3	<p>The pcap (malicious_pcap.pcap) of [Pliatsios20] is processed by Suricata offline, using the following command.</p> <pre>sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap</pre>		
Input data	A pcap file (malicious_pcap.pcap) of [Pliatsios20]. The following figure shows a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes		

20 packets related to DNP3 Cold Restart Message Attack and 150 normal DNP3 packets.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	198	197	TCP	74	36639 → 20000 [SYN] Seq=0 Win=29200 Len=0 MSS=
2	0.000043	197	198	TCP	74	20000 → 36639 [SYN, ACK] Seq=0 Ack=1 Win=2896
3	0.000294	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len=0
4	0.000629	197	198	DNP 3.0	83	Unsolicited Response
5	0.000893	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=18 Win=29312 Len=0
6	0.003323	198	197	DNP 3.0	93	Read, Class 0123
7	0.003338	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=28 Win=29056 Len=0
8	0.003947	198	197	DNP 3.0	81	Confirm
9	0.003965	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=43 Win=29056 Len=0
10	0.004188	197	198	DNP 3.0	358	from 10 to 1, len=255, Unconfirmed User Data
11	0.043865	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=310 Win=30336 Len=0
12	0.043903	197	198	DNP 3.0	106	Response
13	0.044150	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=350 Win=30336 Len=0

Figure 27. Pcap of [PlatiSios20] for test case DNP3_Suricata_02

Result

The DNP3 Cold Restart Message Attack was detected successfully by Suricata. The detection results are stored in the eve.json file. The corresponding alert produced by Suricata is provided below.

```
{
  "timestamp": "2017-02-14T06:24:28.099147+0200",
  "flow_id": "2144573915774774",
  "pcap_cnt": "21984",
  "event_type": "alert",
  "src_ip": "XX.XX.XX.XX",
  "src_port": "XX",
  "dest_ip": "XX.XX.XX.XX",
  "dest_port": "XX",
  "proto": "TCP",
  "tx_id": "7",
  "alert": {
    "action": "allowed",
    "gid": "1",
    "signature_id": "11112041",
    "rev": "1",
    "signature": "SCADA_IDS: DNP3 - Cold Restart From Authorized Client",
    "category": "Attempted Denial of Service",
    "severity": "2",
    "dnp3": {
      "request": {
        "type": "request",
        "control": {
          "dir": "true",
          "pri": "true",
          "fcb": "false",
          "fcr": "false",
          "function_code": "4",
          "src": "1",
          "dst": "10",
          "application": {
            "control": {
              "fir": "true",
              "fin": "true",
              "con": "false",
              "uns": "false",
              "sequence": "5",
              "function_code": "13",
              "objects": [],
              "complete": true
            }
          }
        }
      },
      "app_proto": "dnp3",
      "flow": {
        "pkts_toserver": "18",
        "pkts_toclient": "13",
        "bytes_toserver": "1358",
        "bytes_toclient": "1632",
        "start": "2017-02-14T06:24:17.704310+0200"
      }
    }
  }
}
```

Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{20 + 150}{20 + 150 + 0 + 0} = 1$$

$$True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{20}{20 + 0} = 1$$

$$True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{150}{150 + 0} = 1$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 150} = 0$$

$$F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 20}{2 \times 20 + 0 + 0} = 1$$

Therefore, based on these metrics, the following evaluation results are presented

Accuracy	TPR	TNR	FPR	F1
1	1	1	0	0

Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks

	or without the appropriate specification rules, then the detection results could present FP and FN.
Test Case Result	Achieved

Test Case ID	DNP3_Suricata_03	Component	Suricata (Sensor of XL-SIEM)
Description	<p>This unit test intends to recognise the DNP3 Info attack explained in subsection 2.4.2. To this end, a particular Suricata DNP3-related specification rule is used from subsection 2.4.4 and Annex 2. In contrast, the DNP3-related network traffic data (pcap file) of [Pliatsios20] is utilised as the malicious DNP3-related network traffic.</p> <p>First, the configuration file of Suricata (/etc/suricata/suricata.yaml) was edited to take into consideration the DNP3 keywords. Subsequently, a specification rule related to the DNP3 Info attack is defined and stored in the configuration file (/etc/Suricata/rules/suricata.rules), which includes all specification rules of Suricata. Finally, the pcap file of [Pliatsios20] is parsed by Suricata, thus recognising successfully the relevant attack.</p>		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	Medium
Prepared by	OINF	Tested by	OINF
Pre-condition(s)	-		
Test steps			
1	<p>The configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to take into consideration the DNP3 keywords. Specifically, in the /etc/suricata/suricata.yaml file, the rows of the DNP3 keywords were activated, as illustrated in the following figure.</p> <div><pre>944 # DNP3 945 dnp3: 946 enabled: yes 947 detection-ports: 948 dp: 20000 949</pre></div> <p>Figure 28. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_03</p>		
2	<p>The following Suricata specification rule was adopted to recognise the DNP3 Info attack, which is described in subsection 2.4.2.</p> <pre>alert tcp \$DNP3_SERVER 20000 -> any any (flow:established; content:" 81 "; offset:12; depth:1; pcre:"/[\Ss]{1}(\x01)/iAR"; msg:"SCADA_IDS: DNP3 - Function Code Scan"; threshold: type threshold, track by_src, count 3, seconds 60; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-recon; sid:1111214; rev:1; priority:2;)</pre>		

- 3 The pcap (malicious_pcap.pcap) of [Pliatsios20] is analysed by Suricata offline, using the following command. In particular, this pcap file (malicious_pcap.pcap) includes 20 packets related to DNP3 Info attack and 100 normal DNP3 packets.

```
sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap
```

Input data

A pcap file (malicious_pcap.pcap) of [Pliatsios20]. The following figure shows a sample of this pcap file.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	198	197	TCP	74	36639 → 20000 [SYN] Seq=0 Win=29280 Len=0 MSS=
2	0.000043	197	198	TCP	74	20000 → 36639 [SYN, ACK] Seq=0 Ack=1 Win=2896
3	0.000294	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len
4	0.000629	197	198	DNP 3.0	83	Unsolicited Response
5	0.000893	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=18 Win=29312 Le
6	0.003323	198	197	DNP 3.0	93	Read, Class 0123
7	0.003338	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=28 Win=29056 L
8	0.003947	198	197	DNP 3.0	81	Confirm
9	0.003965	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=43 Win=29056 L
10	0.004188	197	198	DNP 3.0	358	from 10 to 1, len=255, Unconfirmed User Data
11	0.043865	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=310 Win=30336
12	0.043903	197	198	DNP 3.0	106	Response
13	0.044150	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=350 Win=30336

Figure 29. Pcap of [Pliatsios20] for test case DNP3_Suricata_03

Result

The DNP3 Info attack was recognised successfully by Suricata. The detection results are stored in the eve.json file. The respective alert generated by Suricata is shown below.

```
{"timestamp":"2017-02-14T06:24:28.538383+0200","flow_id":2144573915774774,"pcap_cnt":21987,"event_type":
:"alert","src_ip":"XX.XX.XX.XX","src_port":XX,"dest_ip":"XX.XX.XX.XX","dest_port":XX,"prot
o":"TCP","alert":{"action":"allowed","gid":1,"signature_id":1111214,"rev":1,"signature":"S
CADA_IDS: DNP3 - Function Code Scan","category":"Attempted Information Leak","severity":2},
"app_proto":"dnp3","flow":{"pkts_toserver":18,"pkts_toclient":16,"bytes_toserver":1358,"by
tes_toclient":1864,"start":"2017-02-14T06:24:17.704310+0200"}}
```

Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{20 + 100}{20 + 100 + 0 + 0} = 1$$

$$True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{20}{20 + 0} = 1$$

$$True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{100}{100 + 0} = 1$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 100} = 0$$

$$F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 20}{2 \times 20 + 0 + 0} = 1$$

Therefore, based on these metrics, the following evaluation results are presented

Accuracy	TPR	TNR	FPR	F1
1	1	1	0	0

Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks

	or without the appropriate specification rules, then the detection results could present FP and FN.
Test Case Result	Achieved

Test Case ID	DNP3_Suricata_04	Component	Suricata (Sensor of XL-SIEM)
Description	<p>This unit test aims at detecting the DNP3 Enumerate attack, which is presented in subsection 2.4.2. A particular Suricata DNP3-related specification rule is used from subsection 2.4.4 and Annex 2. On the contrary, the DNP3-related network traffic data (pcap file) of [Pliatsios20] is used as the malicious DNP3-related network traffic.</p> <p>First, the configuration file of Suricata (/etc/suricata/suricata.yaml) was configured to consider the DNP3 keywords. Next, a specification rule related to the DNP3 Enumerate attack is specified in the configuration file (/etc/Suricata/rules/suricata.rules), which contains all specification rules of Suricata. Finally, the pcap file of [Pliatsios20] is analysed by Suricata, thereby detecting the relevant attack.</p>		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	Medium
Prepared by	OINF	Tested by	OINF
Pre-condition(s)	-		
Test steps			
1	<p>The configuration file of Suricata (/etc/suricata/suricata.yaml) was edited to consider the DNP3 keywords. More precisely, in the /etc/suricata/suricata.yaml file, the lines related to the DNP3 keywords were uncommented, as depicted in the following figure.</p> <div><pre>944 # DNP3 945 dnp3: 946 enabled: yes 947 detection-ports: 948 dp: 20000 949</pre></div> <p>Figure 30. Activation of the DNP3 keywords of Suricata for test case DNP3_Suricata_04</p>		
2	<p>The following Suricata specification rule was used to detect the DNP3 Enumerate attack, which is presented in subsection 2.4.2.</p> <pre>alert tcp \$DNP3_SERVER 20000 -> any any (flow:established; content:" 81 "; offset:12; depth:1; pcre:"/[\S\s]{1}(\x01)/iAR"; msg:"SCADA_IDS: DNP3 - Function Code Scan"; threshold: type threshold, track by_src, count 3, seconds 60; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-recon; sid:1111214; rev:1; priority:2;)</pre>		

- 3 The pcap (malicious_pcap.pcap) of [Pliatsios20] is parsed by Suricata, utilising the following command.

```
sudo suricata -c /etc/suricata/suricata.yaml -r malicious_pcap.pcap
```

Input data

A pcap file (malicious_pcap.pcap) of [Pliatsios20]. The following figure illustrates a sample of this pcap file. In particular, this pcap file (malicious_pcap.pcap) includes 40 packets related to DNP3 Enumerate attack and 100 normal DNP3 packets.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	198	197	TCP	74	36639 → 20000 [SYN] Seq=0 Win=29200 Len=0 MSS=
2	0.000043	197	198	TCP	74	20000 → 36639 [SYN, ACK] Seq=0 Ack=1 Win=2896
3	0.000294	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len
4	0.000629	197	198	DNP 3.0	83	Unsolicited Response
5	0.000893	198	197	TCP	66	36639 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len
6	0.003323	198	197	DNP 3.0	93	Read, Class 0123
7	0.003338	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=28 Win=29056 L
8	0.003947	198	197	DNP 3.0	81	Confirm
9	0.003965	197	198	TCP	66	20000 → 36639 [ACK] Seq=18 Ack=43 Win=29056 L
10	0.004188	197	198	DNP 3.0	358	from 10 to 1, len=255, Unconfirmed User Data
11	0.043865	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=310 Win=30336
12	0.043903	197	198	DNP 3.0	106	Response
13	0.044150	198	197	TCP	66	36639 → 20000 [ACK] Seq=43 Ack=350 Win=30336

Figure 31. Pcap of [Pliatsios20] for test case DNP3_Suricata_04

Result

The DNP3 Info attack was detected successfully by Suricata. The detection results are stored in the eve.json file. The corresponding alert produced by Suricata is depicted below.

```
{"timestamp": "2017-02-14T06:24:28.538383+0200", "flow_id": "2144573915774774", "pcap_cnt": "21987", "event_type": "alert", "src_ip": "XX.XX.XX.XX", "src_port": "XX", "dest_ip": "XX.XX.XX.XX", "dest_port": "XX", "proto": "TCP", "alert": {"action": "allowed", "gid": "1", "signature_id": "1111214", "rev": "1", "signature": "SCADA_IDS: DNP3 - Function Code Scan", "category": "Attempted Information Leak", "severity": "2"}, "app_proto": "dnp3", "flow": {"pkts_toserver": "18", "pkts_toclient": "16", "bytes_toserver": "1358", "bytes_toclient": "1864", "start": "2017-02-14T06:24:17.704310+0200"}}
```

Based on the aforementioned terms (TN, TP, FP and FN), the following metrics are defined.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{40 + 100}{40 + 100 + 0 + 0} = 1$$

$$True\ Positive\ Rate\ (TPR) = \frac{TP}{TP + FN} = \frac{40}{40 + 0} = 1$$

$$True\ Negative\ Rate\ (TNR) = \frac{TN}{TN + FP} = \frac{100}{100 + 0} = 1$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} = \frac{0}{0 + 100} = 0$$

$$F1 = \frac{2TP}{2TP + FP + FN} = \frac{2 \times 40}{2 \times 40 + 0 + 0} = 1$$

Therefore, based on these metrics, the following evaluation results are presented

Accuracy	TPR	TNR	FPR	F1
1	1	1	0	0

Since the appropriate specification rules were defined correctly and Suricata is a signature/specification-based intrusion detection and prevention system, the detection results are accurate completely. However, in the case of zero-day attacks

	or without the appropriate specification rules, then the detection results could present FP and FN.
Test Case Result	Achieved

4.4 IEC 61850 Unit Tests – STB-Aware

This subsection intends to examine up to what extent the IEC 61850 detection tool described in **Error! Reference source not found.** is able to detect any undesired MMS message (report and request) that should not be present in the substation. The result of the tests is evaluated according to the substation electric topology, as well as the logical nodes (and devices) which control the switchgear. Therefore, all tests are divided into two steps. In the first one, the sclCrawler extracts the substation information and is dumped in a file, which can be restricted or not by the substation engineer. In the second step, the detection tool is listening to the communications channels in order to detect any MMS not present in the file.

As explained in **Error! Reference source not found.**, the SCL interpreter output is a file whose data model must be interpretable in by the detection tool. Therefore, the file structure depends on the detection engine and the way this engine loads the data when generating rules. In the tests, the sclCrawler writes the file in XML files, where reports and request are dumped in XML CDATA sections. The detection tool is a Suricata, which reads the file and runs a LUA script upon MMS (port 102), launching an alert whenever a request is not present in the CDATA sections.

Test Case ID	61850_SBT_Config	Components	sclCrawler
Description	This unit test extracts the allowed MMS messages that can be present in the substation. Although it is not a detection test case, the aim of this test is just extract information and check whether the reports, nodes, functions, etc. is present in the output file.		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	Medium
Prepared by	Tecnia	Tested by	Tecnia
Pre-condition(s)	- Example of SCL extracted from TC 57 group for integration testing (21 IEDs)		
Test steps			
1	Run the sclCrawler with the substation file: IOP_2019_HV_2.scd: java -jar sclCrawler.jar -all dump.txt IOP_2019_HV_2.scd		
2	Open the output file dump.txt to see the nodes.		
3	Check that the <ipaddresses> has 21 elements, whose names are the IED_name in the SCL file and with the correct IPs.		

4	Check that <services> contains 21 elements with all the services for each IED.
5	Check that <reportSettingsService> only contains IEDs with configured reports (16 elements) with all the settings for them.
6	Check that <GOOSE> contains all GOOSEs identifications, which IED generates it and, when available, which IEDs consume them.
7	Check that <Report> contains all reports clasified by IED
8	Check that <LNnodesObj> contains all texts that can be present in a MMS communication (including bay, node names, variable and functional constraint)
Input data	The proper substation configuration (SCD) file: IOP_2019_HV_2.scd
Result	<p>An XML file containing all data:</p> <pre> <ipaddresses> <BUS_PU_SEL_487B>22 ... </BUS_PU_SEL_487B><TXA_MU2_GE_320>33 ... < 2_BCU_OMI_SSC>31 </L2_BCU_OMI_SSC><TXA_PU1_SEL_487E>10.11.17.21 </TXA_PU1_SEL_487E> </ipaddresses> <services> <BUS_PU_SEL_487B>"ClientServices" "DynAssociation" "GetDirectory" "GetDataObjectDefinition" "D vices" </TXA_BCU_TMW_DTM><TXB_PU2_ABB_670>"FileHandling" "GetDataSetValue" "GetDirectory" "Dat DataSet" "ReadWrite" "ConfReportControl" "GetCBValues" "ReportSettings" "ConflNs" "GOOSE" "Fil nAssociation" "SettingGroups" "GetDirectory" "GetDataObjectDefinition" "DataObjectDirectory" " Settings" "GSESettings" "ConflNs" "ConflName" "GOOSE" "FileHandling" "SupSubscription" "Value ettings" "GSESettings" "ConflNs" "GOOSE" "FileHandling" "RedProt" "SettingGroups" "SMVSettings </services> <reportSettingsService> <BUS_PU_SEL_487B>bufTime="Dyn" cbName="Conf" dataSet="Conf" intgPd="Dyn" optFields="Dyn" resvTm OMI_SSC><L2_PU_GE_P443>bufTime="Dyn" cbName="Fix" dataSet="Conf" intgPd="Dyn" optFields="Dyn" o trgOps="Dyn" </TXB_MU1_BCU_SEL_401><L2_BCU_OMI_SSC>bufTime="Dyn" dataSet="Dyn" intgPd="Dyn" opt </reportSettingsService> <gseSettingsService> <BUS_PU_SEL_487B>appID="Conf" cbName="Conf" dataSet="Conf" </BUS_PU_SEL_487B><TXA_MU2_GE_320>ap "Conf" dataLabel="Fix" kdaParticipant="false" </L1_MU_SIE_7S3><TXB_MU3_VIZ_PMU>appID="Conf" </ </gseSettingsService> <GOOSE> <L2_MU_SCU_VIZ_MGUSYS/LLN0\$G0\$gcb01 from="L2_MU_SCU_VIZ_MGU">(name="gcb01" dataSet="TxGOOSE_Phy </L2_MU_SCU_VIZ_MGUSYS/LLN0\$G0\$gcb01> <L2_MU_SCU_VIZ_MGUSYS/LLN0\$G0\$gcb02 from="L2_MU_SCU_VIZ_MGU">(name="gcb02" dataSet="TxGOOSE_CB1 L2_BCU_OMI_SSC L2_PU_GE_P443 BUS_PU_SEL_487B </L2_MU_SCU_VIZ_MGUSYS/LLN0\$G0\$gcb02> <L2_PU_GE_P443System/LLN0\$G0\$gcb01 from="L2_PU_GE_P443">(name="gcb01" dataSet="dataset1" type=" L1_BCU_SIF_200E TXA_MU1_SCU_VIZ_MGU TXB_MU1_BCU_SEL_401 RSS_BCU_OMI_SSC </L2_PU_GE_P443System/LLN0\$G0\$gcb01> <L2_PU_GE_P443System/LLN0\$G0\$gcb02 from="L2_PU_GE_P443">(name="gcb02" dataSet="dataset2" type=" </pre> <p>Figure 32. sclCrawler output (XML containing CDATA for MMS)</p>
Test Case Result	Achieved

Test Case ID	61850_IED_Sniffing	Components	Suricata (Sensor of XL-SIEM) adapted for LUA scripting
---------------------	--------------------	-------------------	--

Description	This unit test aims at detecting an MMS message trying to request for a control switch that is not configured, and therefore not present in the sclCrawler output file.		
Spec ID	SPEC-F1, SPEC-F2, SPEC-F3, SPEC-F4	Priority	Medium
Prepared by	Tecnalia	Tested by	Tecnalia
Pre-condition(s)	- A real IED, installed in a substation with a mirror port for attack detection		
Test steps			
1	Run the sclCrawler with the CID file: L1.scd: java -jar sclCrawler.jar -all substrings_192_168_2_11.txt 11.cid		
2	Open the output file substrings_192_168_2_11.txt to see the nodes and delete the data which shows the physical node state LPHD1.PhyHealth: <pre>L1CTRL/LLN0\$ST\$EstLocTel\$opOpnOr L1CTRL/LLN0\$ST\$EstLocTel\$opClsOr L1CTRL/LLN0\$CF\$EstLocTel\$ctlModel L1CTRL/LLN0\$CF\$EstLocTel\$sboTimeout L1CTRL/LLN0\$CF\$EstLocTel\$sboClass L1CTRL/LLN0\$CF\$EstLocTel\$pulseConfig L1CTRL/LLN0\$CF\$EstLocTel\$operTimeout L1CTRL/LPHD1\$DC\$PhyNam\$vendor L1CTRL/LPHD1\$DC\$PhyNam\$hwRev L1CTRL/LPHD1\$DC\$PhyNam\$swRev L1CTRL/LPHD1\$DC\$PhyNam\$serNum L1CTRL/LPHD1\$DC\$PhyNam\$model L1CTRL/LPHD1\$DC\$PhyNam\$d L1CTRL/LPHD1\$ST\$PhyHealth\$stVal L1CTRL/LPHD1\$ST\$PhyHealth\$q L1CTRL/LPHD1\$ST\$PhyHealth\$t L1CTRL/LPHD1\$DC\$PhyHealth\$d L1CTRL/LPHD1\$ST\$Proxy\$stVal L1CTRL/LPHD1\$ST\$Proxy\$q L1CTRL/LPHD1\$ST\$Proxy\$t L1CTRL/LPHD1\$DC\$Proxy\$d</pre>		
Figure 33. Extract from sclCrawler otuput for bay 1 CID file			
3	Configure Suricata to import substrings_192_168_2_11.txt		

```

--if #a > 1 then
if #a >= 50 and #a <= 120 then
--if a:find("RCB_SIGNALS") or a:find("RCB_SIGNALS") then
if a:find("RCB_SIGNALS_TEST") or
a:find("RCB_SIGNALS_HMI") or a:find("RCB_SIGNALS_RIU") or
a:find("RCB_MEASURES_HMI") or a:find("RCB_MEASURES_RIU") then
return 0
else
--print('leemos fichero')
local file = io.open("substrings_192_168_2_11.txt")
local tblines = {}
local i = 0
if file then
for line in file:lines() do
i = i + 1
tblines[i] = line
end
file:close()
else
error('file not found')
print('file substrings_192_168_2_11.txt not found')
end
--print ('fichero leido')
for key,value in ipairs(tblines)
do
if a:find(value) then
--print('ENCONTRADO', key, value)
return 0
end
end
end
print (#a)
print (a)
return 1
end

```

Figure 34. LUA script to add substation specific information


4	Connect Suricata to a switch mirror port connected to the bay 1 IED
5	Configure Suricata only to watch the bay 1: TCP, XX.XX.XX.11, port YY2
6	Apply substation rules for bay1: alert tcp any any -> XX.XX.XX.11 YY2 (msg:"Accessed variable not in configuration "; luajit:script1.lua; sid:101010; rev:1;)
7	Check that an alert is launched only when the SCADA checks the bay 1
Input data	<p>The configured IED for the substation (CID) file for bay 1: L1.cid</p> <p>The LUA script: IED for the substation (CID) file for bay 1: script1.lua</p> <p>Real substation on-line traffic (mirror port connected to the Suricata)</p>
Result	<p>An alert is launched when the SCADA tries to check the state:</p> 
Test Case Result	Achieved

Figure 35. Alert launched when checking the state

5 Innovation Summary

Table 6 summarizes the protocols that have been considered in this deliverable, mapped to the main attacks threatening these protocols and linked to the attacks tools used in SDN-microSENSE. The information contained in this table also summarizes the main innovations carried in this task, which are related to the detection of incidents associated to widely used EPES protocols, both using standard rule based approaches (as described in this document) or machine learning based (as described in D5.3 [SDN53])

Table 6. Summary of protocols attacks and tools involved

Protocol	Attacks Category	Attack description	Attacker tool	Available datasets	Attack detector
IEC 61850	DoS	Flood made-up GOOSE frames to congest the substation network.	Ettercap https://www.ettercap-project.org/	IEC61850 Security Dataset (https://github.com/smartgrid4sc/IEC61850SecurityDataset)	ML Model (T5.3)
					Tecnia tool (T5.2)
	Message Suppression	Man in the middle, session hijacking, Interception of information. A message suppression (MS) attack refers to the hijacking of the communication channel by modifying the GOOSE header fields to prevent legitimate IEDs from receiving critical messages or updates. (sqNum, stNum)	Scapy Script	IEC61850 Security Dataset (https://github.com/smartgrid4sc/IEC61850SecurityDataset)	ML Model (T5.3)
					Tecnia tool (T5.2)
	Data Injection	Unauthorised Access, Information leakage, Failure of devices and systems, Manipulation of information, Replay of messages. Data injection refers to the process of injecting	Scapy Script	IEC61850 Security Dataset (https://github.com/smartgrid4sc/IEC61850SecurityDataset)	ML Model (T5.3)
					Tecnia tool (T5.2)

		modified network payloads into the network to negatively impact the power grid stability or to mask unauthorized changes.			
IEC 60870-5-101/104	Network Reconnaissance and Information Gathering	Discovery: Attempts to identify IEC 60870-5-104 ICS protocol.	Nmap NSE	Not needed	Suricata (T5,2)
	DoS	DoS against IEC104 (m_sp_na_1_DoS)	IEC Server Simulator	UOWM IEC104 Dataset	Common ML Model provided (T5.3)
		DoS against IEC104 (c_ci_na_1_DoS)	Bash script based on Metasploit	UOWM IEC104 Dataset	Common ML Model provided (T5.3)
		DoS against IEC104 (c_se_na_1_DoS)	Bash script based on Metasploit	UOWM IEC104 Dataset	Common ML Model provided (T5.3)
		DoS against IEC104 (c_sc_na_1_DoS)	Bash script based on Metasploit	UOWM IEC104 Dataset	Common ML Model provided (T5.3)
	Unauthorised Access, Information leakage, Failure of devices and systems, Manipulation of information	Malicious IEC104 command (c_ci_na_1)	Metasploit, Bash script based on Metasploit	UOWM IEC104 Dataset	Common ML Model provided (T5.3)
		Malicious IEC 104 (c_se_na_1)	Metasploit, Bash script based on Metasploit	UOWM IEC104 Dataset	Common ML Model provided (T5.3)
		Malicious IEC 104 (c_sc_na_1)	Metasploit, Bash script	UOWM IEC104 Dataset	Common ML Model provided (T5.3)

			based on Metasploit		
DNP3	Network Reconnaissance and Information Gathering	dnp3-enumerate: This attack enumerates those assets using DNP3	Nmap NSE	Not needed	Suricata (T5.2)
		dnp3-info This attack sends a command to query through the first 100 addresses of DNP3 to see if a valid response is given. If a valid response is given it will then parse the results based on function ID and other data.	Nmap NSE	Not needed	Suricata (T5.2)
	Unauthorised Access, Failure of devices and systems, Manipulation of information	DNP3 Disable Unsolicited Messages Attack: The attacker implements this attack by first initiating a connection with the outstation node (the victim) posing as the Master node. He then sends a message with function code 21 (disable unsolicited messages) to the outstation requesting the outstation to disable all unsolicited messages. At this point the outstation will not be able to send any alarming messages to the Master in case there is a failure or abnormal operation in the outstation node.	OpenDNP3	UOWM DNP3 Dataset	Common ML Model provided (T5.3)
		DNP3 Cold Restart Message Attack: When DNP3 Cold Restart request command is received by the outstation and the packet is confirmed to have originated from the master, the outstation then performs a full restart on completion of the communications sequence. The outstation will also send a reply to the master with the time the outstation is available before restarting. This attack involves sending a command	OpenDNP3	UOWM DNP3 Dataset	Common ML Model provided (T5.3)

		called Cold Restart to an outstation which causes the outstation to restart completely			
		DNP3 Warm Restart Message Attack	OpenDNP3	UOWM DNP3 Dataset	Common ML Model provided (T5.3)
Modbus	DoS	modbus/dos/writeSingleCoils:	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/dos/writeSingleCoils attack is a DoS which send continuously malicious Modbus packets (function code 5) to the target system.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		modbus/dos/writeSingleRegister:	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/dos/writeSingleRegister is a DoS attack, which sends continuously malicious Modbus packets (function code 06) to the target system.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
	Unauthorised Access, Failure of devices and systems, Manipulation of information:	modbus/function/writeSingleCoils	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/function/writeSingleCoils aims to change the value of a coil.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		modbus/function/writeSingleRegister	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/function/write Single Register attack changes the values of a single holding register.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
	UID brute force attack against PV/Battery inverters' RPI Unauthorised Access, Failure of devices and systems, Manipulation of information		Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)

	Unauthorised Access, Information leakage	modbus/function/readCoils	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/function/readCoils attack reads the value of a specific coil.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		modbus/function/readDiscreteInput	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/function/readDiscreteInput can extract the values of the discrete inputs supported by the target.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		modbus/function/readHoldingRegister	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/function/readHoldingRegister can return the values of the holding registers supported by the target system.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		modbus/function/readInputRegister	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		The modbus/function/readInputRegister reads the values of the input registers.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
	Network Reconnaissance and Information Gathering	modbus/scanner/getfunc	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		This attack discovers the functions codes supported by the target system.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		modbus/scanner/uidc	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)
		This attack enumerates the UIDs supported by the target system.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		modbus/scanner/discover	UOWM Smod	UOWM Modbus Dataset	Common ML Model provided (T5.3)

		This attack identifies if Modbus runs in the target system.	Smod	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
	Network Reconnaissance and Information Gathering	auxiliary/scanner/scada/modbusclient This attack exploits a Modbus vulnerability that allows to an unauthorized actor to read or write against the Modbus slave targeted	Metasploit	Not needed	Suricata (T5.2)
MQTT	DoS	DoS attacks against MQTT broker: Connect flood Attacker sends multiple connection messages to exhaust server resources	Python scripts	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		DoS attacks against MQTT broker: Large payload attack Attacker publishes spam messages repeatedly to a specific topic, legitimate users cannot publish	Python scripts	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
	Man in the middle	MITM attack against gateways Attacker intercepts the communications, filters and dumper the measurements send/received by gateway	Python scripts	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
	Unauthorised Access, Failure of devices and Systems, Manipulation of information	Unauthorized publishing to smart devices Attacker connects to the broker, subscribes to all topics and publish unauthorized commands	Python scripts	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)

BACnet	Unauthorised Access, Failure of devices and Systems, Manipulation of information	Fuzzing An attacker utilizes a python script in order to continuously send BACnet packets with different parameters each time in order to discover vulnerabilities.	Open source BACnet fuzzer from VDA Labs	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
	DoS	Reflected DoS – Flooding attack	BACnetstack 0.8.6	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
NTP	Time manipulation	Clock time skimming attack	Delorean	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
		Kiss of death packet elicitation attack	Scapy	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
Radius	Unauthorised Access, Failure of devices and Systems, Manipulation of information	Radius User-Password based password Attack. This attack assumes that the attacker has access to the Radius packets and is able to capture them and aims to crack a valid user's password by trying to authenticate with a known possibly wrong password and extracting information from the captured packets	Python script	CERTH SPEAR-Smart home Dataset	ML Model (T5.3)
no specific protocol	Ransomware	Ransomwares are the type of malwares that prevent or limit users from accessing their system or their files unless a ransom is paid. 18 Ransomware infection scenarios and 1 cryptomining infection scenario are examined.	RanSIM tool	CERTH FORTIKA Dataset	ML Model (T5.3)
no specific protocol	web based attacks	Cross Site Scripting (XSS), Bruteforce, Portscan	Kali Linux	CERTH FORTIKA Dataset	ML Model (T5.3)

HTTP 1.1	Unauthorized access	An unauthorized actor could request access to sensitive information (e.g. meter information)	No tool is expected to be developed	Not needed	Logs that could potentially indicate this are generated by the OPF (T5.4)
HTTP 2	Access bruteforcing	An attacker could try to bruteforce the system to find any potential vulnerability in the RBAC system that could lead to granting access to secured assets	No tool is expected to be developed	Not needed	Logs that could potentially indicate this are generated by the OPF (T5.4)
TLS 1.3/1.2	Anomaly on data request usage	An attacker that has successfully infiltrated in the network with valid credentials could try to dump all the database to perform exfiltration attacks	No tool is expected to be developed	Not needed	Logs that could potentially indicate this are generated by the OPF (T5.4)

6 Conclusions

This deliverable has presented the results of T5.2, focused on the detection of cyber incidents threatening protocols that are specific of the EPES domain. The protocols IEC61850, IEC60870-5-101/104, Modbus and DNP3 are described in detail, also detailing the main attacks they are exposed to. This deliverable also presents the results of the mechanisms developed to detect those attacks, describing the techniques that are integrated in several of the tools that are also described in this deliverable.

More specifically, three tools are described in this deliverable, which incorporates the mechanisms developed to detect cyber incidents in the EPES domain. One of them, Nightwatch, is an SDN based IDPS, which uses information retrieved from SDN controllers to detect anomalies and trigger events collected by the XL-EPDS for its correlation, as it is described in D5.1. The other two tools (Suricata and SBT Aware) monitors network traffic and are based on rules. To this end, additional rules have been created to detect incidents associated to the protocols mentioned above. All of them reports their verdicts to the XL-EPDS, which interpret those events, correlates them and trigger the corresponding alerts in case of certain pattern matching (for example, two events from different tools associated to the same incident during certain a certain time window).

The results included in this deliverable are continued in T5.3 and T5.4, where additional tools are developed to detect some of the attacks listed here. More specifically, T5.3 focuses on the development of machine learning algorithms to detect cyber incidents, while T5.4 focuses on the detection of privacy-related incidents.

Therefore, the results described in this deliverable, together with the results of T5.3 and T5.4, are used as input for the components described in T5.1, which output is used as input for the components of T5.5, closing the loop of the cyber incident detection platform included in SDN-microSENSE and developed in WP5.

7 References

- [Bhatia14] S. Bhatia, N. Kush, C. Djameludin, A. Akande, and E. Foo, “Practicalmodbus flooding attack and detection,” in Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014) [Conferences in Research and Practice in Information Technology, Volume 149]. Australian Computer Society, Inc., 2014, pp. 57–65.
- [Bristow08] M. Bristow, “Modscan: a scada modbus network scanner,” in DefCon-16 Conf., Las Vegas, NV, 2008.
- [Clarke04] G. Clarke, D. Reynodes and E. Wright, *Practical modern SCADA protocols*. London, Elsevier, 2004.
- [East09] S. East, J. Butts, M. Papa, S. Sheno, A taxonomy of attacks on the dnp3 protocol”, in: C. Palmer, S. Sheno (Eds.), *Critical Infrastructure Protection III*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, pp.67–81.
- [Huitsing08] P. Huitsing, R. Chandia, M. Papa, and S. Sheno, “Attack taxonomies for the modbus protocols,” *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, 12 2008.
- [IEC60870-104] Introduction to the IEC 60870-5-104 standard. Available at <https://www.ensotest.com/iec-60870-5-104/introduction-to-the-iec-60870-5-104-standard> [Accessed Sep 2020].
- [IEC61850] Introduction to the IEC 61850 standard. Available at <https://www.ensotest.com/iec-61850/introduction-to-iec-61850-protocol/> [Accessed Sep 2020].
- [IEC62351] IEC TS 62351-1. TECHNICAL SPECIFICATION. Power systems management and associated information exchange – Data and communications security. Part 1: Communication network and system security – Introduction to security issues. 2007.
- [IECTC57] IEC TC57 WG15. IEC 62351 Security Standards for the Power System Information Infrastructure, Feb 2016
- [Igbe17] O. Igbe, I. Darwish and T. Saadawi, "Deterministic Dendritic Cell Algorithm Application to Smart Grid Cyber-Attack Detection", 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017. Available: 10.1109/csccloud.2017.12 [Accessed Sep 2020].
- [Kabir16] Kabir-Querrec, Maëlle, et al. "A test bed dedicated to the study of vulnerabilities in IEC 61850 power utility automation networks." 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2016.
- [Modbus15] Modbus-IDA, “Modbus application protocol specification v1. 1b3,” 2015
- [Nyasore20] O. N. Nyasore, P. Zavorsky, B. Swar, R. Naiyeju and S. Dabra, "Deep Packet Inspection in Industrial Automation Control System to Mitigate Attacks Exploiting Modbus/TCP Vulnerabilities," 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 2020, pp. 241-245, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00051.

- [Pliatsios20] D. Pliatsios, P. Sarigiannidis, T. Lagkas and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1942-1976, thirdquarter 2020, doi: 10.1109/COMST.2020.2987688.
- [Radoglou-Grammatikis19] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis and E. Panaousis, "Attacking IEC-60870-5-104 SCADA Systems," 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019, pp. 41-46, doi: 10.1109/SERVICES.2019.00022.
- [Radoglou-Grammatikis20] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.-A. Karypidis, and A. Sarigiannidis, "Diderot: An intrusion detection and prevention system for dnp3-based scada systems," in Proceedings of the 15th International Conference on Availability, Reliability and Security, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020.
- [Radoglou-Grammatikis20+1] P. Radoglou-Grammatikis, I. Siniosoglou, T. Liatifis, A. Korouniadis, K. Rompoulos, P. Sarigiannidis, 'Implementation and Detection of Modbus Cyberattacks: A Case Study', Proceedings of 10th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2020.
- [SDN22] SDN-microSENSE Deliverable D2.2. User & Stakeholder, Security and Privacy Requirements 2020
- [SDN23] SDN-microSENSE Deliverable D2.3 Platform Specifications and Architecture. 2020
- [SDN24] SDN-microSENSE Deliverable D2.4 Pilot, Demonstration & Evaluation Strategy. 2020
- [SDN33] SDN-microSENSE Deliverable D3.3 EPES Honeypots. 2020
- [SDN51] SDN-microSENSE Deliverable D5.1 XL-SIEM System. 2020
- [SDN53] SDN-microSENSE Deliverable D5.3 ADS and CLS Discovery Systems. 2020
- [SDN54] SDN-microSENSE Deliverable D5.4. Overlay Privacy Framework. 2020
- [SDN55] SDN-microSENSE Deliverable D5.4. Cloud-based Anonymous Repository of Incidents. 2020
- [Voyiatzis15] A. G. Voyiatzis, K. Katsigiannis, and S. Koubias, "A modbus/tcpfuzzer for testing internetworked industrial systems," in 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA). IEEE, 2015, pp. 1–6.
- [Wong17] K. Wong, C. Dillabaugh, N. Seddigh and B. Nandy, "Enhancing Suricata intrusion detection system for cyber security in SCADA networks," 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, 2017, pp. 1-5, doi: 10.1109/CCECE.2017.7946818.
- [Yang17] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono and H. F. Wang, "Intrusion Detection System for IEC 60870-5-104 based SCADA networks," 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1-5, doi: 10.1109/PESMG.2013.6672100.

Annex I: IEC104 Suricata Signature/Specification Rules

The following table lists the new rules created for Suricata to detect IEC104 related attacks.

1	alert tcp \$HOME_NET any -> \$EXTERNAL_NET 2404 (msg:"PROTOCOL-SCADA IEC 104 traffic to/from EXTERNAL_NET"; flow:established; content:" 68 "; depth:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41079; rev:4;)
2	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 2404 (msg:"PROTOCOL-SCADA IEC 104 traffic to/from EXTERNAL_NET"; flow:established; content:" 68 "; depth:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41078; rev:4;)
3	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 unknown ASDU type detected"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x16-\x1D\x29-\x2C\x34-\x39\x41-\x45]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41077; rev:4;)
4	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 double command issued"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x2e\x3b]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41076; rev:4;)
5	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 counter interrogation command"; flow:established; content:" 68 "; content:" 65 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41075; rev:4;)
6	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 clock sync command"; flow:established; content:" 68 "; content:" 67 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41074; rev:4;)
7	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 bitstring of 32 bits"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x33\x40\x07\x21]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41073; rev:4;)
8	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Test command with time tag"; flow:established; content:" 68 "; content:" 6B "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41072; rev:4;)
9	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Step point information"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x05\x20]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41071; rev:4;)
10	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Single point information"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x14\x01\x1e]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41070; rev:4;)

11	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Single command"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x2d\x3a]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41069; rev:4;)
12	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Set point command"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x30\x31\x32\x3d\x3e\x3f]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41068; rev:4;)
13	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Rest process command"; flow:established; content:" 68 "; content:" 69 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41067; rev:4;)
14	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Regulating step command"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x2f\x3c]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41066; rev:4;)
15	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Read command"; flow:established; content:" 68 "; content:" 66 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41065; rev:4;)
16	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Query Log"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x7a\x7f]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41064; rev:4;)
17	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Parameter value"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x71\x6e\x6f\x70]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41063; rev:4;)
18	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Packed start events"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x26\x27\x28]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41062; rev:4;)
19	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Measured value"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x09\x0b\x0d\x15\x22\x23\x24]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41061; rev:4;)
20	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 List directory"; flow:established; content:" 68 "; content:" 7E "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41060; rev:6;)
21	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Last section"; flow:established; content:" 68 "; content:" 7B "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41059; rev:4;)

22	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Interrogation command"; flow:established; content:" 68 "; content:" 64 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41058; rev:4;)
23	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Integrated totals"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x0f\x25]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41057; rev:4;)
24	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 File ready"; flow:established; content:" 68 "; content:" 78 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41056; rev:4;)
25	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 End of initialization"; flow:established; content:" 68 "; content:" 46 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41055; rev:4;)
26	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Double point information"; flow:established; content:" 68 "; pcre:"/\x68.{5}[\x03\x1f]/"; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41054; rev:4;)
27	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 Ack file"; flow:established; content:" 68 "; content:" 7C "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41053; rev:4;)
28	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 TESTFR CON"; flow:established; content:" 68 "; depth:1; content:" 83 "; within:1; distance:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41052; rev:4;)
29	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 TESTFR ACT"; flow:established; content:" 68 "; depth:1; content:" 43 "; within:1; distance:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41051; rev:4;)
30	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STOPDT CON"; flow:established; content:" 68 "; depth:1; content:" 23 "; within:1; distance:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41050; rev:4;)
31	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STOPDT ACT"; flow:established; content:" 68 "; depth:1; content:" 13 "; within:1; distance:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41049; rev:4;)
32	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STARTDT CON"; flow:established; content:" 68 "; depth:1; content:" 0B "; within:1; distance:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41048; rev:4;)



33	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 STARTDT ACT"; flow:established; content:" 68 "; depth:1; content:" 07 "; within:1; distance:1; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:41047; rev:4;)
34	alert tcp \$EXTERNAL_NET 102 -> \$HOME_NET any (msg:"PROTOCOL-SCADA IEC 61850 virtual manufacturing device domain variable enumeration attempt"; flow:to_client,established,no_stream; content:" 61 "; content:" 03 "; within:1; distance:5; content:" A0 03 80 01 00 A1 "; distance:0; content:" 81 "; within:1; distance:1; detection_filter:track by_src,count 10,seconds 15; metadata:policy max-detect-ips drop; reference:url,dragos.com/blog/crashoverride/CrashOverride-01.pdf; reference:url,us-cert.gov/ncas/alerts/TA17-163A; reference:url,welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf; classtype:attempted-recon; sid:43253; rev:3;)
35	alert tcp \$EXTERNAL_NET 102 -> \$HOME_NET any (msg:"PROTOCOL-SCADA IEC 61850 device connection enumeration attempt"; flow:to_client,established,no_stream; content:" E0 00 00 "; depth:3; offset:5; content:" 00 "; within:1; distance:2; content:" C1 "; depth:9; offset:11; content:" C2 "; depth:9; offset:11; content:" C0 "; depth:9; offset:11; detection_filter:track by_src,count 10,seconds 15; metadata:policy max-detect-ips drop; reference:url,dragos.com/blog/crashoverride/CrashOverride-01.pdf; reference:url,us-cert.gov/ncas/alerts/TA17-163A; reference:url,welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf; classtype:attempted-recon; sid:43252; rev:3;)
36	alert tcp \$EXTERNAL_NET 2404 -> \$HOME_NET any (msg:"PROTOCOL-SCADA IEC 104 force on denial of service attempt"; flow:to_client,established,no_stream; content:" 68 "; depth:1; content:" 2D "; within:1; distance:5; content:" 01 "; within:1; distance:8; detection_filter:track by_src,count 50,seconds 5; reference:url,dragos.com/blog/crashoverride/CrashOverride-01.pdf; reference:url,us-cert.gov/ncas/alerts/TA17-163A; reference:url,welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf; classtype:attempted-dos; sid:43228; rev:4;)
37	alert tcp \$EXTERNAL_NET 2404 -> \$HOME_NET any (msg:"PROTOCOL-SCADA IEC 104 force off denial of service attempt"; flow:to_client,established,no_stream; content:" 68 "; depth:1; content:" 2D "; within:1; distance:5; content:" 00 "; within:1; distance:8; detection_filter:track by_src,count 50,seconds 5; reference:url,dragos.com/blog/crashoverride/CrashOverride-01.pdf; reference:url,us-cert.gov/ncas/alerts/TA17-163A; reference:url,welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf; classtype:attempted-dos; sid:43227; rev:4;)
38	alert udp \$EXTERNAL_NET any -> \$HOME_NET 50000 (msg:"PROTOCOL-SCADA Siemens SIPROTEC V4.24 crafted packet denial of service attempt"; flow:to_server; content:" 11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E "; depth:18; metadata:policy max-detect-ips drop; reference:cve,2015-5374; reference:url,siemens.com/cert/pool/cert/siemens_security_advisory_ssa-732541.pdf; classtype:attempted-dos; sid:43177; rev:2;)



39	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_SC_NB_1"; flow:established; content:" 68 "; depth:1; content:" 7F "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52203; rev:1;)
40	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_DR_TA_1"; flow:established; content:" 68 "; depth:1; content:" 7E "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52202; rev:1;)
41	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_SG_NA_1"; flow:established; content:" 68 "; depth:1; content:" 7D "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52201; rev:1;)
42	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_LS_NA_1"; flow:established; content:" 68 "; depth:1; content:" 7B "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52200; rev:1;)
43	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_SC_NA_1"; flow:established; content:" 68 "; depth:1; content:" 7A "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52199; rev:1;)
44	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_SR_NA_1"; flow:established; content:" 68 "; depth:1; content:" 79 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52198; rev:1;)
45	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 P_AC_NA_1"; flow:established; content:" 68 "; depth:1; content:" 71 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52197; rev:1;)
46	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_FR_NA_1"; flow:established; content:" 68 "; depth:1; content:" 78 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52196; rev:1;)
47	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 F_AF_NA_1"; flow:established; content:" 68 "; depth:1; content:" 7C "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52195; rev:1;)
48	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 P_ME_NC_1"; flow:established; content:" 68 "; depth:1; content:" 70 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52194; rev:1;)
49	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_RP_NA_1"; flow:established; content:" 68 "; depth:1; content:" 69 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-

	detection-rules.html; classtype:protocol-command-decode; sid:52193; rev:1;)
50	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_CS_NA_1"; flow:established; content:" 68 "; depth:1; content:" 67 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52192; rev:1;)
51	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_IC_NA_1"; flow:established; content:" 68 "; depth:1; content:" 64 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52191; rev:1;)
52	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_RD_NA_1"; flow:established; content:" 68 "; depth:1; content:" 66 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52190; rev:1;)
53	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_CI_NA_1"; flow:established; content:" 68 "; depth:1; content:" 65 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52189; rev:1;)
54	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 P_ME_NB_1"; flow:established; content:" 68 "; depth:1; content:" 6F "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52188; rev:1;)
55	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 P_ME_NA_1"; flow:established; content:" 68 "; depth:1; content:" 6E "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52187; rev:1;)
56	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_TS_TA_1"; flow:established; content:" 68 "; depth:1; content:" 6B "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52186; rev:1;)
57	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_EI_NA_1"; flow:established; content:" 68 "; depth:1; content:" 46 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52185; rev:1;)
58	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_BO_TA_1"; flow:established; content:" 68 "; depth:1; content:" 40 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52184; rev:1;)
59	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SE_TC_1"; flow:established; content:" 68 "; depth:1; content:" 3F "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52183; rev:1;)

60	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SE_TB_1"; flow:established; content:" 68 "; depth:1; content:" 3E "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52182; rev:1;)
61	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SE_TA_1"; flow:established; content:" 68 "; depth:1; content:" 3D "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52181; rev:1;)
62	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_RC_TA_1"; flow:established; content:" 68 "; depth:1; content:" 3C "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52180; rev:1;)
63	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_DC_TA_1"; flow:established; content:" 68 "; depth:1; content:" 3B "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52179; rev:1;)
64	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SC_TA_1"; flow:established; content:" 68 "; depth:1; content:" 3A "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52178; rev:1;)
65	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_BO_NA_1"; flow:established; content:" 68 "; depth:1; content:" 33 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52177; rev:1;)
66	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SE_NC_1"; flow:established; content:" 68 "; depth:1; content:" 32 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52176; rev:1;)
67	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SE_NB_1"; flow:established; content:" 68 "; depth:1; content:" 31 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52175; rev:1;)
68	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SE_NA_1"; flow:established; content:" 68 "; depth:1; content:" 30 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52174; rev:1;)
69	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_RC_NA_1"; flow:established; content:" 68 "; depth:1; content:" 2F "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52173; rev:1;)
70	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_DC_NA_1"; flow:established; content:" 68 "; depth:1; content:" 2E "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-

	detection-rules.html; classtype:protocol-command-decode; sid:52172; rev:1;)
71	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 C_SC_NA_1"; flow:established; content:" 68 "; depth:1; content:" 2D "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52171; rev:1;)
72	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_EP_TF_1"; flow:established; content:" 68 "; depth:1; content:" 28 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52170; rev:1;)
73	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_EP_TE_1"; flow:established; content:" 68 "; depth:1; content:" 27 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52169; rev:1;)
74	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_EP_TD_1"; flow:established; content:" 68 "; depth:1; content:" 26 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52168; rev:1;)
75	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_IT_TB_1"; flow:established; content:" 68 "; depth:1; content:" 25 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52167; rev:1;)
76	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ME_TF_1"; flow:established; content:" 68 "; depth:1; content:" 24 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52166; rev:1;)
77	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ME_TE_1"; flow:established; content:" 68 "; depth:1; content:" 23 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52165; rev:1;)
78	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_BO_TB_1"; flow:established; content:" 68 "; depth:1; content:" 21 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52164; rev:1;)
79	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ME_TD_1"; flow:established; content:" 68 "; depth:1; content:" 22 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52163; rev:1;)
80	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ST_TB_1"; flow:established; content:" 68 "; depth:1; content:" 20 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52162; rev:1;)

81	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_IT_NA_1"; flow:established; content:" 68 "; depth:1; content:" 0F "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52161; rev:1;)
82	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_SP_TB_1"; flow:established; content:" 68 "; depth:1; content:" 1E "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52160; rev:1;)
83	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_PS_NA_1"; flow:established; content:" 68 "; depth:1; content:" 14 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52159; rev:1;)
84	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ME_NC_1"; flow:established; content:" 68 "; depth:1; content:" 0D "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52158; rev:1;)
85	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_DP_TB_1"; flow:established; content:" 68 "; depth:1; content:" 1F "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52157; rev:1;)
86	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ME_ND_1"; flow:established; content:" 68 "; depth:1; content:" 15 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52156; rev:1;)
87	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ME_NB_1"; flow:established; content:" 68 "; depth:1; content:" 0B "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52155; rev:1;)
88	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ME_NA_1"; flow:established; content:" 68 "; depth:1; content:" 09 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52154; rev:1;)
89	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_BO_NA_1"; flow:established; content:" 68 "; depth:1; content:" 07 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52153; rev:1;)
90	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_ST_NA_1"; flow:established; content:" 68 "; depth:1; content:" 05 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52152; rev:1;)
91	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_DP_NA_1"; flow:established; content:" 68 "; depth:1; content:" 03 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-

	detection-rules.html; classtype:protocol-command-decode; sid:52151; rev:1;)
92	alert tcp any [1024:] <> any 2404 (msg:"PROTOCOL-SCADA IEC 104 M_SP_NA_1"; flow:established; content:" 68 "; depth:1; content:" 01 "; within:1; distance:5; reference:url,blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html; classtype:protocol-command-decode; sid:52150; rev:1;)

Annex II: Modbus/TCP Suricata Signature/Specification Rules

The following table lists the new rules created for Suricata to detect Modbus/TCP related attacks.

1	<pre> alert tcp \$MODBUS_CLIENT any -> \$MODBUS_SERVER 502 (flow:from_client,established; content:" 00 00 "; offset:2; depth:2; content:" 08 00 04 "; offset:7; depth:3; msg:"SCADA_IDS: Modbus TCP - Force Listen Only Mode"; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp- rules; classtype:attempted-dos; sid:1111001; rev:2; priority:1;) </pre>
2	<pre> alert tcp \$MODBUS_CLIENT any -> \$MODBUS_SERVER 502 (flow:from_client,established; content:" 00 00 "; offset:2; depth:2; content:" 08 00 01 "; offset:7; depth:3; msg:"SCADA_IDS: Modbus TCP - Restart Communications Option"; reference:url,digitalbond.com/tools/quickdraw/modbus- tcp-rules; classtype:attempted-dos; sid:1111002; rev:2; priority:1;) </pre>
3	<pre> alert tcp \$MODBUS_CLIENT any -> \$MODBUS_SERVER 502 (flow:from_client,established; content:" 00 00 "; offset:2; depth:2; content:" 08 00 0A "; offset:7; depth:3; msg:"SCADA_IDS: Modbus TCP - Clear Counters and Diagnostic Registers"; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; classtype:misc-attack; sid:1111003; rev:2; priority:3; </pre>
4	<pre> alert tcp \$MODBUS_CLIENT any -> \$MODBUS_SERVER 502 (flow:from_client,established; content:" 00 00 "; offset:2; depth:2; content:" 2B "; offset:7; depth:1; msg:"SCADA_IDS: Modbus TCP - Read Device Identification"; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp- rules; classtype:attempted-recon; sid:1111004; rev:2; priority:3;) </pre>
5	<pre> alert tcp \$MODBUS_CLIENT any <> \$MODBUS_SERVER 502 (flow:established; dsize:>300; msg:"SCADA_IDS: Modbus TCP - Illegal Packet Size, Possible DOS Attack"; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; classtype:non-standard-protocol; sid:1111008; rev:1; priority:1;) </pre>
6	<pre> alert tcp \$MODBUS_SERVER 502 <> \$MODBUS_CLIENT any (flow:established; byte_jump:2,4; isdataat:0,relative; msg:"SCADA_IDS: Modbus TCP - Incorrect Packet Length, Possible DOS Attack"; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; classtype:non- standard-protocol; sid:1111012; rev:1; priority:2;) </pre>
7	<pre> alert tcp \$MODBUS_SERVER 502 -> \$MODBUS_CLIENT any (flow:established; content:" 00 00 "; offset:2; depth:2; byte_test: 1, >=, 0x80, 7; content:" 01 "; offset:8; depth:1; msg:"SCADA_IDS: Modbus TCP - Function Code Scan"; threshold: type threshold, track by_src, count 3, seconds 60; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; classtype:attempted-recon; sid:1111014; rev:2; priority:2;) </pre>
8	<pre> alert tcp any any -> \$HOME_NET 27700 (msg:"ET SCADA SEIG Modbus 3.4 - Remote Code Execution"; flow:established,to_server; content:" 42 42 ff ff 07 03 44 00 64 "; fast_pattern; content:" 90 90 90 90 90 90 90 90 90 90 "; distance:0; metadata: former_category SCADA; reference:url,exploit-db.com/exploits/45220/; reference:cve,2013-0662; classtype:attempted-user; sid:2026005; rev:1; metadata:created_at 2018_08_21, updated_at 2018_08_21;) </pre>
9	<pre> alert tcp any any -> any 502 (msg:"ET SCAN Modbus Scanning detected"; content:" 00 00 00 00 00 02 "; flow:established,to_server; depth:6; threshold: </pre>



	type both, track by_src, count 100, seconds 10; reference:url,code.google.com/p/modscan/ reference:url,www.rtaautomation.com/modbustcp/ reference:url,doc.emergingthreats.net/2009286; classtype:bad-unknown; sid:2009286; rev:5; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
10	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA Modbus user-defined function code - 65 to 72"; flow:to_server,established; byte_test:1,>,64,7; byte_test:1,<,73,7; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15074; rev:5;)
11	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA Modbus user-defined function code - 100 to 110"; flow:to_server,established; byte_test:1,>,99,7; byte_test:1,<,111,7; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15075; rev:5;)
12	alert tcp \$EXTERNAL_NET 502 -> \$HOME_NET any (msg:"PROTOCOL-SCADA Modbus exception returned"; flow:established,to_client; byte_test:1,&,128,7; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15071; rev:4;)
13	alert tcp \$EXTERNAL_NET any -> \$HOME_NET \$HTTP_PORTS (msg:"PROTOCOL-SCADA Microsys Promotic directory traversal attempt"; flow:to_server,established; content:"/webdir/../../../../../../"; metadata:service http; reference:bugtraq,50133; reference:cve,2011-4518; reference:url,ics-cert.us-cert.gov/alerts/ICS-ALERT-11-286-01; classtype:attempted-user; sid:28917; rev:3;)
14	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA Modbus invalid encapsulated interface request"; flow:established,to_server; content:" 00 00 "; depth:2; offset:2; content:" 2B "; depth:1; offset:7; content:" 0D "; within:1; content:" 0E "; within:1; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:29319; rev:1;)
15	alert tcp \$EXTERNAL_NET 502 -> \$HOME_NET any (msg:"PROTOCOL-SCADA Modbus invalid encapsulated interface response"; flow:established,to_client; content:" 00 00 "; depth:2; offset:2; content:" 2B "; depth:1; offset:7; content:" 0D "; within:1; content:" 0E "; within:1; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:29318; rev:1;) alert tcp \$EXTERNAL_NET 502 -> \$HOME_NET any (msg:"PROTOCOL-SCADA Modbus invalid exception message"; flow:established,to_client; content:" 00 00 "; depth:2; offset:2; byte_test:1,&,128,7; isdataat:9; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:29317; rev:1;)
16	alert tcp \$HOME_NET 502 -> \$EXTERNAL_NET any (msg:"PROTOCOL-SCADA Modbus value scan"; flow:established,to_client,no_stream; content:" 00 00 "; depth:2; offset:2; byte_test:1,&,128,7; content:" 03 "; depth:1; offset:8; detection_filter:track by_dst, count 3, seconds 10; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:29316; rev:2;)



17	alert tcp \$HOME_NET 502 -> \$EXTERNAL_NET any (msg:"PROTOCOL-SCADA Modbus list scan"; flow:established,to_client,no_stream; content:" 00 00 "; depth:2; offset:2; byte_test:1,&,128,7; content:" 02 "; depth:1; offset:8; detection_filter:track by_dst, count 3, seconds 10; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:29315; rev:2;)
18	alert tcp \$HOME_NET 502 -> \$EXTERNAL_NET any (msg:"PROTOCOL-SCADA Modbus function scan"; flow:established,to_client,no_stream; content:" 00 00 "; depth:2; offset:2; byte_test:1,&,128,7; content:" 01 "; depth:1; offset:8; detection_filter:track by_dst, count 3, seconds 10; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:29314; rev:2;)
19	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA invalid modbus protocol identifier"; flow:to_server, established; content:" 00 00 "; depth:2; content:!" 00 00 "; within:2; reference:url,modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; reference:url,modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf; classtype:misc-activity; sid:42109; rev:1;)
20	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA Schneider Modicon Quantum modbus start command attempt"; flow:to_server,established; content:" 5A "; depth:1; offset:7; content:" 40 FF 00 "; distance:0; reference:url,schneider-electric.com; classtype:misc-activity; sid:45234; rev:1;)
21	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA Schneider Modicon Quantum modbus stop command attempt"; flow:to_server,established; content:" 5A "; depth:1; offset:7; content:" 41 FF 00 "; distance:0; reference:url,schneider-electric.com; classtype:misc-activity; sid:45233; rev:1;)
22	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 27700 (msg:"PROTOCOL-SCADA Schneider Electroc ModbusDrv.exe buffer overflow attempt"; flow:to_server,established; content:" FF FF 00 00 "; depth:4; byte_test:2,>,1048,4; metadata:policy max-detect-ips drop, policy security-ips drop; reference:cve,2013-0662; classtype:attempted-admin; sid:43986; rev:2;)
23	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA Modbus user-defined function code - 100 to 110"; flow:to_server,established; byte_test:1,>,99,7; byte_test:1,<,111,7; metadata:policy max-detect-ips drop; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15075; rev:6;)
24	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 502 (msg:"PROTOCOL-SCADA Modbus user-defined function code - 65 to 72"; flow:to_server,established; byte_test:1,>,64,7; byte_test:1,<,73,7; metadata:policy max-detect-ips drop; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15074; rev:6;)
25	alert tcp any any -> any 502 (msg:"ET SCAN Modbus Scanning detected"; content:" 00 00 00 00 00 02 "; flow:established,to_server; depth:6; threshold: type both, track by_src, count 100, seconds 10; reference:url,code.google.com/p/modscan/; reference:url,www.rtaautomation.com/modbustcp/;



	reference:url,doc.emergingthreats.net/2009286; classtype:bad-unknown; sid:2009286; rev:3; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
26	alert modbus any any -> any 502 (modbus: function !3; msg:"Modbus/TCP Alert - Not Allowed Moudbus/TCP Function Code"; sid: 2;)

Annex III: DNP3 Suricata Signature/Specification Rules

The following table lists the new rules created for Suricata to detect DNP3 related attacks.

1	alert tcp any any -> \$DNP3_SERVER 20000 (msg:"TCP SYN flood attack detected"; flags:S; threshold: type threshold, track by_dst, count 20 , seconds 10; sid: 5000001; rev:1;)
2	alert tcp any any -> \$DNP3_SERVER 20000 (msg:"SCADA_IDS: DNP3 - Disable Unsolicited Responses"; dnp3_func:21; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112011; rev:1; priority:2;)
3	alert tcp \$DNP3_SERVER 20000 -> \$DNP3_CLIENT any (flow:established; content:" 82 "; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Unsolicited Response Storm"; threshold: type threshold, track by_src, count 5, seconds 10; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:1111203; rev:1; priority:2;)
4	alert tcp \$DNP3_CLIENT any -> \$DNP3_SERVER 20000 (msg:"SCADA_IDS: DNP3 - Cold Restart From Authorized Client"; dnp3_func:13; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112041; rev:1; priority:2;)
5	alert tcp !\$DNP3_CLIENT any -> \$DNP3_SERVER 20000 (msg:"SCADA_IDS: DNP3 - Cold Restart From Unauthorized Client"; dnp3_func:13; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:denial-of-service; sid:11112051; rev:1; priority:1;)
6	alert tcp !\$DNP3_CLIENT any -> \$DNP3_SERVER 20000 (msg:"SCADA_IDS: DNP3 - Unauthorized Read Request to a PLC"; dnp3_func:1; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:11112061; rev:1; priority:2;)
7	alert tcp !\$DNP3_CLIENT any -> \$DNP3_SERVER 20000 (flow:from_client,established; content:" 05 64 "; depth:2; pcre:"/[S\s]{10}(\x02 \x04 \x05 \x06 \x09 \x0A \x0F \x12)/iAR"; msg:"SCADA_IDS: DNP3 - Unauthorized Write Request to a PLC"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:1111207; rev:1; priority:1;)
9	alert tcp any any -> \$DNP3_SERVER 20000 (msg:"SCADA_IDS: DNP3 - Stop Application"; dnp3_func:18; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:denial-of-service; sid:11112091; rev:1; priority:2;)
10	alert tcp any any -> \$DNP3_SERVER 20000 (msg:"SCADA_IDS: DNP3 - Warm Restart"; dnp3_func:14; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112101; rev:1; priority:2;)
11	alert tcp \$DNP3_CLIENT any -> \$DNP3_SERVER 20000 (flow:from_client,established; content:" FF FF "; offset:4; depth:2; msg:"SCADA_IDS: DNP3 - Broadcast Request from Authorized Client"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:misc-attack; sid:1111211; rev:1; priority:2;)