



A coordinated framework for cyber resilient supply chain systems over complex ICT

infrastructures

D6.4 IT-2 FISHY final release

Document Identification				
Status	Final	Due Date	31/08/2023	
Version	1.0	Submission Date	08/09/2023	

Related WP	WP6	Document Reference D6.4		
Related Deliverable(s)	D6.2, D6.3, D5.2	Dissemination Level (*)	PU	
Lead Participant	SYN	Lead Author	Alexandra Lakka	
Contributors	SYN, XLAB, UPC, TUBS, Sonae, Capgemini, STS, ATOS	Reviewers	Guillermo Jiménez Prieto, Araceli Rojas Morgan (CAPGEMINI)	
			Antonis Gonos (OPTIMUM/Entersoft)	

Keywords:

Pilot scenario, validation activities, validation metrics, use cases, proof of concept, results

This document is issued within the frame and for the purpose of the FISHY project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 952644. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the FISHY Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the FISHY Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the FISHY Partners.

Each FISHY Partner may use this document in conformity with the FISHY Consortium Grant Agreement provisions.

(*) Dissemination level: **PU**: Public, fully open, e.g. web; **CO**: Confidential, restricted under conditions set out in Model Grant Agreement; **CI**: Classified, **Int** = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.



Document Information

List of Contributors				
Name	Partner			
Antonio Álvarez Romero	ATOS			
Guillermo Yuste Fernández	ATOS			
Miguel Martín Pérez	ATOS			
Jorge Martínez Olmo	ATOS			
Rui Guilherme Gonçalves	SONAE			
João Marques	SONAE ARAUCO			
Lakka Alexandra	SYN			
Panagiotis Athanasoulis	SYN			
Panagiotis Karkazis	SYN			
Guillermo Jiménez Prieto	CAPGEMINI			
Jan Antic	XLAB			
Grigorios Kalogiannis	STS			
Andreas Zacharakis	STS			
Andreas Miaoudakis	STS			
Manolis Chatzimpyrros	STS			
Eva Marín Tordera	UPC			
Ayaz Husain	UPC			
Mounir Bensalem	TUBS			

	Document History						
Version	Date	Change editors	Changes				
0.1	4/4/2023	ATOS, SYN	ToC and initial structure				
0.2	20/6/2023	SYN, Capgemini, SONAE	Contribution in chapters 2-5 on attack modelling				
0.3	11/7/2023	SYN	Integration of contributions from SONAE and Capgemini				
0.4	24/7/2023	Capgemini, UPC	Integration of updated contribution from CAP and comments from UPC				
0.5	28/7/2023	Capgemini	Comments from first review round				
0.6	31/7/2023	SYN	Updated contributions in chapter 2 and revisions based on the received comments				
0.7	2/8/2023	UPC	User manual added				
0.8	4/8/2023	SONAE, Entersoft	Comments from first review round included (Entersoft), updated chapter 3 (SONAE)				
0.9	23/8/2023	SYN	Integration of revised contributions and comments primarily from ATOS and UPC				

Document name:	D6.4 IT-2 FISHY final release					Page:	2 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



0.10	30/8/2023	SYN, ATOS	Improvements across all chapters and integration of revised contributions to improve the quality
1.0	08/09/2023	ATOS	FINAL VERSION

Quality Control				
Role	Who (Partner short name)	Approval Date		
Deliverable leader	Alexandra Lakka (SYN)	30/08/2023		
Quality manager	Juan Andrés Alonso (ATOS)	31/08/2023		
Project Coordinator	Antonio Álvarez (ATOS)	08/09/2023		

Document name:	D6.4 IT-2 FISHY final release					Page:	3 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Table of Contents

Document Information	2
Table of Contents	4
List of Tables	6
List of Figures	7
List of Acronyms	12
Executive Summary	13
1 Introduction	14
1.1 Purpose of the document	14
1.2 Relation to other project work packages	14
1.3 FISHY Validation Methodology	14
1.4 Structure of the document	15
2 FISHY validation in Farm to Fork supply chain	17
2.1 Introduction	17
2.2 Farm-to-Fork (F2F) vertical application and attack modelling	17
2.3 Demo script	25
2.3.1 Demo script Sequel A	25
2.3.2 Demo script Sequel B	27
2.3.3 Demo script Sequel C	29
2.3.4 Demo script Sequel D	31
2.3.5 Demo script Sequel E	33
2.3.6 Demo script Sequel F – VAT component used	35
2.3.7 Demo script Sequel F – PMEM component used	36
2.4 FISHY-enabled security enhancement in F2F supply chain	38
2.5 Improvements compared to IT-1 and final assessment	40
2.6 KPIs satisfaction	42
3 FISHY validation in Wood-based Panel Trusted Value-Chain	43
3.1 Introduction	43
3.2 Wood-based Panel Trusted Value vertical application and attack modelling	43
3.3 Demo script	50
3.3.1 Demo script Sequel A and E	52
3.3.2 Demo script for Sequel B and G	55
3.3.3 Demo script for Sequel C	57
3.3.4 Demo script for Sequel D	61
3.3.5 Demo script for Sequel F	63
3.3.6 Demo script for Sequel H	66
3.4 FISHY-enabled security enhancement in WBPTV supply chain	68
3.5 Improvements compared to IT-1 and final assessment	
3.6 KPIs satisfaction	
4 FISHY validation in Securing Autonomous Driving Function at the edge (SADF)	
4.1 Introduction	
4.2 SADE vertical application and attack modelling	

Document name:	D6.4 IT-2 FISHY final release				Page:	4 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4.3	Demo script	80
4.3.3	1 Demo script for Sequel A- Car activation	81
4.3.2	2 Demo script for Sequel B - Power on	83
4.3.3	3 Demo script for Sequel C and D - Software patch certification and correction	89
4.3.4	4 Demo script for Sequel E - Vehicle compromised	91
4.4	FISHY-enabled security enhancement in SADE pilot	
4.5	Improvements compared to IT-1 and final assessment	
4.6	KPIs satisfaction	
5 FISH	IY IT-2 overall evaluation	
6 Con	clusions	100
7 Refe	erences	101
8 Ann	ex: User Manual	102
8.1	XL-SIEM	103
8.2	RAE	107
8.3	WAZUH	110
8.4	SACM	111
8.5	VAT	113
8.6	PMEM	115
8.7	IRO	116
8.8	Trust Monitor	118

Document name:	D6.4 IT-2 FISHY final release					Page:	5 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



List of Tables

Table 1: The ENISA-aligned models of the F2F attacks	19
Table 2: Asset/Impact Synthesis for the F2F use case	20
Table 3: Success probability assessment for potential attacks	24
Table 4: The FISHY components employed in the detection of F2F attacks	39
Table 5: Improvements with respect to the feedback provided by the 1 st pilot round	40
Table 6: Satisfaction of KPIs defined in the DoA	42
Table 7: Satisfaction of KPIs defined in D6.1	42
Table 8: ENISA framework applied to the WBP identified attacks	45
Table 9: Asset/Impact Synthesis	48
Table 10: Success probability assessment for potential attacks	50
Table 11: FISHY Components integrated in the WBP UC	68
Table 12: Rules defined for the detection of the attacks	70
Table 13: Business and Technical metrics defined in D6.3	73
Table 14: ENISA modelling of SADE use case attacks	76
Table 15: Asset/Impact Synthesis	77
Table 16: Success probability assessment for potential attacks	80
Table 17: Example of information OEMs add using the FISHY dashboard to certify their softwar	re
versions	93
Table 18: Business and Technical metrics defined in D6.3	97
Table 19: FISHY components used in each of the three pilot cases	99

Document name:	D6.4 IT-2 FISHY final release					Page:	6 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



List of Figures

Figure 1: ENISA model for supply-chain specific attacks	15
Figure 2: The F2F platform and its interconnection with the FISHY platform	17
Figure 3: Overview of the MITRE ATT&CK navigator	20
Figure 4: The attacks that can be detected based on logs shown/highlighted in green	21
Figure 5: The ATT&CK information provided of the "default credentials" threat	21
Figure 6: The ATT&CK information provided of the "Denial of Service" threat	22
Figure 7: The ATT&CK information provided of the "Unsecured credentials" threat	22
Figure 8: The ATT&CK information provided of the "Network Denial of Service" threat	23
Figure 9: The ATT&CK information provided of the "Brute force" attack	23
Figure 10: The threats that can be detected based on logs and traffic analysis information are	
coloured (65 out of 80, i.e. 81%)	24
Figure 11: The "sequels" of demonstration of the FISHY operation in the Farm to Fork use case	25
Figure 12: Malicious farmer attempts to register fake information through a device (with	
unauthorised wallet ID)	26
Figure 13: Screenshot from the dashboard of SACM that detects the wallet ID attack	26
Figure 14: Screenshot from the FISHY platform capturing the defined policy.	27
Figure 15: Screenshot from the F2F platform where the inability of the malicious user to enter	
information is shown	27
Figure 16: The adversary (transporter) attempts to register fake information through a device (with	1
Distributed Identified that has not been assigned by the F2F platform)	28
Figure 17: Screenshot from the dashboard of Wazuh that detects the DID attack	28
Figure 18: Screenshot from FISHY where the defined policy to protect against the DID attack is	
presented	29
Figure 19: Screenshot from the F2F platform where the inability of the malicious user to enter	
information is shown	29
Figure 20: Malicious warehouse operator attempts to register fake information through a device	
(with unauthorised wallet ID)	30
Figure 21: Screenshot from the dashboard of FISHY where the defined policy is presented	30
Figure 22: Print screen from the F2F platform where the inability of the malicious user (Chris) to ent	ter
information is shown	31
Figure 23: Malicious consumer attempts to register fake information compromising a user account	
(brute force attack)	31
Figure 24: Screenshot from the dashboard of Wazuh that detects the brute force attack issued by	
David (masquerading a consumer)	32
Figure 25: Screenshot from the dashboard of FISHY where the defined policy is presented	32
Figure 26: Screenshot from the F2F platform where the inability of the malicious user (David) to ent	er
the platform is shown	32
Figure 27: The adversary retrieves the public keys of the blockchain nodes	33
Figure 28: SACM monitors the IPs being connected to the blockchain node and checks whether these	е
are whitelisted IP addresses	34
Figure 29: Screenshot from the dashboard of FISHY where the defined policy is presented	34

Document name:	D6.4 IT-2 FISHY final release				Page:	7 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Figure 30: Screenshot from the attempt of the malicious user (Eric) to insert a fake farming platfor	т
in the F2F platform	. 34
Figure 31: Screenshot of the output of the malicious user's attempt to insert his/her farming platfo	rm
in the F2F platform	. 35
Figure 32: Configuration of VAT to scan the F2F platform	. 35
Figure 33: Results of the VAT scan of the F2F platform	. 35
Figure 34: VAT monitors the availability of nodes	. 36
Figure 35: VAT has detected that the port is closed	. 36
Figure 36: PMEM dashboard showing the traffic of the system under examination	. 37
Figure 37: PMEM dashboard showing the statistics of the traffic per connection	. 37
Figure 38: PMEM dashboard showing the statistics which show the results of the Machine Learning	g
model (which classifies the traffic in benign and suspicious)	. 38
Figure 39: Details of the PMEM prediction results as shown in the PMEM dashboard	. 38
Figure 40: The connected factory architecture and its interconnection with the FISHY Platform in th	ie
FRF	. 43
Figure 41: SAP EDI communications architecture and its interconnection with the FISHY Platform in	1
the FRF	. 44
Figure 42: attacks that can be detected with logs as data source	. 48
Figure 43: Attacks that can be detected with network traffic as data source	. 48
Figure 44: Attacks that can be detected with both logs and network traffic as data sources (53 out	of
80, i.e. 66%)	. 49
Figure 45: MITRE ATT&CK Exploit Public-Facing Application technique details on procedure exampl	es,
mitigation actions and detection sources	. 49
Figure 46: High level view of the three main nodes and streams of work affected by the WBP UC in	
FISHY	. 50
Figure 47: Priority threats identified and tested on FISHY for the EDI communications	. 51
Figure 48: Priority threats identified and tested on FISHY for the production monitoring	. 51
Figure 49: Evidence of the 102 calls made using the batch script created for the simulation	. 52
Figure 50: Evidence of the IoT Hub telemetry being above 1000	. 53
Figure 51: XL-SIEM alarm on the DoS	. 53
Figure 52: XL-SIEM displaying details on the events that originated the DoS	. 54
Figure 53: RAE displaying a risk level increase due to the risk of denial-of-service.	. 54
Figure 54: EDC recommendation on the IRO dashboard to "filter ip and port on impacted node"	. 54
Figure 55: Brute force login attempt simulation via Postman using a wrong password multiple time	25
	. 55
Figure 56: XL-SIEM alarm on the brute force attack attempt	. 56
Figure 57: XL-SIEM displaying details on the events that originated the Brute Force detection	. 56
Figure 58: RAE displaying a risk level increase on the denial-of-service risk model	. 56
Figure 59: EDC recommendation on the IRO dashboard to block malicious user IP	. 57
Figure 60: Malicious URL request simulation via Postman by calling an unauthorized URL	. 58
Figure 61: XL-SIEM alarm on the invalid URL request	. 59
Figure 62: XL-SIEM displaying details on the events that originated the malicious URL detection	. 59
Figure 63: RAE risk increases due to the invalid URL reauest	. 60
Figure 64: EDC recommendation on the IRO dashboard to react to the malicious URI risk	. 60

Document name:	D6.4 IT-2 FISHY final release				Page:	8 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Figure 65: Cyberagent identifying the connection of an unknown new device with the Mac Address	
74:fe:48:56:9d:21	. 61
Figure 66: XL-SIEM alarm on the unknown device from the WIFI Controller IP, the source of the sigr	nal . 62
Figure 67: XL-SIEM displaying details on the device detected including the MAC Address	. 62
Figure 68: RAE risk increase due to the unauthorized connection	. 63
Figure 69: EDC recommendation on the IRO dashboard to react to the unknown device/asset by	
suggesting to block the MAC Address	. 63
Figure 70: Logging in to the SRVPT5004 server with a valid user ID	. 64
Figure 71: Logging in to the SRVPT5110 server with the same user ID from Figure 64 simultaneous	ly
	. 64
Figure 72: XL-SIEM alarm on attempt to login in different servers with the same user ID	. 65
Figure 73: RAE displaying a risk increase due to the possible session hijacking	. 65
Figure 74: EDC recommendation on the IRO dashboard to block the user ID identified in the attemp	ot
of session hijacking	. 66
Figure 75: Simulating an ICMP flood	. 66
Figure 76: SACM configuration of a new asset/device to be monitored	. 67
Figure 77: SACM definition of rule specifications including every threshold value	. 67
Figure 78: SACM monitoring results regarding the satisfaction of applied rules	. 68
Figure 79: Screenshot of syslog of WLAN Controller sending logs to TIM (XL-SIEM module) – use cas	se
scenario 1	. 71
Figure 80: Registered IoT device information set from WLAN Controller to TIM (XL-SIEM module) -	use
case scenario 1	. 72
Figure 81: Screenshot of the SAP Web Dispatcher server logs sent to TIM (XL-SIEM module) – use co	ase
scenario 2	. 72
Figure 82: SADE use case deployment	. 74
Figure 83: The attacks that can be detected based on logs shown/highlighted in Blue (53 out of 80,	i.e.
66%)	. 78
Figure 84: Module firmware threat	. 78
Figure 85: Adversary in the middle threat	. 79
Figure 86: Brute force threat	. 79
Figure 87: SADE use cases	. 80
Figure 88: Dealer's fishy dashboard workspace. With the add vehicle form (fishy_sb user is a dealer	r)81
Figure 89: Log row in SADE API logs	. 81
Figure 90: Not existing car events in XL-SIEM dashboard	. 81
Figure 91: Brute force attack alarm	. 82
Figure 92. Mail received by Local Operator	. 82
Figure 93: Allow new driver form. Only available for car owner (fishy_sc)	. 83
Figure 94: Unauthorized driver log row	. 83
Figure 95: Unauthorized driver event	. 84
Figure 96: First unauthorized driver alarm	. 84
Figure 97: Second unauthorized driver alarm à Pin blocked alarm	. 85
Figure 98: Qualitative risk analysis	. 85
Figure 99: Quantitative risk analysis	. 86

Document name:	D6.4 IT-2 FISHY final release					Page:	9 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Figure 100: Mail telling the allowed drivers to input its PIN	86
Figure 101: Insert PIN form in the car owner workspace in FISHY dashboard	87
Figure 102: Unauthorized PIN error	87
Figure 103: The evant of unauthorized PIN error as shown in the dashboard	88
Figure 104: Car blocked alarm	88
Figure 105: Certification management in the manufacturer workspace	89
Figure 106: Mail asking manufacturer to update an IoT device online	90
Figure 107: Mail asking dealer to schedule a recall to update components offline	90
Figure 108: Normal workflow of a vehicle power on	91
Figure 109: Possible malware alarm	91
Figure 110: Mail asking manufacturer to update an IoT device online	92
Figure 111: Mail asking dealer to schedule a recall to update components offline	92
Figure 112: JSON object including vehicle data in SADE use case	95
Figure 113: Accessing FISHY dashboard	102
Figure 114: Main page in FISHY dashboard	102
Figure 115: FISHY tools in FISHY dashboard	103
Figure 116: Through the FISHY dashboard, we are able to select the XL-SIEM	103
Figure 117: Main view [1] At first glance, we can observe a threat level based on the events and	
alarms generated in the recent hours and we also have a summary of the alarms and statistics	
generated in the last few hours	104
Figure 118: Statistics on the detected attacks are provided	104
Figure 119: We use the navigation menu of the XL-SIEM to view the list of events	105
Figure 120: Events List	105
Figure 121:We use the navigation menu of the XL-SIEM to view the list of alarms	105
Figure 122:Alarms List	106
Figure 123:Alarms details	106
Figure 124: RAE selection from the landing page	107
Figure 125. The user can choose a risk model	107
Figure 126:Main RAE view with basic info	108
Figure 127. RAE qualitative risk assessment	108
Figure 128. RAE quantitative risk assessment	109
Figure 129: Printscreen from the dashboard of Wazuh	110
Figure 130: Printscreen from the dashboard of Wazuh that detects a brute force attack	110
Figure 131: Printscreen from the dashboard of SACM that detects the wallet ID attack	111
Figure 132: Printscreen from the dashboard of SACM on configurating new assets to monitor	111
Figure 133: Printscreen from the dashboard of SACM on configurating new rules to monitor the as	sets
	112
Figure 134: Configuration of VAT to scan a specific platform	113
Figure 135: Results of the VAT scan of the F2F platform	113
Figure 136: VAT monitors the availability of nodes	114
Figure 137: PMEM front end showing different status	115
Figure 138: PMEM showing events detected in the last 24 hours.	115
Figure 139: PMEM showing different scan results reports.	116
Figure 140: IRO in the main FISHY Dashboard	116
	-

Document name:	D6.4 IT-2 FISHY final release				Page:	10 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Figure 141:List of alerts on the dashboard from different tools (e.g.SACM detects wallet ID attack	:) 117
Figure 142: EDC recommendation on the IRO dashboard	118
Figure 143: Trust Monitor listing the monitored nodes	119
Figure 144: Trust Monitor during a Remote Attestation execution	120

Document name:	D6.4 IT-2 FISHY final release				Page:	11 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



List of Acronyms

Abbreviation / acronym	Description
DDoS	Distributed Denial of Service
DID	Decentralised Identifier
EDC	Enforcement and Dynamic Configuration
ELK	Elastic search, Logstash and Kibana
F2F	Farm to Fork
FA	Federation Adapter (of the SOFIE platform)
IAM	Identity and Access Manager
IoT	Internet of Things
IRO	Intent-based Resilience Orchestrator
JSON	JavaScript Object Notation
Jwt	JSON web token
K8S	Kubernetes
NED	Network Edge Device
OEM	Original Equipment Manufacturer
PoC	Proof-of-Concept
POD	<i>Pods</i> are the smallest deployable units of computing that can be created and manage in Kubernetes
RAE	Risk Assessment Engine
SACM	Security Assurance & Certification Management
SADE	Securing Autonomous Driving function at the Edge
SIA	Secure Infrastructure Abstraction
SSH	Secure Shell
SSID	Service Set Identifier
TIM	Trust & Incident Manager
UC	Use Case
UML	Unified Modelling Language
UTC	Universal Time Coordinated
UUID	Universally Unique Identifier
VAT	Vulnerability Assessment Tool
WBPTV	Wood-based Panels Trusted Value-chain

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					12 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Executive Summary

Deliverable D6.4 titled "IT-2 FISHY final release" reports the second and final iteration in the process of deploying, validating and assessing the FISHY Platform in the three use cases. For each pilot, the specific attacks of interest are presented and modelled according to ENISA and MITRE frameworks. Per use case, different scenarios to demonstrate the way FISHY contributes to mitigating these supply chain specific attacks are described and instances from the demonstration are included. Additionally, videos presenting the execution of these scenarios have been prepared and exist on the YouTube channel of the project. Furthermore, the updates and improvements with respect to the FISHY-IT 1 are elaborated and the achievement of the pilot -specific KPIs is detailed. This deliverable also includes an overall assessment of the final release of the FISHY platform and a user manual to guide prospective users to test the open-source version of the FISHY platform.

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					13 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



1 Introduction

1.1 Purpose of the document

Deliverable D6.4 is the final report of the activities that were performed in WP6 until the end of the project. These activities focused on the validation and assessment of the final release of the FISHY platform in three different use cases. The results of these activities have been continuously informed to guide further developments and improvements of the platform towards the go-to-market stage. In this second round of validation the focus has been placed on:

- a) issues pointed out in the first round of validation,
- b) the validation of the enriched (additional) functionality of the final release compared to IT-1, and
- c) the verification of the pilot-specific KPI achievement.

1.2 Relation to other project work packages

This deliverable highly interrelates with WP2, WP5 and WP6 and more specifically with:

- D6.2 [1] which presents the results from the first round of piloting activities,
- D6.3 [2] which describes the validation methodology for the IT-2 as well as the threats and attacks to be detected,
- D5.2 [3] which includes the final version of the integrated platform,
- D2.4 [4] which presents the final architecture and deployment options of the FISHY platform,
- D7.4 [5], which presents the market needs.

It uses all these deliverables as inputs and does not affect any other deliverable, as it comes at the final month of the project.

1.3 FISHY Validation Methodology

Already in M12, in D6.1, [6], FISHY consortium defined the FISHY platform evaluation methodology that would be followed throughout the project lifetime. As such, the current deliverable presents the outcome of the steps 6 (pilot activities using IT-2) and step 7 (final feedback collection) of the methodology presented in D6.1, figure 1.

However, as the project evolved, it became imperative to:

- a) Carefully consider User Interface aspects: for this reason, in this last piloting round, we recruited people outside the FISHY teams for carrying out the evaluation of the UI and used the prepared user manual to do so.
- b) Examine and verify that FISHY platform is GDPR compliant: all use case partners have double checked with the FISHY technical partners that no personal data are collected and used in the platform (as also reported in the ethics-relevant deliverables).
- c) Examine and ensure that the functionality and value of *all* the FISHY components is validated.
- d) Validate the fact that the attacks that FISHY places emphasis on are supply-chain specific attacks: for this reason, we have modelled all the attacks we consider for validation using the ENISA model described in the "Threat landscape for the supply chain attacks" [7].
- e) Check the extensibility of the FISHY platform to address additional attacks that may be considered in the future as important for the FISHY supply chains. To examine this possibility, we have used the MITRE ATT&CK framework [8]. This has also allowed us to ensure that FISHY

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					14 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



employs techniques that are aligned with the state-of-the-art (reflected in MITRE ATT&CK) and that the techniques we use in FISHY enable the detection of a wide set of additional attacks in the future.

The way we have used ENISA model is detailed in chapter 2 (using the Farm to Fork use case as an example) and then, the same methodology is adopted for the rest two use cases. It is important to point out that according to ENISA, the definition of supply chain attacks is as follows:

"A supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. Therefore, for an attack to be classified as a supply chain one, both the supplier and the customer have to be targets." [7]

The following figure (copied from [7]) illustrates the concept.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection Social Engineering Brute-Force Attack Exploiting Software Vulnerability Exploiting Configuration Vulnerability Open-Source Intelligence (OSINT)	Pre-existing Software Software Libraries Code Configurations Data Processes Hardware People Supplier	Trusted Relationship [T1199] Drive-by Compromise [T1189] Phishing [T1566] Malware Infection Physical Attack or Modification Counterfeiting	Data Personal Data Intellectual Property Software Processes Bandwidth Financial People

Figure 1: ENISA model for supply-chain specific attacks

The steps we use to evaluate the extensibility of the FISHY platform adopting MITRE framework is similarly described in chapter 2 (again using as example the Farm to Fork use case) and then, followed for the rest use cases in chapters 3 and 4. It is worth point out that MITRE ATT&CK[®] is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. With the creation of ATT&CK, MITRE aspires to fulfil its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge [8].

1.4 Structure of the document

The rest of this document is organised in the following major chapters:

• **Chapter 2-4:** These chapters report the validation activities for the final release of the FISHY platform in each one of the three FISHY use cases (F2F, WBPTV and SADE). These chapters are organised in a uniform manner: after the introduction, the vertical application considered in the specific use case is briefly presented followed by the attacks of interest to the specific use

Document name:	D6.4 IT-2	D6.4 IT-2 FISHY final release					15 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



case and their modelling according to ENISA and MITRE frameworks. Then, the demonstration scenarios are described, and indicative screenshots are provided. A separate section is devoted to the enhancements offered by FISHY and another one presents the improvements compared to IT-1. The last section in each chapter details the use-case specific KPI achievement.

- **Chapter 5: Result consolidation.** In this chapter, the feedback from the three use cases is consolidated to draw conclusions for the platform and guide exploitation.
- Chapter 6: Conclusions. This chapter provides the conclusions of this deliverable.

Finally, in the Appendix, the user manual is included.

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release				Page:	16 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



2 FISHY validation in Farm to Fork supply chain

2.1 Introduction

In this chapter, we focus on the validation of FISHY IT-2 in the Farm-to-Fork supply chain. The structure of this chapter follows the one presented in section 1.4.

2.2 Farm-to-Fork (F2F) vertical application and attack modelling

In the Farm to Fork (F2F) pilot, we distinguish the following five actors:

- the actor in the farm (user/administrator of the IoT island that is deployed in the farm),
- the actor of the transportation company which associates the products with the conditions under which the products are transported (captured by the IoT island deployed in the vehicle),
- the actor in the **warehouse** where the products are stored and associates the conditions under which the products are kept up to the point they are purchased by a consumer,
- the **consumer** who purchases the product and based on the RFID tag attached to the product they can inspect the full history of the product and finally,
- the **administrator of the platform** that gathers the information from all IoT islands and delivers it to the consumer.

In real life, there are additional actors of the same type (e.g., transportation and supermarket actors) who perform the same activities as the transporter and the warehouse manager. Each of the above represents a node in this supply chain and can be supplier and customer at the same time. For example, the actor from the transportation company represents a consumer for the farmer and a supplier for the actor of the warehouse.

We now briefly describe the F2F platform from a technical point of view and present (again) the attacks to ease the reading: In the Farm to Fork supply chain, to protect the F2F platform, SYN, ENTERSOFT have implemented the components that deliver to the FISHY platform information from four distinct points of the deployed F2F platform. The "security probes" have been described in [1], of the F2F platform are shown in the following Figure 2. Entry points 1 and 2 are relevant to the registration of information in the farm, transportation and warehouse steps of the supply chain during which the information is stored in the ledger maintained per step. Entry points 3 is relevant to the consumer or administrator of platform and entry points 4a and 4b are relevant to the consortium level operations. These data are sent to FISHY platform through SIA in the form of a JSON object which will include the following fields: UUID (Unique Universal ID), Timestamp (UTC timestamp), Type, Metadata.



Figure 2: The F2F platform and its interconnection with the FISHY platform

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					17 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



In the framework of the FISHY lifetime, we have studied this pilot and we have identified four types of attacks of interest. These are:

- Type 1: Unauthorised device –wallet ID level
 - Metadata: {Attacker wallet ID, Expected Legitimate Wallet ID, Device name}
- Type 2: Unauthorised device Decentralised Identifier DID level (with DID characterizing the device)
 - Metadata: {Attacker DID, Device name, Jwt}
- Type 3: Unauthorised User
 - Metadata: {username, IP}
- Type 4: Attack to Blockchain node
 - Metadata: {IP, port, incident type}

We have also discussed with other partners and decided to protect the F2F platform against additional attacks, to check how easy it is to extend the protection against additional attacks, if this is feasible and what extra actions are needed.

With respect to <u>attack modelling according to the ENISA model</u> which has been introduced in chapter 1, for each type of attack we need to identify the following four elements:

- Attack Techniques Used to Compromise the Supply Chain
- Supplier Assets Targeted by the Supply Chain Attack
- Attack Techniques Used to Compromise the Customer
- Customer Assets Targeted by the Supply Chain Attack

These four components per attack are shown in the following Table 2. For example, in the first attack, we assume that a malicious user can guess the wallet ID of a benign device (e.g., the aggregator of the information collected in the Farm). In this case, the malicious user targets the data that will be registered for this product (Supplier Assets Targeted by the Supply Chain Attack). The Attack Techniques Used to Compromise the Customer is counterfeiting as the farm device is impersonated and registers fake information (e.g., with respect to the farming conditions and the used fertilizers). This implies that the transporter (who is the consumer in this case) that will collect the product will either inspect this information and consider this product as of inappropriate quality and will not accept them or will accept them along with the fake information which means that this information will propagate further in the supply chain affecting all of it.

We present one additional attack (the 3rd of the table), where a well-known attack technique, namely brute-force attack technique (Attack Techniques Used to Compromise the Supply Chain) is adopted by the adversary and she manages to gain access to the F2F platform – here the Supplier Assets Targeted by the Supply Chain Attack is the F2F platform- which keeps information about all the history of the products. In this case, she can modify part of this information – this information is the Customer Assets Targeted by the Supply Chain Attack- and thus, affect the trusted relationship (Attack Techniques Used to Compromise the Customer) between the producer (farmer) and the consumer (transporter) who will access this (fake) information. While brute force attack is a well known attack from all IT systems, here it has direct implications on the subsequent actors of the supply chain, and this makes it a supply chain attack. This is why ENISA has clearly included brute-force attack in its lists of potential attacks of the supply chain.

The fourth attack is relevant to the blockchain operations of the considered supply chain. While blockchain technology improves the security, it still has vulnerabilities which could be exploited by adversaries. In this type of attack, we consider that the adversary compromises the blockchain nodes (exploiting the IP addresses or ports used) in which case the processes running in the nodes are compromised. In this case, the relationship between the producer and the consumer (business or

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release				Page:	18 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



individual) is jeopardized as the consumer will not be able to access these services and thus, will not be able to access the relevant information.

	SUPPLIER		CUSTOMER	
Attack	Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
F2F- Type 1: Unauthorized device – wallet ID level	Social Engineering / Brute-Force (SOFIE wallet ID becomes known to the adversary)	The data for which we want to store information about	Counterfeiting (Impersonate a farmer and register false information)	Data (The data relevant to a product's transportation)
F2F- Type 2: Unauthorized device – DID level	Social Engineering/ Brute Force (Device private key with which it signs token becomes known to the adversary)	The data which the IoT device sends to the platform	Trusted relationship [T1199] (Between the SOFIE platform and the IoT device)	Data (the condition of the products)
F2F- Type 3: Unauthorized user	Brute-force (SOFIE platform to gain privileges)	The SOFIE platform	Trusted relationship [T1199] (Between the SOFIE platform and the producer)	The data relevant to the conditions of the food would be compromised
F2F- Type 4: Attack to blockchain node	Open-Source Intelligence (OSINT) (blockchain nodes' IP and ports are exposed)	The processes (The docker services running the nodes)	Trusted relationship [T1199] (Between the SOFIE platform and the producer)	Data (The availability of data in the blockchain)

Table 1: The ENISA-aligned models of the F2F attacks

With respect to <u>the MITRE ATT&CK framework [9]</u>, first we must clarify that ATT&CK stands for Adversarial Tactics, Techniques and Common Knowledge, and these are what the framework and accompanying ATT&CK knowledge base consist of. This framework aims at addressing the gap left by traditional models which are very focused on the study of attacks rather than their role in Risk Analysis, where the concern is not how the attack is executed but more on the effects and exploitation opportunities that can impact the system. This is of particular interest in the supply chain environments where the attacks to one of the interconnected IoT islands directly affect other actors in the chain. Additionally, MITRE table is enriched by the open community that supports it. MITRE ATT@CK analysis

Document name:	D6.4 IT-2 I	ISHY final release	Page:	19 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



approach can be beneficially used for risk analysis for complex and interdependent systems as justified in [11] and [12]. In more detail, the Asset/Impact-centric approach suggested in [13] is appropriate for supply chain systems and is used when adversaries, vulnerabilities and group threats are challenging to recognise or when assets are considered more critical.

We now describe the steps of applying the asset/impact-centric approach (suggested by UMINHO) to the Farm to Fork pilot.

Step 1: System description:

The system deployed in the farm to fork supply chain has already been presented above and thus here, we identify the main assets and their potential impact on security properties in Table 2. The 'Exposition' column highlights the medium by which the assets can be reached, being the primary source of attacks. The "impact" column describes the potential impact on security properties.

ASSET	EXPOSITION	IMPACT	Notes
Resource limited devices (IoT devices in the three islands)	None	Low	Not considered in the previous list
Nodes in the edge (e.g., FA - federated adapter)	Wireless	High	Type 1 and 2 attacks of the previous list
Network nodes	Limited	Medium	
IAM	None	High	Type 3 attack from the above list (Brute force attack)
Blockchain nodes	None	High	Type 4 attack of the previous list
Web application	Internet	Medium	Type 3 attack from the above list (Brute force attack)

Table 2: Asset/Impact Synthesis for the F2F use case

Step 2: threat modelling

Threat modelling is an activity aiming to understand threats better and identify how the related attacks are deployed, the tools used, and the explored vulnerabilities. This is made easy by the MITRE ATT&CK Navigator an overview of which is shown in Figure 3, where the full list of threats identified so far by this group appear grouped.

Drive-by Compromise Specification Specifi	Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Name Notice Notice <td>Drive-by Compromise</td> <td>Change Operating</td> <td>Hardcoded</td> <td>Exploitation for</td> <td>Change Operating</td> <td>Network Connection</td> <td>Default Credentials</td> <td>Adversary-in-the-</td> <td>Commonly Used Port</td> <td>Activate Firmware Update</td> <td>Brute Force I/O</td> <td>Damage to Property</td>	Drive-by Compromise	Change Operating	Hardcoded	Exploitation for	Change Operating	Network Connection	Default Credentials	Adversary-in-the-	Commonly Used Port	Activate Firmware Update	Brute Force I/O	Damage to Property
Interface Module Firmware Evaluation (module firmware) Evaluation (module firmware) Remote System (holds firmware) Bard object (module firmware) Bard object fiel infection Band object fiel (module firmware) Band object fiel	xploit Public-Facing	Command-Line	Modify Program	Hooking	Exploitation for	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Instant Regist Private Private File Infection Discovery's Contentiants Information Information Private Reside Block Reporting House State Analiants Stand Private Private Accessibility Spate File Infection Spate File Infection Masquerating Discovery's Credentials File Private Block Reporting Message Block Reporting Message Loss of Private Block Senial Cont Block Senia	ploitation of Remote	Interface	Module Firmware		Evasion	Remote System	Hardcoded	Data from	Standard Application	Block Command Message	Module Firmware	Denial of View
Arror of operation in microaria Arror of opera	rvices	Execution through	Project File Infection		Indicator Removal on	Discovery	Credentials	Information	cuper riotocor	Block Reporting Merrage	Spoof Reporting	Loss of Availability
Nicks National Services Natio	ternal Remote	Graphical User	Froject file Intection		Massueradian	Remote System	Lateral Tool Transfer	Data from Local		Block Ferial COM	Use therized	Loss of Control
Notice Notice <td>rvices</td> <td>Interface</td> <td>System Pirmware</td> <td></td> <td>Restlik</td> <td>Discovery</td> <td>Program Download</td> <td>System</td> <td></td> <td>Changes Conduction</td> <td>Command Message</td> <td>Loss of Productivity</td>	rvices	Interface	System Pirmware		Restlik	Discovery	Program Download	System		Changes Conduction	Command Message	Loss of Productivity
Model parte Model parte Model parte Data Destruction (Dirage Data	evice	Hooking	valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Detect Operating		Change Credential		and Revenue
gelataton Trocom syate Alarter syate Matter syate Matter syate Matter syate Matter syate Matter syate Matter syate Matter syate Matter syate Matter Syatem Firmage Of minge Unit di Tig Syatem Firmage Design of Discover Discover System Firmage Design of Discover Discover Discover System Firmage Design of Discover D	emote Services	Modify Controller			Message		Valid Accounts	1/O Image		Data Destruction		Loss of Protection
get Matter Scripting Density interaction Density interaction Density interaction get Matter Scripting Manipulation Manipulation get Automation Density interaction Manipulation get Automation Density interaction Manipulation get Automation Screen Capture Rootbit Manipulation mainter Ober Asset Wretees Sniffing Speen Firmware	plication Through	Native API						Monitor Process State		Device Restart/Shutdown		Loss of View
Important Identification Modily Atam Settings Control apply Chain antiert Cyber Asset Program Upload Rootist Manipulation Streem Capture antiert Cyber Asset Service Stop Thermany	oque Master	Scripting						Point & Tag		Manipulate I/O Image		Manipulation of
tacdriment ************************************	pearphishing	User Execution						Identification		Modify Alarm Settings		Control
pply Chain Screen Capture Theed Open Information Information and Information I	ttachment							Program Upload		Rootkit		Manipulation of View
Aniset Cyber Asset Wreters Sniffing System Firmware	apply Chain							Screen Capture		Service Ston		Theft of Operational
ajaen ummare	ansient Oxber Asset							Wireless Sniffing		Sustem Eirmware		momadon
for the second	Finishent Cyther Poster									System minute		

Figure 3: Overview of the MITRE ATT&CK navigator

Document name:	D6.4 IT-2 I	FISHY final release				Page:	20 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Up to now, the attacks identified by SYN and OPT have been proposed to be detected using logs. To verify our decision, we select as "control element" log in the MITRE navigator and we see the set of attacks that can be detected using logs, shown in green colour in the figure.



Figure 4: The attacks that can be detected based on logs shown/highlighted in green

From the green boxes highlighted in the figure, we then select one-by-one the threat most relevant to our system. For example, the "default credentials" attack and the "denial of service" attack. Then, selecting the attack, the MITRE ATT&CK navigator displays all the procedures that an adversary may follow that have been registered in the framework, the mitigation measures identified so far and the detection alternatives. Examples are shown in Figure 5, Figure 6, Figure 7, Figure 8 and Figure 9.

									and a second		_		-
NTRE ATT&CK					Matrices • Tactics • 1	iechniques -	Deta Sources Mitigations • Groups S	loftware Campaigns	Resources	• Blog G	Cor	stribute	Search Q
ECHNIQUES		Home + Tr	ectrologues + ICS > Default C	redentials									
Iterprise oblie S nitial Access Execution Persistence Privilege Escalation Evasion Discovery Lateral Movement Default Credentials Exploration of Remote Br	• • • • • • • • • • • • • • • • • • •	Defa Adversarie may be no manufactu Default cre through un	ault Credeni is may leverage manufactu sesany for initia contgura zers may have services that sedentitals are normally document official means. Adversaries	tials error supplier set default ordentials on cont tion of the device. It is general beat practice intermediates and the set of the set of the mented in an instruction manual that is either may inversign default credentials that have	tol system devices. These default credentials may have administrative p to change the passends for these accounts as soon as possible, but so de changel. I ¹² r packaged with the device, published online through official means, or p of been properly modified or disabled.	ermissions and me	ID: T0812 Sub-sechniques: No sub-lechniques O Tactic: Lateral Adversaria O Platform: Control Server, Explaneors Controller, RTU/FCLB, Human Mac System, Toxetochon Resp. Version: 1.0 Crested: 21 Mix 2020 Last Modified: 09 March 2023	g Wonstation, Field Inne Inderface, Safety Instr Inatink	umented				
Lateral Tool Transfer		in in	Mitigation	Description									
Program Download		MOBOT	Access Management	Ensure embedded controls and network of	levices are protected through access management, as these devices offs	in have unknow	default accounts which could be used to gain una	uthorized access.					
Valid Accounts		M0927	Password Policies	Review vendor documents and security a	ierts for potentially unknown or overlooked default credentials within exis	ting devices							
offection	×	Deteo	ction										
whibit Response Function	*	ID	Data Source	Data Component	Detects								
npact	~	D50028	Logon Session	Logon Session Creation	Monitor logon sessions for default credential use.								
		DS0029	Network Traffic	Network Traffic Content	Monitor network traffic for default credential use in protocols	that allow uners	rypted authentication.						
		Refer	ences	to Industrial Control Systems (ICS) Security	het/seved. 2018//03/28								

Figure 5: The ATT&CK information provided of the "default credentials" threat

Document name:	D6.4 IT-2 I	ISHY final release				Page:	21 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



$\leftrightarrow \rightarrow G$		attack	.mitre.org/t	chniques/T0814/	Q	L B	\$	•	9	*		Ç
ITRE ATT&CK				Matter - Taller - Taller - Taller - Bakhar	a Mantan -	-	-	Cerevign	heart		17 OF	•••
CHNIQUES	-	· Territore · (01 ·)	Name of Barries									
rprise -	De	inial of Se	rvice									
Inf Access	Apres	sarias may jarhern Dar tou hou to handia. Dan	ial of Genius (Dol) actable to going device actable may served	nga ngana daria Germaniy Gangka yi Solanda resda anashenyi teraga laria anti a tip nisea if ngana a salan teragani ana lanto ye anga ina a anga ye inga daria ang								
estitation w	burne i	ict to other events in the ICS declares are particu- effort malware. ²¹	animanan ary sensitive to Doli events, a	ng beams wegenesis is well as the set of page ang. Advances may as emergen anound for an framer beam from the page and from the page and the page an								
Intropy Excession · ·		narian may applicit a not ara that can be used to	to are rule and the to cause a t cause a discipline of service cond	Weight of a distribution of the programming and in a program, service, or within the special postern software or leased listed to another advectory control block. Volveshill tools, Volveshill, Volves								
aberal Moremany w pleman w	Advers that in	sarias may have prior to those uncontrolled tea	nvolatija abovt industrial prim turta siznavroptija, ¹⁰ M M	a or server de las cant e transversent insige Tenne Spann Mension Stanson, Dealer and advances versage autore a server de las								
ommand and Control ribit Response Function Anti-une Ennount Unders Mode	Pro	cedure Exar	mples									
Karm Suppression		12 Inclusion Colores	The Bankelow Dates and	na staan mutata serene DR statum tu internetein vaan Tea suut saan aktist internetein en astatum ta dest internetein en astatum ta								
Azok Command Message Nock Reporting Message	1812 Manage TPUTED (and a significance (PUTED) (and a sign											
Diarge Dedental	8100	0A PLOBlame	The metastanian the PLC of	to engand by interruption year time from the PLC discuss implements are indiced any segment process within the PLC with the impact of a 2012 H								
Denial Destruction Denial of Service	Miti	tigations										
Device Restart/ShubBovel			Magazine	Description								
Hangulate VO Hispe Modify Alarm Bettinge	UC#	115	Washing Times	Tipmen ent process instants about the performant other a transmit condition accurs.								
Austria Ince	Det	tection										
System Firmware		Data Source	Data Component	laws								
rgair Process Control +	9809	OTE Application Log	Appleanse Log Contern	Ventor for againants togging, messaging, and to other and many mean from Decise of Benning Cost) and all the foreign of the antibility of services to a and in the decision, services the decision, services togging and recommendation and the decision.								
	0800	C29 Return Traffic	Nativolit Talfic Contain	Vector and exceptional general and public dependences of the processing of the data of the sector and the start of the sta	melalism with process							
			Alatorich Traffic Film	Maniter network data for uncommon data flow. Processes utilizing the network that do not normally have network communication of how invertient averaged out.								
	580	Ord Operational Date	Data Propess Mabbry/Live	Vanity spectrum day for indicating divergency data to which may indicate a Darks of being, including of the behavior, but here at may privide additional endormation and and may complement of the devictors.								
	Ref	ferences	CK Alem (CS-44,000-17-102-0 27 Adriany (CSA-15-055-01) manatur 2016, January 18-01	Eleventhementational device the set (2011) 101 encode (2012) 2014 (Sector Department (2012) 2014) Construction of the set of construction of construction of the set of construction of construction of the set of construction of the set of construction of co								

Figure 6: The ATT&CK information provided of the "Denial of Service" threat

← → C	1	atta	ack.mitre.	rg/techniques/T1552/	Q	B	6 4	6 4 9	🖻 🌣 🌖 🛸	🖻 🌣 🧕 🗯 🗖	🖻 🌣 🌖 🗯 🗖
TACK				and the second	n 10	 -	-	Martin Charles Street 1	Martin	Martin Tran Shart Grante Second	Martin Stat. Shart Sealar Sealar St.
4.0	-	· Petrone I free	The statement incomes								
		a day under	Andentiale								
		secured	Cregentials								
	54	a-searchig-sea (8)		× 8-m							
	-	arma ina, manifi sar	wormed parameter frequencies	result and refere to the second function of t							
na familia				PAPER As and its forward and and the second se							
16011 *				Automatical Automatical Strength Streng							
drama a				Dwine 1 A Avenue 1011							
-				1000 THE TABLE 1 (1) THE TABLE 1							
Paraviri Desa	-	Service and	and the second se	Table Annual Control of Control o							
An Orale Mar Access	-	Cedure Exa	mpres								
anieritata in	2										
ator metaptic	Mt	igations									
method or Report Derivator	н.	-		Normal State Stat							
-		ra intefne	key Sprilgenter	Name a constitution of the first functions of							
tor Access Torge	**	10 AN		Analysis and for File stretures and on the anderse in the entry is related for a particular to the streture in the file for the							
Automotivation (Sertification	***	ar broughdan	ala virtaine	type integrate mediate in television oblights provide media in the providence of the							
dist Colors		at the heat	is hults	Limit assume in the memory instance with a property surface of the algebrane minute () and may here exerce and exerce the approx () aller and here algebrane () and may a memory () and may a memor							
antica in			a managed the result	profit and a case of an error and the set of a property and the set of a property case of a set of a property of the set							
-fine	***	DR Assessed	eet Intairen	These are an approximation of proceeding to the control of the con							
4		of Personal d	the second s	In any paralysis in the product or right reading Physic Revenues control by each of the legan band of the approximation game and strange in the							
d and the second second	***	III Forlaget A		It is a manage for advance of the advance of the state of the advance of the streng arm and the generative and the advance of the streng arm and the advance of the advance of the streng arm and the advance of the							
Peterenas	-	u tarrita	and Disatory Harmanica.	Automitie dealers in gewind dealerse und Automaties in terressenter autor							
	-	at lotrebri		Aug) used reportants in the parameter section being sector (sector)							
-	-	in inclusion		Investigation of space after space and of the strandom of the strange protocol and space strange of the strange of s							
	Deb	action									
been in		-	Non-Temporary								
	181		-	mente applicante (qui fe antre) date esta appliquí entre cua appliquí							
	180	and descent	Correspond Statistics								
÷	1.81	the sta	******		n' servaite		*	*	*	*	*
	1411		mission Transmission	HISTOR FOR CHARGE AND							
	1.817		And Address	inter the analysis of the second s							
	-	thi induation	to an and the second se	the transmission of the state o							
	Ref	ferences men 4 process ment process quer, trave (21)	en 18. ogfarførter som storetige 19. ogfar 129 forsænder og 1 fog 11. oggan av Tendera o	general and an end of the second of the seco							

Figure 7: The ATT&CK information provided of the "Unsecured credentials" threat

Document name:	D6.4 IT-2 I	FISHY final release	Page:	22 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



PE ATT&CK			ang teen	4		Rep 17	Contribute	Search
NE ANON		To perform	Network DoS atta	cks several aspects	s apply to multiple methods, including IP address spoofing, and bothets. Created: 17 April 2019	1000	Statistics	Contractor
HNIQUES		Advertarie	s may use the orig	inal IP address of a	n attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking			
ise	~ *	system or	to enable reflection	. This can increase	the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the Version Permaters			
naissance	~	source add	iress on network d	efense devices.				
ce Development	~	For DoS at	tacks targeting the	hosting system dire	ectly see Endpoint Denial of Service.			
Access	× .	Deser	dura Euro					
ion .	Č.	Proce	dure Exa	mpies				
e Encalation	0	10	Name	Descripti	See .			
e Evasion		60007	APT28	in 2016	1, AP128 conducted a distributed denial of service (DDoS) attack against the World Anti-Doping Agency ¹⁶			
tial Access	-	80532	Lucifer	Lucifer	can execute TDP, UDP, and HTTP denial of service (DoS) attacks. ²¹¹			
rγ	~							
Movement	~	Mitig	ations					
on	~	10	Mitigation	Description				
ind and Control	~	141027	Citter Neberski	When Read unlast				
bon	Ĩ.		Traffic	be provided by th	e hosting letered Service Provider (ISP) or by a bio party such as a Content Delivery Nethonk (CDN) or providers specializing in DoS mitigations 111			
ant Access Removal				Depending on flo	nod volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport 🏁			
Destruction				As immediate ret respond to incide	toponse may require taple engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to ents 18			
Encrypted for Impact Manipulation	~	Deter	tion					
ement	č.	10	Data Source	Data Component	Delects			
pint Denial of Service		D50029	Network Traffic	Network Traffic	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.			
rare Corruption				Flow				
System Recovery		DS0013	Sensor Health	Host Status	Detection of Network DoS can sometimes be achieved before the traffic volume is sufficient to cause impact to the availability of the service, but such response time typically requires very appressive			
ork Denial of Service	^				interneting and responsements to remove up an upperson remove promote women for logging, messaging, and oner antifacts righting the relation or nost denotes (ex. metrics, errors, and/or exceptions from logging applications)			
ct Network Flood								
ection Amplification		Refer	ences					
Ince Higacking		1. Ned	Moran, Mike Scott,	Mike Oppenheim of	FireEye, (2014, November 3). Operation Poisoned Handover: Unveiling Ties 4. Brady, S. (2018, October 3). Indictment - United States vs Alekaei Sergeyevich Morenets, et al., Retrieved October 1, 2020.			
ce stop	-	Beta	een AFT Activity in	Hong Kong's Pro-D	remocracy Movement. Nethoved April 16, 2019. 5 Hou, K. et al. (2020, June 24). Lucifer: New Cryptolaciling and DDoS Hybrid Malware Exploiting High and Critical			

Figure 8: The ATT&CK information provided of the "Network Denial of Service" threat

	atta	ck.mitre.org	g/techniques/i		ਮ	
				Maller - Tarlie - Tar	Campaigns	Recorder
	Proc	cedure Exampl	es			
		Name		Inscription		
ç	coest	2016 Uleare	District Prover Atlank	During the 2016 United Depth Prove Application Trans and a samption amongs BPC automation against a number of Notas 27		
÷	9500	APT28		LPT28 an perfer local free muchs to stimule evidencia, 2001		
Y	6008	APTER		APTER has used found hore techniques to attempt account rooms when passwords and view on when passwords hashes are consultates. ³¹		
č	deper	48728		JUT 20 has used formati to remail understatu. ¹⁴		
Ŷ	40473	Categolier We		Categorier Intelliger has a resolute to perform have from attracts on a system ¹⁰⁰		
ž	41722	Chane		Chease conducts from three annulas against 60% services to gain trans against 60% and against 60% and against 60% and against 60% and against 60% against 60\% agai		
	\$144	CacitrapEre		Dashhagilar san huan Nata kugaled yar undantaka kotok a netwoli kanja ¹⁰		
	00155	DarkVishope		Sublidarys and humfnes statics static type lass. ¹⁰		
	docar	Draganty		Disport, has ensempted to loss from condentials to pair access. ²¹¹		
	60068	End.		FIGE two has used the tool GET2 Prevention in loss for environ logic and hardwooder condentials, ¹⁶ 010		
2007	60711	fox X25an		Pro Chan-has trace front 309 uniterial/19		
ccess v	0100	HEXING		HC00FTHs used from firsts attacks to comparison with predential, 74		
	00099	Kening		Vising the interpret to from these them and 10x1/10		
ž	0004	0.01		COTINg has used bruck those techniques to determine and the control of the contro		
	C0022	Operation Dre	ari Juk	During Operation Desemulation Laborate Broade Advancement Index appairest administrators assessed. ¹⁰⁸		
Interception	00378	PeakC2		Praid 20 has read-out for the optional attriviation and AD usan accounts (M		
vednesi necericov	00583	Pyse		Pyss has used hole force anerges against a certain management control e, as well as some Active Diversity accounts 🏁		
Y	9246	Geblie		Dalder on confut half free media to capitor ordenia), VP000		
n Cartificates	00011	Ture		Turk may exempt to connect to optime within a international using using part connected and a production of parameters of parameters (24)		
ets 🗸 🗸						
	Mito	gations				
		Mapaton	Description			
~		ALLEVENT	or from outside defined organiza	(a) a subtract of a standard to broad framework can used framework as a standard st 3 tandard standard stand Standard standard stand Standard standard s		
9 9	AHOR	2 Multi-factor Authentication	One multi-factor authentication	The possible, was write much deconsulteration on exemption for persons		
	MHOZ	Passound Policies	Refer to MST publicities when o	weld travershipsing in		
	6103	User Account	Proact/vely reset accounts that a	nkinovin to bę pars of brazdwie oxidenski kilike i innekalely, to akteriokacing brazdwie zavenega.		
v		Varagement				
	Dete	ection				
	10	Data tource	Data Component	Period		
	09901	 Approxion Log 	Application Log Contain	Monitor subvertication logs to spotter and application login to loss of initial documents. If subvertication follows are high then there may be about those entering to gain access to a system care login to loss.		
	0307	r connerd	Comment Aveculian	Monor execute commands and arguments that may use orus more economic to pain ecosts to accounts when passivors or when passivors by when years of hashes are obtained.		

Figure 9: The ATT&CK information provided of the "Brute force" attack

Step 3: Impact assessment

In this final step, we assess the impact together with the success probability using the information provided by MITRE ATT&CK table. In more detail, for each row in the previous table, based on the information of the MITRE table, we check whether FISHY platform implements a detection technique and whether the mitigation identified (and recommended and/or enforced) in FISHY is aligned with the one suggested by MITRE table. Based on this information, we fill the following table:

Document name:	D6.4 IT-2 I	FISHY final release	Page:	23 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



ASSET	IMPACT	Success probability	Notes
Resource limited devices (IoT devices in the three islands)	Low	Low	Not considered in the previous list
Nodes in the edge (e.g., FA - federated adapter)	High	Low	Type 1 and 2 attacks of the previous list
Network nodes	Medium	Low	
IAM	High	Low	Type 3 attack from the above list (Brute force attack)
Blockchain nodes	High	Low	Type 4 attack of the previous list
Web application	Medium	Low	Type 3 attack from the above list (Brute force attack)

Table 3: Success probability assessment for potential attacks

Detection of additional attacks

Another way to use the MITRE ATT&CK framework is the following: to check what can be detected based on specific controls. The rationale behind this choice is the following: in the Farm to fork system, FISHY is capable of detecting threats based on logs and based on traffic analysis. So, we selected first "log" and then "traffic" and the result is shown in Figure 10. The attacks that can be detected based on traffic analysis are marked in orange colour while those that can be detected using logs and not on traffic analysis are marked in green colour. (A subset of the orange-coloured threats are also detected using logs).



Figure 10: The threats that can be detected based on logs and traffic analysis information are coloured (65 out of 80, i.e. 81%)

Document name:	D6.4 IT-2 FISHY final release						24 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



This has an **important implication for FISHY:** FISHY components can detect almost 90% of the identified threats which shows that FISHY is a flexible platform that can be exploited to detect the proliferating attacks that supply chain systems suffer today. As regards mitigation, the flexible FISHY user interface allows for easy registration of multiple mitigation rules which could be drawn from MITRE ATT&CK table.

2.3 Demo script

In this section, we present the script of the FISHY demonstrator for the Farm to Fork use case. The demonstration is organized in the following set of sequels aiming at showcasing:

- FISHY detecting all use-case specific attacks (type 1 to 4 described in D6.1)
- Additional attacks in sequel F (such as DDoS attacks and attacks to exposed ports)
- All stages of the supply chain. This becomes evident by inspecting the supply chain actors involved in the different sequels: Farm (sequel A), transportation company (Sequel B), warehouse/retailer (sequel C), consumer (Sequel D, F) and whole supply chain administrator (Sequel E).





2.3.1 Demo script Sequel A

The aim in this sequel is to demonstrate that FISHY platform detects the attacks of type 1 titled "unauthorized device- wallet ID level". This is an attack more likely to occur in the IoT island that is deployed in the farm. For example, a malicious actor uses an unauthorized device and attempts to enter "fake" information in the F2F platform. In this platform, the IoT devices (through the so-called federation adapter- FA) register information about the fresh products and in this registration, they use a wallet-ID.

Document name:	D6.4 IT-2 I	ISHY final release	Page:	25 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Script

Antony (the malicious farmer that intends to push to the platform fake information) uses a device which has not been registered in the F2F platform.

=	Food Supply C		ashboard	
	SOFIE		Box product Use this form in order to register farming product inside boxes	
÷	Home		Select farm 2 Select boxes Enter product details	
۵	Actions	^	Select farm	
	Box Product		Farms that belong to the farming platform of the actor	
			NEXT	
			*	
			The attempt of the malicious Adapter was detected.	
			Something went wrong when signing the transaction! CLOSE	

Figure 12: Malicious farmer attempts to register fake information through a device (with unauthorised wallet ID)

The FISHY platform detects this event (attack) as shown in Figure 13 through the SACM tool. In this validation, SIA, SPI, TIM and IRO were involved. As shown in the figure, this event has been registered in the FISHY blockchain network as indicated by the green (check mark) symbol on the right-hand side of the event.

FISHY							"8	nhy fa 🙎
IRO Dashboard IRO Dashboard Alerts Configurations	Detailed Reports DataTables containing all informatio DataTable Show 10 • entries	n received from	n monitoring tools				Search:	
	ID	÷	Description	Full Text	Additional info	-	Smart Contracts Verification	i.
	0d05c337-17a3-4ce9-ab90-c0	a83b0d8fa0	Source: SACM	pilot: F2F Sender: AuditingComponent	Sender	Outcome	Verified	
	-			Upatteg at: 202-00-3010202132.007702 Description: AssessmentResultD: 27 AssessmentResultD: 27 AssessmentResultIngodule Severity: 75 AssessmentReseutionD: 79 AssetD: 11 Source: EventCollectionEngine Event: F2F type 1 Attack: WalletD Action: ("Action.type: "ban.dd", "wid:: "0x10070as9f2af68660007038bs682f07Be60566f")	AuditingComponent	Satisfaction		
	1a8fc697-3105-4036-94aa-67	534f9315a9	Source: SACM	pilot: F2F Sender: AuditingComponent	Sender	Outcome	Pending	
				updated_at: 2023-03-3013:02:23.9077762 Description: Auguments: ['I'] AssessmentBesultD: 24 Receiver: AuditingModule Severity: 75 AssessmentExecutionID: 79 AssetD: 11 Source: [PeutCollectionEngine Event: F2F type i attack: WalletID Action: ['action.type': 'bam.ud', 'Wid': '0x10678a99f24f866500703056402f0b78e0056f']	AuditingComponent	Satisfaction		
	2ad4b562+ee5b+d29b+ad15+b2	62315df8e1	Source: SACH	nilot: E2E	2		O Marillant	

Figure 13: Screenshot from the dashboard of SACM that detects the wallet ID attack

Next, to the detection, FISHY platform proposes a policy to be enforced. This policy is generated in IRO and turned to low level policy by EDC, which then enforces it in the F2F use case, as shown in the Figure

Document name:	D6.4 IT-2 I	FISHY final release	Page:	26 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



14. To be more precise, the FISHY platform presents to the actor the suggested policy and asks him/her to confirm he/she wants the policy to be enforced.



Figure 14: Screenshot from the FISHY platform capturing the defined policy.

Now, the F2F platform will no longer communicate with the malicious federation adapter. Instead, the F2F platform displays a message to the attacker (Antony) that the information he tries to register is not accepted.

=	Food Supply C	hain D	ashboard				
	SOFIE			Box product Use this form in order to regist	er farming product inside boxes		
÷	Home			Select farm	Select boxes	Inter product details	
۵	Actions Box Product	^			Select farm Integrated Farm 1 Farms that belong to the farming platform of the actor	_	
						NEXT	
						k	
				FISHY platform wa notify the adminis	illet ID 0x310678a99124fe86650D7038b9e82f0b7Be6D56f ba irator. CLOSE	anned. Please	
SOF	F H2020 project @ Sv	nelivis	colutions S & 2021				

Figure 15: Screenshot from the F2F platform where the inability of the malicious user to enter information is shown.

2.3.2 Demo script Sequel B

The aim in this sequel is to demonstrate that FISHY platform detects the attacks of type 2 titled "unauthorized device- Distributed ID level". This is an attack more likely to occur in the IoT island that is deployed during the transportation. For example, an adversary uses an unauthorized device (DID) and attempts to enter "fake" information regarding the conditions during the transportation of the fresh vegetables in the F2F platform. In this platform, the IoT devices (through the so-called federation adapter) register information about the fresh products and in this registration, they use a DID.

It is work pointing out that both sequels A and B refer to cases where a malicious actor uses (different) exploits the information attached to a device in an IoT island of the supply chain to attack and compromise the relevant data. The difference is that in sequel A the malicious actor compromises the wallet ID while in sequel B the device's DID to attack the supply chain. Both ways can be employed in the IoT islands deployed in any of the supply chain steps.

Script

Bob (the adversary that intends to push to the platform fake information) uses a device which has not been registered in the F2F platform.

Document name:	D6.4 IT-2 I	FISHY final release	Page:	27 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



≡ Food Su	pply Cha	in Da	shboard		LOGOUT
sor	È			Farm handover Use this form is order to register boxes handed over by a farming actor	
A Home				Select transport	
Actions Register Box		^		Select transport Integrated Transporter 1 Transport which that the actor is correctly using	
Register Box Se	Islon			NEXT	
Handover from	roducer			k	
Handover to wa	ehouse i	-			
Handover to sur	ermark_	ап ±/			
			The at	tempt of the malicious Adapter was detected.	
SOFIE H2020 proj	ct @ Svne	ixis S	Nutions S.A. 2021	Something went wrong war taken of na does not pass nos token vermication CLOSE	

Figure 16: The adversary (transporter) attempts to register fake information through a device (with Distributed Identified that has not been assigned by the F2F platform)

The FISHY platform detects this event (attack) as shown in Figure 17 through the Wazuh tool. In this validation, SIA, SPI, TIM and IRO were involved.

😔 Elastic														0 0
■ WAZUH > / Modules / Security	event	ls												
Security events (0)														
Dashboard Events														🖗 Explore agent
🖫 🗸 Search									KQL	≣∨ Las	t 24 hours		Show dates	C Refresh
manager.name: localhost.localdomain + Add filter														
wazuh-alerts-* ∨ 🤤								226 hits						
Q Search field names						Jun 22, 2023	3 @ 13:51:12.698 - Ju	n 23, 2023 @ 13:51:12.6	Auto	· ·				
Filter by type 0 Selected fields i it agent name i it nule description i it nule id i	Count	200 150 100 50 0	15.00	18.00		2100	00.00	03.00			00.00	09:00	12:00	
ruio.level Available fields							tin	nestamp per 30 minutes	5					
t agent.id		Time	•	agent.name	rule.descrip	ption							rule.level	rule.id
t data.command t data.dstuser	>	Jun	23, 2023 0 13:51:08.795	localhost.localdo main	Synelixsi NiJ9.eyJz	s unauthorized de dWIiOiIweDk5MjQ1Y	vice, DID level. TkyOTAyOUQ4YjVGNk	9XFFSoIjt7ehKPARh8X MxMmI3ZDgwMTU4ZjcxZi	cNt, name kFDMTkxOT	AberonIoT, gifQiYM8au	token: eyJ0eXA101 w-Ewq32MFSW11F5C96	JKV1QiLCJhbGci0iJIUzI1 51JNLIY75mcCD9Dc34	3	300004
t data.gid	>	Jun	23, 2023 0 13:51:03.792	localhost.localdo main	Synelixsi	s unauthorized us	er, IP level. use	r from 163.23.164.1	66				3	300006
data.metadata.attacker_did	>	Jun	23, 2023 0 13:50:58.791	localhost.localdo main	Synelixsi: NiJ9.eyJz	s unauthorized de dWI101IweDk5MjQ1Y	vice, DID level. TkyOTAyOUQ4YjVGNk	mjjls34UQxVdvxEETyM MxMmI3ZDgwMTU4ZjcxZi	hLD, name kFDMTkxOT	AberonIoT, gifQiYM8au	token: eyJBeXA101 w-Ewq32MFSW11F5C96	JKV1Q1LCJhbGc101JIUzI1 51JNLIY75mcCD9Dc34	3	300084
data.metadata.device_name data.metadata.ip	>	Jun	23, 2023 0 13:50:53.789	localhost.localdo main	Synelixsi NiJ9.eyJz	s unaüthorized de dWIi0iIweDk5MjQ1Y	vice, DID level. TkyOTAyOUQ4YjVGNk	mjjls34UQxVdvxEETyM MxMmI3ZDgwMTU4ZjcxZi	hLD, name kFDMTkxOT	AberonIoT, gifQiYM8au	token: eyJ0eXA101 w-Ewq32MFSW11F5C96	JKV1QiLCJhbGci0iJIUzI1 5iJNLIY75mcCD9Dc34	3	300004
 data.metadata.token data.metadata.user 	>	Jun	23, 2023 0 13:50:48.792	localhost.localdo main	Synelixsi NiJ9.eyJz	s unauthorized de dWI101IweDk5MjQ1Y	vice, DID level. TkyOTAyOUQ4YjVGNk	mjjls34UQxVdvxEETyM MxMmI3ZDgwMTU4ZjcxZi	hLD, name kFDMTkxOT	AberonIoT, gifQiYM8au	token: eyJ0eXA101 w-Ewq32MFSW11F5C96	JKV1QiLCJhbGci0iJIUzI1 5iJNLIY75mcCD9Dc34	3	300004
t data.pwd t data.sca.check.command	>	Jun	23, 2023 0 13:50:43.786	localhost.localdo main	Synelixsi: NiJ9.eyJz	s unauthorized de dWI101IweDk5MjQ1Y	vice, DID level. TkyOTAyOUQ4YjVGNk	mjjls34UQxVdvxEETyM MxMmI3ZDgwMTU4ZjcxZi	hLD, name kFDMTkxOT	AberonIoT, gifQiYM8au	token: eyJ0eXA101 w-Ewq32MFSW1lF5C96	JKV1QiLCJhbGci0iJIUzI1 51JNLIY75mcCD9Dc34	3	300004
t data.sca.check.compliance.cis	\.	Jun 3	23. 2023 0 13:50:38.784	localhost.localdo	Synelixsis	s unauthorized us	er. IP level. use	r from 163.23.164.1	66				3	300006

Figure 17: Screenshot from the dashboard of Wazuh that detects the DID attack

Document name:	D6.4 IT-2 I	ISHY final release	Page:	28 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Next, to the detection, FISHY platform proposes a policy to be enforced. This policy is generated in IRO and turned to low level policy by EDC which then enforces it in the F2F use case, as shown in the Figure 18.

Autoscroll:0n FullScreen:0ff Timestamps:0ff Wrap:0ff [24/Jun/2023 12:25:40] - [fishy.management.commands.action_parser:46] - [INFO] [x] Received {'action': 'ban_did', 'did': 'Ju8fj4qL52q53odR545kXR', 'command': 'BAN DID: Ju8fj4qL52q53odR545kXR' [24/Jun/2023 12:25:40] - [fishy.management.commands.action_parser:78] - [INFO] [x] Created action=3

Figure 18: Screenshot from FISHY where the defined policy to protect against the DID attack is presented.

Finally, the F2F platform displays a message to the attacker (Bob) that the information he tries to register is not accepted.

=	Food Supply Cl		ashboard	
	SOFIE		Warehouse handover Use this form in order to handover boxes to a given warehouse Collect boxes Collect Col	
 ≎	Home	^	Select transport	_
	Register Box Register Box Session		Integrated Transporter 1 *	
	Handover from producer	**	k	
	Handover from wareho	•		
	Handover to supermark	Ë		
				ed
			action and when a new request is made, FISHY platform DID Julff4g52qt30dR845XXR banned. Please notify the administrator cLOSE	
SOFI	E H2020 project © Syr	nelixis	iolutions S.A. 2021	

Figure 19: Screenshot from the F2F platform where the inability of the malicious user to enter information is shown

Before proceeding to the presentation of sequel C, it is worth pointing out that both Wazuh and SACM operate in a rule-based manner. However, in FISHY we have opted to integrate both of them because: a) Wazuh is an open-source component. Integrating such a component, we aim at demonstrating that FISHY platform is capable of easily integrating components that will emerge in the future at low cost; b) even if the open-source components currently available are discontinued in the future, FISHY has integrated its own component which is powerful as it embraces the event calculus logic that Auditing module of SACM uses, via which an operator of the FISHY platform can write its own security rules beyond field-value and time / event-count based custom modelling of Wazuh. Furthermore, being able to detect an attack employing different components with potentially different pricing models, makes the platform stronger and more flexible, as our customer may prefer one over the other or decides to use multiple components for redundancy.

2.3.3 Demo script Sequel C

The aim in this sequel is to demonstrate that FISHY platform detects the attacks of type 1 titled "unauthorized device- wallet ID level". This is an attack more likely to occur in the IoT island that is deployed in the warehouse. For example, the attacker uses an unauthorized device and attempts to enter "fake" information in the F2F platform regarding the conditions under which the fresh vegetables are maintained in the warehouse. In this platform, the IoT devices (through the so-called federation adapter) register information about the fresh products and in this registration, they use a wallet-ID.

Document name:	D6.4 IT-2 I	ISHY final release	Page:	29 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Script

Chris (the attacker pretending to be the malicious warehouse operator that intends to push to the platform fake information) uses a device which has not been registered in the F2F platform.

=								
	SOFIE			Box warehouse Use this form in order to assign bo	ores to individual sections of a given warehouse			
n	Home			Select warehouse	Select boxes	Assign boxes		
٥	Actions	^			Select house			
	Box warehouse				Boxes that are going to be assigned to a section inside the watehouse			
	Packetize product	۵		BACK		NEXT		
			Here, the w	arehous	se emplovee is re	egister	ring	
			the boxes	s transp	orted to the war	enous	e.	
SOF	IE H2020 project @ Sy	melixis :	Solutions S.A. 2021					

Figure 20: Malicious warehouse operator attempts to register fake information through a device (with unauthorised wallet ID)

The FISHY platform detects this event (attack) through the SACM tool (similarly to scenario A). In this validation, SIA, SPI, TIM and IRO were involved. Next, to the detection, FISHY platform proposes a policy to be enforced. This policy is defining that the detected malicious wallet ID should be banned and it is generated in IRO and turned to low level policy by EDC which then enforces it in the F2F use case, as shown in the Figure 21.



Figure 21: Screenshot from the dashboard of FISHY where the defined policy is presented.

Finally, the F2F platform displays a message to the attacker (Chris) that the information he tries to register is not accepted.

Document name:	D6.4 IT-2 FISHY final release					Page:	30 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



					LOGOUT
	SOFIE			Box warehouse Use this form in order to assign boxes to individual sections of a given warehouse	
÷	Home		_	Select warehouse	
٥	Actions	^		Select workhouse Integrated Warehouse 1	
	Box warehouse			Choose a warshouse that is part of your is?" platform	
		2			
				×	
				FISHY platform wellet ID 0xa/234g84504874488F0625fa35e1C8tc4a046EC banned. Please audity the administrator: CL05E	

Figure 22: Print screen from the F2F platform where the inability of the malicious user (Chris) to enter information is shown

2.3.4 Demo script Sequel D

The aim in this sequel is to demonstrate that FISHY platform detects the attacks of type 3 titled "unauthorized user". Assuming that this attack occurs from a consumer that uses the F2F platform to check the conditions under which the products he/she is about to purchase were experienced. For example, the attacker uses the wrong password or issues a brute force attack to gain access and potentially alter information relevant to specific products either to create a mesh or to diminish the value of specific brands.

Script

David (the attacker pretending to be the consumer that intends to access and potentially alter information in the F2F platform) tries different combinations of username and password to enter the F2F platform.

SOFIE Login Access the SOFIE dashboard with your seycloak credentia Username dosjiwdr Password I Password I Password is required		SOFIE
SOFIE Login Access the SOFIE dashboard with your Reveloat credentia Usemane dosjiwdr Password I Password is required		
SOFIE Login Access the SOFIE dashboard with your Reycloak credentia Username dcsjiwdr Password I Password is required		
Access the SOFIE dashboard with your Revoltant credentia Username dosjiwdr Password Password is required	SOFIE	Login
dcsjiwdr Password I Password is required		
dcsjiwdr Password I Password is required	Access the SOI	EIE dashboard with your keycloak credentials
Password I Password is required	Access the SO	FIE dashboard with your keycloak credentials
Password I Password is required	Access the SO Username dcsjiwdr	FIE dashboard with your keycloak credentials
Password is required	Access the SOI Username dcsjiwdr	FIE dashboard with your keycloak credentials
Password is required	Access the SOI Username dcsjiwdr Password	FIE dashboard with your keycLoak credentials
- PAIR	Access the SOI Username dcsjiwdr Password	FIE dashboard with your keyclaak credentials
	Access the SOI Username dcsjiwdr Password	FIE dashboard with your keycloak credentials

Figure 23: Malicious consumer attempts to register fake information compromising a user account (brute force attack)

Document name:	D6.4 IT-2 FISHY final release					Page:	31 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



The FISHY platform detects this event (attack) as shown in Figure 24 through the Wazuh tool. In this validation, SIA, SPI, TIM and IRO were involved.

🔗 Elastic		0 0
	ty events	
Security events 0		
Dashboard Events		(1) Explore agent
t data.dstuser	In UZ21NLJ9.eyJZdRE101Iw0k9Mj01YTky0TAy00Q4YjV0MAM#E32DgwHTU4Zjcx2kFDHTkx0Tg1F01VMBauw-Ewg52MFBH1F5C965LJHL1Y75ecC09 Dc34	
data.gid data.home data.nmtadata.attacker_did	Jun 23, 2023 0 13:12:23.434 localbost.localdoms Symelixsis unauthorized device, BD level.sjlsk#UpVeVwETyMCD, name: AberonioT, token: eyJMeXASLANYOBLCAMBOGIDLT In DCH4	3 300004
data.metadata.device_name data.metadata.ip	3 Jun 23, 2023 0 13:12:18.826 localhost.localdoma Symelixeis unauthorized user, IP level. user from 163.23.164.166 In	3 300005
(i) data.metadata.token	Jun 23, 2023 0 13:52:13.024 localhost.localdoma Symelixis: Device AberonIoT has tried to log in 10 times in 2 hours in	10 30005
data metadata user data, pwd	C Expanded document View surrounding	documents View single document
t data.sca.check.command	Table JSON	
data.sca.check.compliance.cis data.sca.check.compliance.cis_csc data.sca.check.compliance.gdpr_IV data.sca.check.compliance.gdpr_IV	r sgent.id 000 k	
t data.sca.check.compliance.gpg_13	③ data.metadata.attacker_did mjjls340QxVdvxEETyM%LD	
t data.sca.check.compliance.hipsa t data.sca.check.compliance.	data.metadata.device_name AberoxIaT	
nist_800_53 t data.sca.check.compliance.pci_dss	Intersection of the second	1F5C9651JNLIY75mcCD9Dc34
t data.sca.check.compliance.tsc	🗇 data.timestamp Jan 26, 2022 0 11:59:36.000	
t data.sca.check.description	f data.type 2	

Figure 24: Screenshot from the dashboard of Wazuh that detects the brute force attack issued by David (masquerading a consumer)

Next, to the detection, FISHY platform proposes a ban-IP policy to be enforced. This policy is generated in IRO and turned to low level policy by EDC which then enforces it in the F2F use case, as shown in the Figure 25.



Figure 25: Screenshot from the dashboard of FISHY where the defined policy is presented.

Finally, the F2F platform displays a message to the attacker (David) that the information he tries to register is not accepted.

This site can't be reached
192.168.2.11 refused to connect.
Try: - Checking the connection - Checking the proxy and the firewall
ERR_CONNECTION_REFUSED
A
Detailo

Figure 26: Screenshot from the F2F platform where the inability of the malicious user (David) to enter the platform is shown

Document name:	D6.4 IT-2 FISHY final release					Page:	32 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



2.3.5 Demo script Sequel E

The aim in this sequel is to demonstrate that FISHY platform detects the attacks of type 4 titled "Attack to blockchain node". This is an attack more likely to occur from a knowledgeable person to insert fake information in the blockchain used by F2F platform. For example, the attacker (Eric) tries to compromise the blockchain node.

Script

Eric (the attacker of the F2F platform) tries to connect to the blockchain node from a device with an IP address that is not whitelisted in the F2F platform. It should be noted that the F2F platform utilizes Quorum, a private blockchain network, along with the Tessera transaction manager. Tessera is responsible for the management of the nodes' public keys. A malicious actor could utilize the knowledge of the port Tessera runs on (usually on 9001) and its API endpoints to get that information (more specifically the */partyinfo* endpoint). Having acquired that information, the attacker could make a transaction and re-write data stored on-chain or insert his/her own data.

Figure 27 shows the output of the user's attempt to retrieve the public keys of the Quorum nodes.



Figure 27: The adversary retrieves the public keys of the blockchain nodes

The F2F platform continuously monitors the activity of the system and maintains a list of whitelisted IP addresses.

Document name:	D6.4 IT-2 FISHY final release					Page:	33 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Should an external connection from an unknown IP occur, then the FISHY platform and more specifically SACM tool is notified as shown in Figure 28. In this validation, SIA, SPI, TIM and IRO were involved.



Figure 28: SACM monitors the IPs being connected to the blockchain node and checks whether these are whitelisted IP addresses.

Next, to the detection, FISHY platform proposes a policy to be enforced. This policy is a ban-IP policy and is generated in IRO and turned to low level policy by EDC which then enforces it in the F2F use case, as shown in the Figure 29. The end result is that the connection with the adversary has been terminated and can no longer have access to the blockchain network.



Figure 29: Screenshot from the dashboard of FISHY where the defined policy is presented.

Figure 30 shows an example of an adversary's attempt to tamper with the data. It should be noted that in this case, the malicious user has managed to find all the necessary information (contract address, ABI, keys) to construct a request and make a transaction in order, for example, to register a new farming platform in the system.



Figure 30: Screenshot from the attempt of the malicious user (Eric) to insert a fake farming platform in the F2F platform

Document name:	D6.4 IT-2 FISHY final release					Page:	34 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Figure 31 shows that the user will be unable to send the request, after the actions of the FISHY platform.

requests.exceptions.ConnectionError: HTTPConnectionPool(host='192.168.1.238', port=32232): Max retries exceeded with url: / (Caused by NewConnection rror('<urllib3.connection.HTTPConnection object at 0x7f63ac6595b0>: Failed to establish a new connection: [Errno 111] Connection refused'))

Figure 31: Screenshot of the output of the malicious user's attempt to insert his/her farming platform in the F2F platform

2.3.6 Demo script Sequel F – VAT component used

As in the F2F supply chain the reduction of the downtime is of prime importance, we have decided to use VAT functionality to check the vulnerability of the nodes hosting the F2F platform. To do so, we first configure VAT tool of the FISHY platform providing the IP address of the node where the F2F platform is deployed.

		a defailet ~
1 VULNERABILITY SCANS	SCAN CONFIGURATION > NEW SCAN	
	1 SELECT SCAN TYPE	TARGET CONFIGURATION
	2 SELECT GENERIC SUITE TYPE	THE REPORT OF
	3 BASIC TARGET CONFIGURATION 4 TASK DETAILS	http://192.168.190.20/sojt
	5 RUN OPTIONS	
	6 SCAN SUMMARY	
		Back Next

Figure 32: Configuration of VAT to scan the F2F platform

Once the scan has been executed, the following screen appears indicating that a medium risk vulnerability has been detected and providing information on ways to mitigate it.

VULNERABILITY SCANS VULNERABILITY SCANS SCAN Download JSON	can report 5:19 PM		×	CURAN -
Vulnerability risk	Vulnerability Click-Jacking vulnerability	0 S	Scanner State A	
desc solution	The application has no prote Clickjacking (User Interface Web user into clicking on so revealing confidential inform pages. The server digital reserver clickjacking attack. The 'K' browser should be allowed to attacks, by ensuring that the	ction against Click-Jacking attacks. edress attack, UI redress attack, UI redressing) is a mething different from what the user perceives they attack of the terrogrammeter while clicking m an "X-Frame-Options" header which means that t ame-Options" HTTP response header can be used t render a page inside a frame or iffame. Sites can u c content is not embedded into other sites.	malicious technique of tricking a are clicking on, thus potentially on seemingly innocuous web his website could be at risk of a to indicate whether or not a see this to avoid clickjacking	
-		•	Close	
STATUS	pont	COUNT	1	
STARTED	23.06.2023 13:45:19	INTERVAL	1	
FINISHED	23.06.2023 13:47:33	START AFTER	1	
LAST RUN	23.06.2023 13:47:33	UPDATED	1	
NEXTRUN				

Figure 33: Results of the VAT scan of the F2F platform

VAT is also used to monitor the availability of all the nodes comprising the supply chain platform as shown in Figure 34.

Document name:	D6.4 IT-2 FISHY final release					Page:	35 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	rted	Finished	Result	Output uris
13.0	06.2023 16:22:14	13.06.2023 16:22:33	Report	container_output_1686662552146.txt cscan-log.txt genscan-out.json
13.0	06.2023 16:19:04	13.06.2023 16:19:56	Report	container_output_1686662394373.txt cscan-log.txt genscan-out.json
12.0	06.2023 17:12:57	12.06.2023 17:13:49	Report	container_output_1686579228491.txt cscan-log.txt genscan-out.json
- Andrewski - A				
RUN	US DONE		COUNT	1
STAT STAT	US DONK RTED 13.06.20)23 16:22:14	COUNT	1 4 /
STAT STAT	US DONE TYED 13.06.20 SHED 13.06.20	D23 16:22:14 D23 16:22:33	COUNT INTERV START A	1 1 PTER /
STAT STAT FINIS LAST	US 00000 RTED 13.06.20 SHED 13.06.20 TRUN 13.06.20	223 16:22:14 223 16:22:33 223 16:22:33	COUNT INTER/J START A UPDATE	1 L / TTER / D /

Figure 34: VAT monitors the availability of nodes

In case a node is down, this is promptly detected by VAT. We have on purpose closed a node and VAT has detected it as shown in Figure 35.

	VULNERABILITY SCAN REPORT Jun 13, 2023, 4:22:14 PM Download JSON	5			×	
	Vulnerability risk Information (1)	 Vulnerability Port 32232 on host 192 	.168.1.236 is closed.	Scanner nmap	÷ ۲	
				cscan-log.txt genscan-out.json		
1	13.06.2023 16:19:04	13.06.2023 16:19:56	Report	container_output_	1686662394373.txt	

Figure 35: VAT has detected that the port is closed

2.3.7 Demo script Sequel F – PMEM component used

The aim in this sequel is to demonstrate that FISHY platform detects the attacks of Distributed Denial of Service (DDoS) attack. This is an attack which more likely to occur on the VM where the services of the F2F platform is running. For example, an adversary tries to send multiple illegitimate requests to different services to put the platform in such a condition where legitimate services are delayed by the system; or in the worst case, the system enters into a denial-of-service state, if the attack is successful. To detect this attack PMEM is used, which utilizes machine learning approaches to detect the normal or the abnormal behaviour of the system.

To do this, the real time network traffic is captured from the platform and then it is sent to the PMEM tool in the FISHY control services continuously. As it is observed in the figure below, the captured flows contain normal traffic which is sent to the PMEM and different traffic statistics are shown.

Document name:	D6.4 IT-2 FISHY final release					Page:	36 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final




Figure 36: PMEM dashboard showing the traffic of the system under examination

The detection result of PMEM when normal traffic is detected to the system is shown (Figure 37) as follows:

						Last So	an Results				
eports	C	SV Excel	Timestamp	Source.IP	Destination.IP	Protocol	Frequency	Predictions	Description	Search:	Severity
	1	F2F	26/07/2023 01:45:06	8.6.0.1	8.0.6.4	0	1	Benign	Benign Traffic is detected	0.02083333	Low
	2	F2F	26/07/2023 01:45:06	193.145.14.196	192.168.190.240	17	1	Benign	Benign Traffic is detected	0.02083333	Low
	3	F2F	26/07/2023 01:45:06	192.168.190.240	8.8.8.8	17	40	Benign	Benign Traffic is detected	0.83333333	High
	4	F2F	26/07/2023 01:45:06	192.168.190.240	192.168.169.189	6	1	Benign	Benign Traffic is detected	0.02083333	Low
	5	F2F	26/07/2023 01:45:06	192.168.190.145	192.168.190.240	6	1	Benign	Benign Traffic is detected	0.02083333	Low
	6	F2F	26/07/2023 01:45:06	192.168.190.20	192.168.190.240	6	1	Benign	Benign Traffic is detected	0.02083333	Low
	7	F2F	26/07/2023 01:45:06	83.235.169.221	192.168.190.240	6	3	Benign	Benign Traffic is detected	0.06250000	Low

Figure 37: PMEM dashboard showing the statistics of the traffic per connection.

PMEM gives the information about the different flows in the network as well as different useful statistics about traffic share and severity of the attacks. Then we intentionally simulate the scenario of a DDOS attack on the F2F platform. This malicious traffic along with the normal traffic is captured and sent to the PMEM tool. The traffic analysis shows that something abnormal is happening in the network.

Document name:	D6.4 IT-2 I	2 FISHY final release					37 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final





Figure 38: PMEM dashboard showing the statistics which show the results of the Machine Learning model (which classifies the traffic in benign and suspicious)

Last Scan Info								Search:			
	Pilot	Timestamp	Source.IP	Destination.IP	Protocol	÷.F	requency	Predictions	Description	Traffic.Share	Severity
)	F2F	26/07/2023 01:55:13	192.168.190.240	192.168.169.189	6		3328	DDOS-HTTP-Attack	DDOS attack is detected.	0.4955330554	High
0	F2F	26/07/2023 01:55:13	192.168.169.189	192.168.190.240	6		3267	DDOS-HTTP-Attack	DDOS attack is detected.	0.4864502680	Hig
1	F2F	26/07/2023 01:55:13	83.235.169.221	192.168.190.240	6		1	DDOS-HTTP-Attack	Severity is low	0.0001488982	Lov
2	F2F	26/07/2023 01:55:13	0.8.0.0	245.129.128.0	0		1	Benign	Benign Traffic is detected	0.0001488982	Low
3	F2F	26/07/2023 01:55:13	8.6.0.1	8.0.6.4	0		1	Benign	Benign Traffic is detected	0.0001488982	Lou

The prediction result of the PMEM for the network flows is as follows:

Figure 39: Details of the PMEM prediction results as shown in the PMEM dashboard

The PMEM has detected specific IP address which are trying to perform a DDOS attack, also including the frequency of the specific combination of source IP and destination IP. The severity of the attack is related to its computed frequency. The system shows, for instance, that the 3rd row in the table is considered a DDoS attack with low severity because the frequency is only 1, whereas the two first rows are considered real DDoS attacks because the frequencies are higher than a specific threshold.

2.4 FISHY-enabled security enhancement in F2F supply chain

As has been shown in the previous section, with the integration of the F2F IT system with FISHY, a set of interesting (to the actors) and important attacks are detected and mitigated. Additionally, we have realised that the different components of the FISHY platform can detect more attacks that those presented above: generating additional security probes, FISHY platform can detect attacks to additional points in the supply chain IT platform based on Wazuh and SACM and also, analysing traffic at different network levels or network islands, based on PMEM additional parts of the supply chain system can be protected. As has been discussed in section 2.2, analysing log information and performing Machine learning based traffic analysis enables the detection of a variety of attacks.

Document name:	D6.4 IT-2 I	ISHY final release				Page:	38 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



With respect to the attack of interest to the use case partners, these are detected and mitigated by involving a subset of components of the FISHY platform. In this subset, we can distinguish another subset that is involved in the detection and mitigation of ALL the attack types and the rest are involved in the detection of specific attacks. The full list of FISHY components is included in the following table where in the column "used in F2F" we have indicated the subset that is triggered in our scenarios. In the column titled "notes" we have mentioned those included in specific attacks (and not in the rest).

FISHY Component	Components	Used in F2F	NOTES
SPI	Identity Manager	YES	
	Data Management	YES	
TIM	PMEM	YES	Used for the ML-based detection of Attacks
	XL-SIEM	NO	
	RAE	NO	
	VAT	YES	
	WAZUH	YES	2 out of the 4 F2F attacks are detected by WAZUH
	Trust Monitor	NO	
	Zeek	NO	
	Smart Contracts	YES	
SACM	Evidence Collection Engine	YES	2 out of the 4 F2F attacks are detected by ECE
	Auditing Mechanism	YES	
IRO	Intent Manager	YES	
	Knowledge Base	YES	
	Policy Configurator	YES	
	Dashboard	YES	
	Learning & Reasoning	YES	
EDC	Controller	YES	
	Register & Planner	YES	
	Enforcer	YES	
SIA	loT Gateway	YES	
FISHY appliance	LOMOS, PMEM	YES	

Table 4: The FISHY components employed in the detection of F2F attacks.

Document name:	D6.4 IT-2 I	FISHY final release	Page:	39 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



2.5 Improvements compared to IT-1 and final assessment

In this 2nd round of piloting, the following main technical changes were tested:

- 1. Updated version of the dashboard.
- 2. Integration of additional components for attack detection (PMEM, VAT) apart from updated version of SACM and Wazuh.
- 3. Integration of smart contracts component. This component enhances the validity of the information/evidence provided by FISHY platform as the information about threat detection and policy enforcement is registered in the FISHY blockchain network and thus, this information is immutable. This implies that when an actor of the supply chain claims that an attack has occurred, this can be verified by the FISHY platform in an immutable manner.
- 4. Updated functionality of IRO-EDC giving the option to the administrator to control whether the FISHY-suggested policy will be deployed.
- 5. Deployment of SIA and FISHY appliance on premises with direct implications in the deployment options.

To assess the FISHY platform as objectively as possible,

- 1. first, the people from Synelixis and Entersoft working in the project performed the tests reported in section 2.3 (plus additional ones not reported in this document).
- 2. then, we presented the platform and asked colleagues outside the project teams and outside of the R&D teams to do so in a workshop that we held internally with four people from Synelixis and 3 from Entersoft. We call this group "external" group, although they are employees of FISHY partners as they are not engaged with the project and not engaged in Research activities.

The first group, initially focused on the comparison with the previous assessment reported in D6.2.

Topic of D6.2	Potential Improvement stated in D6.2	Result from assessment in M36
Validation of SCM	A potential improvement would be to allow the user to define the rules for attack detection through a dedicated graphical interface	The updated dashboard for the configuration of the detection tools (not only of SACM) was found to be satisfying allowing the user to set their own rules and thus flexibly configure the conditions which reveal an attack.
Validation of TIM	A potential improvement would be to allow the user to define the rules for attack detection through a dedicated graphical interface. Additionally, with respect to PMEM component, this was deployed in F2F infrastructure (namely in Synelixis' premises) and analyses the information relevant to the internal network where the platform is deployed. This is then passed to ML algorithms enabling anomaly detection. A concern that was raised and is relevant to the commercialisation of the PMEM component is whether the company operating the F2F	Same as above In the 2 nd phase, the ML algorithms of PMEM were trained with datasets that the use case owner provided fully controlling what was being shared with the people configuring the PMEM. Thus, any concern of confidentiality of the network data was removed.

 Table 5: Improvements with respect to the feedback provided by the 1st pilot round.

Document name:	D6.4 IT-2 I	FISHY final release			Page:	40 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	solution would be willing in exposing the information captured from its internal network to the PMEM operator.	
Validation of EDC		No improvement for EDC was suggested. However, in its new version, the FISHY platform leaves the user to decide whether the FISHY suggested policy that could mitigate the attack will be enforced.
Validation of IRO/ dashboard	A potential improvement anticipated to arrive at IT-2 is to allow the operator set specific rules for threat detection.	Fully accomplished.

Next, the "external" group answered/commented on the following topics:

- **Easiness to use and user friendliness:** Average rating 4.1 (in 5-point Likert Scale), which was considered very good for a platform resulting from a research project.
- Security improvement: The question we asked was: "what would you say if you were to quantify how much more secure is now the platform?". From the discussion that was raised, the answers converged towards the following key points:
 - The platform seems to efficiently detect the main attacks of interest.
 - The flexibility provided by the dashboard makes the operators feel they control what happens in the platform they operate.
 - The flexibility in detection offered by the different tools make the operators feel they can defend a wide range of attack.
 - The FISHY dashboard with its clear presentation of events leaves time to the operator to focus on configuring the platform to detect additional attacks.
 - The immutability of the events guaranteed by the introduction of the blockchain technology and the registration of events in the blockchain network, open the door to IoT vendors to persuade IT platform vendors to consider integrating IoT devices by less popular vendors, thus fostering competition.
- To assess whether the multiple **deployment options** are of interest to the buyers, we asked the group: "deployment options: are they important?". They all found that they are very important as the deployment in each supply chain is different and tailored to the actors of the chain. One of the main business lines of Entersoft is software customisation for big supply chain actors. So, having the option to deploy on premise or on hybrid approach the platform and decide the split of components is offering huge and valuable flexibility.

Other comments we received:

- At the beginning, it was not easy for us to understand how the platform is connected to the IT platform of the supply chain. The user manual helped but needs to be accompanied by a video.
- Not easy to understand the flexibility of the platform. Somebody needs to delve into the details to find out.

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					41 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



2.6 KPIs satisfaction

In the Farm to Fork use case, we have three KPIs identified at the proposal writing stage and another two identified during the project lifetime while discussing with the end users.

In *the Description of Action*, the following three targets and relevant KPIs have been defined:

Pilot specific project target	Target value	Achieved value	Comments
Provide mechanism for evidence-based data sharing	≥ 2 interledger technologies	3 in the pilot(Ethereum public, Quorum and KS,- a blockchain technology developed by GuardTime) any in the future since the evidence sharing is technology agnostic	All the events (evidence) are kept in blockchain supporting for F2F use case any interledger technology.
Reduce monetary losses related to auditing services	> 40% compared to current methods	Achieved	Fully automated auditing through SACM and VAT
Provide negotiated and verified payments of resources	≥ 3 involved stakeholders	Any payment and transaction relevant to the real life supply chain is irrelevant to FISHY. With respect to actors, 4 were involved in the pilot (Farmer, transporter, warehouse operator and consumer)	Cybersecurity protection at multiple layers and points has been demonstrated at the pilots.
Provide mechanism for evidence-based data sharing	≥ 2 interledger technologies	3 in the pilot (Ethereum public, Quorum and KS), any in the future since the evidence sharing is technology agnostic	All the events (evidence) are kept in blockchain supporting for F2F use case any interledger technology.

Table 6: Satisfaction of KPIs defined in the DoA

From the table above, it is evident that all the initially defined KPIs have been reached.

Furthermore, with respect to the KPIs defined in D6.1 during the project lifetime, the achieved values today exceed both the target values and the values achieved in M24. It is important to note that for the number of threats that can be detected, FISHY platform is in the position to protect against large numbers of types upon appropriate configuration of the different components.

Table 7: Satisfaction of KPIs defined in D6.1

Metric ID	Metric description	Туре	Target value	Achieved value in M24	Achieved value in M36
SC1_B1	Number of interledger technologies supported	Business and technical	2	3 (Ethereum public, Quorum and KS)	any (as the operations are blockchain technology agnostic)
SC1_T1	Number/Types of threats that can be detected	Technical	3	4	6

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					42 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



3 FISHY validation in Wood-based Panel Trusted Value-Chain

3.1 Introduction

Following the detailed description of the Wood-based Panels Trusted Value-Chain scenarios and use cases in deliverable D6.3, the following section describes the work developed and improvements made since, to ensure the validation of FISHY in iteration 2 (IT-2), therefore concluding the pilot activities.

3.2 Wood-based Panel Trusted Value vertical application and attack modelling

As described in D6.3, the Wood-based Panels Trusted Value-Chain use case was redefined in 2 parallel scenarios to allow a broader value chain coverage. Several components were implemented in order to deliver to the FISHY platform information from three distinct points of the deployed Sonae Arauco's IoT platform (Figure 40), plus one extra connection point to the SAP web dispatcher (Figure 41). Therefore, FISHY platform:

- (1) Collects information on Network Infrastructure (WLAN Controller);
- (2) Collects information from the Sonae Arauco Infrastructure, systems and IoT devices that are located, some on-prem and others in Azure Cloud
- (3) Collects information on IoT Hub;
- (4) Collects information on the SAP web dispatcher.



Figure 40: The connected factory architecture and its interconnection with the FISHY Platform in the FRF

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					43 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final





All cyber agents have a similar challenge regarding the communications with the tools: they are not integrated inside the FRF, but rather located in remote infrastructures that are not part of the FRF. Therefore, since the FRF has the flexibility to easily accommodate external infrastructures and allow their communication with the FISHY elements, the remote infrastructures ran a VPN tunnel that enables the connection with the SIA component in the FRF (since this last one is hosted in the 5TONIC laboratory premises In Madrid). Afterwards, the SIA module integrates this infrastructure as an external site, providing it with connectivity to the FISHY modules using the IRO to attach the cyber agents and data collector inside the corresponding inter-site networks, while using the NED component to perform the secure link-layer communications between the components.

After establishing the architecture and outlining the nodes involved in the collection and transmission of information within the cybersecurity framework, it is essential to enunciate the list of attacks identified for the UC validation during the lifetime of the project:

- Type 1: Unauthorized device: rogue device (IoT infrastructure)
 - Metadata: {IP addresses; Mac Addresses; Time Stamp}
- Type 2: Process incident by denial of service (IoT Hub and Sap Web Dispatcher)
 - Metadata from IoT Hub: {Time Stamp, source IP, destination IP}
 - Metadata from SWD: {Time Stamp, source IP, type of request, message, response code, message size, machine, net}
- Type 3: Unauthorized access by session hijacking (Windows servers)
 - Metadata from IoT Hub: {Time Stamp, source IP, destination IP, user}
- Type 4: Unauthorized access by brute force (Windows servers and Sap Web Dispatcher)
 - Metadata from Windows servers: {Time Stamp, source IP, destination IP}
 - Metadata from SWD: {Time Stamp, source IP, type of request, message, response code, message size, machine, net}
- Type 5: Malicious URL (Sap Web Dispatcher)

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					44 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



- Metadata: {Time Stamp, source IP, type of request, message, response code, message size, machine, net}
- Type 6: IoT network traffic adulteration (IoT Infrastructure)
 - Metadata: {duration; flow count; received bytes; sent bytes; gateway}

To further examine and understand the consequences of these threats and attacks, which can impact the integrity, availability and security of the value chain, we have studied and modeled them into known frameworks to make sure that a) we are actually considering adequate supply chain attacks, b) we are using techniques that are up to date with the state of the art and c) FISHY framework guarantees there is room for improvement in the future and additional attacks can be latter detected and prevented.

Drawing upon established attack modeling frameworks, namely ENISA and ATT&CK, we were able to explore various attack vectors and their potential impact on different components of the use case. By leveraging on these framework attack models, we can gain insights into the tactics, techniques, and procedures employed by threat actors targeting the value chain.

The ENISA model (introduced in chapter 1) provides a comprehensive framework that outlines different types of attacks across the supply chain, focusing on various stages from sourcing to product delivery.

- Attack Techniques Used to Compromise the Supply Chain
- Supplier Assets Targeted by the Supply Chain Attack
- Attack Techniques Used to Compromise the Customer
- Customer Assets Targeted by the Supply Chain Attack

In the following Table 8 the attacks used as guiding reference for FISHY integration with the WBP use case are depicted inside the framework. As an example, the third attack involves unauthorized access and control of an existing login ID on different servers which typically involves the unauthorized takeover of an active session between a user and a server. The attacker gains control by exploiting vulnerabilities in the session management process (*Attack Techniques Used to Compromise the Supply Chain*), intercepting session tokens, or other means to impersonate a legitimate user. The attacker can view and manipulate the active session data performing actions on behalf of the compromised user including opening files and running processes and network connections. If the compromised user has access to sensitive data stored on the server, the attacker can access it and potentially steal that same data. These could include confidential documents, databases, or personally identifiable information of users or clients (*Supplier Assets Targeted by the Supply Chain Attack*). Such data could be used for instance for phishing uses (*Attack Techniques Used to Compromise the Customer*) which would possibly end on an attempt to reach customers direct data (*Customer Assets Targeted by the Supply Chain Attack*).

	SUPPLIER		CUSTOMER				
Attack	Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack			

Table 8: ENISA framework applied to the WBP identified attacks

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					45 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Type 1: Unauthorized device	Physical Attack or Modification (physical intrusion of an unauthorized IoT device)Exploit Security Vulnerabilities 	Data (readings from sensors) Hardware (other IoT devices) Processes (delays, quality issues, shutdowns)	Trusted Relationship (Faulty products can result in financial losses for the customer or affect their own production processes)	Processes Data
Type 2: Denial of Service	Exploiting Software Vulnerability (by flooding down the machine with traffic)	Pre-existing Software Processes (Disrupt or halt critical processes within the supply chain that depend on the targeted server)	Trusted Relationship (exploit the disruption to impersonate the supplier or establish fake channels, taking advantage of the trusted relationship to deceive)	Business data Personal data Financial data (all submitted by the client if the attacker successfully establish a fake replacing communication channel as a legitimate solution) Plus, block of any attempt of communication and/or requests to the suppliers' systems (customer affected not targeted)
Type 3: Session hijacking	Exploiting software vulnerability (exploitation of the server session control mechanism)	Pre-existing Software Data (Manipulate active session data or exfiltrate data)	Phishing Client information (such as orders, addresses, contacts, financial information) illegally obtained from the system that can be	Business data Personal data Financial data

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					46 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



			used in phishing attacks	
Type 4: Brute force	Brute-force (guessing or using applications or scripts as brute force tools to gain unauthorized access)	Pre-existing Software Configurations Data (credentials theft can allow access to technical users giving access to invoking APIs to access client data)	Phishing Client information (such as orders, addresses, contacts, financial information) illegally obtained from the system that can be used in phishing attacks	Business data Personal data Financial data
Type 5: Malicious URL	Malware Infection (trigger a vulnerability to inject code to access the network)	Pre-existing Software Configurations Data (access to other systems and machines with relevant data, connected in the company's premises, by session sniffing)	Phishing Client information (such as orders, addresses, contacts, financial information) illegally obtained from the system that can be used in phishing attacks	Business data Personal data Financial data
Type 6: IoT network traffic adulteration	Physical Attack or Modification (hardware modification) Exploit Software vulnerabilities (taking advantage of software vulnerabilities present in the IoT devices or supporting software components)	Data (readings from sensors) Hardware (IoT devices) Processes (delays, quality issues, shutdowns)	Trusted Relationship (Faulty products can result in financial losses for the customer or affect their own processes)	Processes

Additionally, the ATT&CK framework offers a detailed catalog of adversarial tactics and techniques commonly observed in cyberattacks. By aligning our analysis with ATT&CK, we can map the identified

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					47 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



attacks to specific techniques employed by threat actors. This mapping aids in understanding the tactics used and help in formulating effective mitigation strategies and the detection alternatives.

Just as it was done before for the Farm To Fork use case we now recover the steps of applying the asset/impact-centric approach in this case for the wood based panels use case.

Step 1: System description

The main assets to consider from the wood-based panels use case in FISHY revolve around the IoT infrastructure and EDI communications, both are detailed and described in terms of exposition and potential impact on security proprieties in Table 9.

ASSET	EXPOSITION	IMPACT	Notes
EDGE node (OPC-UA)	LAN	Medium	Types 2, 3 and 4 attacks of the previous list
Shopfloor control	LAN	High	Types 2, 3 and 4 attacks of the previous list
Resource limited devices (IoT sensors)	LAN/Wireless	Medium	Type 1 and 6 of the previous list
SAP Web	Internet	High	Types 2, 4 and 5 attacks of the previous
Dispatcher			list

Table 9: Asset/Impact Synthesis

Step 2: threat modelling

In order to enhance our understanding of the threats and their associated attacks, threat modelling serves as a valuable activity that involves exploring the deployment techniques, tools utilized, and vulnerabilities exploited. To assist with this process, the MITRE ATT&CK Navigator offers a comprehensive overview, as depicted in chapter 2.2. To use this modelling, we have identified the two main data sources used to detect attacks in the use case, which are application logs (Figure 42) and network traffic analysis (Figure 43). The combination of these two sources gives us the complete set of attack techniques that can be detected by FISHY for our use case in Figure 43.





Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege	Change Operating Mode	Network Connection	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update	Brute Force I/O	Damage to Property
Exploit Public-Facing	Command-Line Interface	Modify Program	Escalation	Exploitation for Evasion	Enumeration	Exploitation of Remote	Automated Collection	Connection Proxy	Nobe	Modify Parameter	Denial of Control
Application	Execution through API	Module Firmware	Hooking	Indicator Removal on Host	Network shiming	services	Data from information	Standard Application	Avarm suppression	Module Firmware	Denial of View
Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Discovery	Harocoded Credentials	Repositories	Layer Protocol	Block Command Message	Spoof Reporting Message	Loss of Availability
External Remote Services	Hooking	System Firmware		Rootkit	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Unauthorized Command	Loss of Control
Internet Accessible Device	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Message	Loss of Productivity and
Remote Services	Native API					Remote Services	VO Image		Change Credential		Revenue
Replication Through	Seriation					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Removable Media	Scripting .						Point & Tag Identification		Denial of Service		Loss of Safety
Rogue Master	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Spearphishing Attachment							Screen Capture		Manipulate I/O Image		Manipulation of Control
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Transient Cyber Asset									Rootkit		Theft of Operational
Wireless Compromise									Service Stop		Information
	-								System Firmware		

Figure 43: Attacks that can be detected with network traffic as data source

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					48 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege	Change Operating Mode	Network Connection	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update	Brute Force I/O	Damage to Property
Exploit Public-Facing	Command-Line Interface	Modify Program	lastice	Exploitation for Evasion	Network Celffree	Exploitation of Remote	Automated Collection	Connection Proxy	Alere Sussessie	Modify Parameter	Denial of Control
Superior of Persons	Execution through API	Module Firmware	Hooking	Indicator Removal on Host	Remete Suter Discourse	Services	Data from Information	Standard Application	Plank Command Massage	Module Firmware	Denial of View
Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Discovery	Hardcoded Credentials	Repusitories	cayer Protocol	Block Command Message	Spoof Reporting Message	Loss of Availability
External Remote Services	Hooking	System Firmware		Rootkit	Information Discovery	Cateral Iool Iranster	Data from Local System		block Reporting Message	Unauthorized Command	Loss of Control
Internet Accessible Device	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	message	Loss of Productivity and
Remote Services	Native API					Kemote Services	(/U image		Change Credential		Revenue
Replication Through	Scripting					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Removable Media	User Execution						Point & lag identification		Denial of Service		Loss of Safety
Rogue Master							Program Upload		Device Restart/Shutdown		Loss of View
Spearphishing Attachment							Screen Capture		Manipulate I/O Image		Manipulation of Control
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Transient Cyber Asset									Rootkit		Theft of Operational
Wireless Compromise									Service Stop		Information
									System Firmware		

Figure 44: Attacks that can be detected with both logs and network traffic as data sources (53 out of 80, i.e. 66%)

From the blue boxes highlighted in the Figure 42, we have then revised one-by-one the threats most relevant to our system. Examples are the "default credentials" attack and the "denial of service" attack. Selecting the attack, the MITRE ATT&CK navigators displays all the procedures that an adversary may follow which have been registered in the framework, the mitigation measures identified so far and the detection alternatives.

From this selection we can in-depth analyze each of the threats to our system. As an example, we can select a technique such as "Exploit Public-Facing Application" so that MITRE ATT&CK displays an overall explanation on the technique, procedure examples from dangerous known groups, mitigation actions already successfully deployed to face this attack and finally all the detection data sources that can be used to identify it, which correspond to the data sources the use case provides to FISHY (Figure 43).

MITRE ATT&CK																						Matrices		Tectics		Tech	iques -		Data Sourc	•	Mitigation		Groups	Softwar		Campaign	R	ecurces -	Blog	Contribu	- C	Search Q	
TECHNIQUES Enterprise Mobile Unital Access Drokely Comparise Exploitation of Nemola Services Exploitation of Nemola Services Internal Revices Replacation Through Removable Regionation Through Removable	v v v v v v v v v v v v v v v v v v v	Home - To Expl Adversarie implement An adversa may be fou vulnerabilit	chrispans > 105 - OIT PUDI a may leverage we ations, an assets o any may seek to tar and through online ses. Exposed cost	Explor Public IC-Fac adversaria to operating syst root public-fac tools that so rol protocol o	Facing Applica Cing A exploit interni em, weak de ang applicati a the interne riemote acco	Ap met-fa defense ations e met for coess p	b b b b c ing n s es, etc s es, etc s es s es, etc s es s es, etc s es s es s es s es s es s es s es s	Cat ofware . Targe y may p ports a ound in	ON for initia s of this ovide di d servic Dommo	al acce rectni rect ac res. Ve nly Use	ess im tique r sccess teraion sed Po	nto an in -may be a into a in numt Port may	industri se inten an ICS i bers foi sy be of	trial net ntional 5 enviro or the e of intere	etwork, i ally expo onment expose rest by a	International In	er facin or the pr e ability fication saries	ng softwi surpose o y to move n may pro	are may of remo e into th wide ad	be user te mane e ICS ne versarie	r applic agertien etwork es an ab	ations, u t and vis Publicly ality to ta	iderlyi bility riposi iget a	ng nëtwo ed applic pecific ka	cation cation	s	đ	ID Su) Ta) Pi Ve Cr La	T0819 b-techniq ctic: initia itforms: F rsion: 1.0 nated: 21 st Modifia	ues: 1 Acces Juman May 20 Hd: 091	lo sub-tech s Machine In 20 Aerch 2023 V	niques serface I	Permaini										
Spearphishing Attachment		10000	Name	mpica	Description	ion																																					
Supply Chain Compromise Transient Cyber Asset		60034	Sandworm T	'eam	Sandworm	ann Tea	iarri act	iors exp	oited vu	Inerabi	bilities	rs in GE	Es Cimj	nplicity	y HML a	and Ad	tvantech	h/Broadv	win Wet	Access	i HMI si	oftware v	hich I	ad been	n direc	tly exp	ised to	the int	ernet, ¹⁹¹²														
Wireless Compromise		Mitiga	ations																																								
Persistence	~	ID .	Mitigation			Desc	scription																																				
Privilege Escalation	*	M0948	Application Isol	ation and San	dboxing	App	plicatio	on isola	on will I	limit sh	he oth	her pro	poesses	es and s	system	m featu	ures an e	exploite	d target	can acc	cess. E	xamples	of buil	t in featu	ures a	re soft	rare res	trictio	n policies,	AppLo	sker for Wir	ndows,	and SELin	ux or AppA	lemor fo	or Linux.							
Discovery	* *	M0950	Exploit Protection	on		Wet	eb Appl	ication	irewalls	s may b	be use	sed to I	limit ex	sxposur	ure of ap	opplicat	tions to	prevent	exploit	traffic fi	form rea	sching th	e appli	cation. ⁵	я																		
Lateral Movement	~	M0930	Network Segme	intation		Seg	gment	externa	y facing	; serve	era an	nd serv	vices fr	from th	he rest (of the	network	rk with a	DMZ or	on sepi	iarate hi	osting inf	iestru	cture.																			
Collection	~	M0926	Privileged Accor	unt Manager	ent	Use	e least	privileg	for ser	vice ac	ccour	ants, 14	100																														
Inhibit Response Function	č	M0951	Update Software	e.		Reg	gularly	scan e	temaily	facing	g syste	nema fo	for vulne	nerabilit	ities an	nd esta	ablish pr	procedure	es to rap	pidly pet	tch syst	terns whe	n criti	cai vulne	erabili	ties are	discov	ered th	rough sca	nning a	nd public d	tisclosu	re.										
Impair Process Control	~	M0916	Vulnerability Sci	anning		Reg	gularly	scan e	ternally '	facing	a syste	aems fo	for vulne	nerabilit	ities an	nd esta	ablish pr	procedure	es to raj	pidly per	tch syst	terns whe	n onti	cal vulne	erabili	ties are	discovi	ered th	rough sca	nning a	nd public d	fisclosu	re:										
Impact	•	Detec	tion																																								
		10	Data Source	Data Compo	cent	Det	etects																																				
		D50015	Application Log	Application Content	Log	De	etectin	g softw r inputs	sie explo attempt	oitation ting ex-	in may oploite	sy be ditation.	afficult	t depen	nding o	on the t	tools av	vailable.	Softwa	re exploi	its may	not alwa	ys su:	ceed or	r may o	cause t	ne explo	ited p	rocess to	ecom	e unstable o	or crast	. Web Ap	plication Fi	rewalls	s may dete	ct						
		D50029	Network Traffic	Network Tr Content	affic	Us	lse dee	p packe	inspect	dion to	a look	(for art	rtifacts	s of con	nom	n exploi	it traffic,	c, such a	s known	n payloa	ids.																						

Figure 45: MITRE ATT&CK Exploit Public-Facing Application technique details on procedure examples, mitigation actions and detection sources

Step 3: Impact assessment

From an analysis on the MITRE ATT&CK table it is easily understood that FISHY can have a wide protection coverage for potential ICS attack techniques used to disrupt the supply chain with a noticeable exception to some attack techniques present in the "Impact" column (Table 10). The data sources being used are not sufficient to detect those attacks which can be critical to a production system. That said it is relevant to understand that an attacker in order to reach this production system via a technique from the "impact" column will need to first have initial access to an exposed system, then the attacker will need to be able to have lateral movement to reach it, and a set of other techniques to finally execute an attack to inflict damages such as loss of availability, which ultimately implies that FISHY can and will have a preventive action in the process.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	49 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



In conclusion, based on MITRE table, FISHY potential to detect most techniques and use this detection to either recommend or enforce a mitigation action highly reduces the risks associated with the assets involved in the use case as seen in the Table 10:

ASSET	IMPACT	Sucess Probability
EDGE node (OPC-UA)	Medium	Low
Shopfloor control	High	Low
Resource limited devices (IoT sensors)	Medium	Low
SAP Web	High	Low
Dispatcher		

Table 10: Success probability assessment for potential attacks

3.3 Demo script

For this chapter we demonstrate how FISHY protects our use case specifically from the attacks we defined as critical for the pilot.

In the wood-based panels UC the involvement of crucial supply chain assets is made obvious with the addition of electronic data interchange (EDI) communications in IT-2. Being a system exposed to the internet and a communication bridge between manufacturer, logistic partners and direct clients, there is a high level of cyber-risk inherent, if monitorization is not effective. In addition, operative technology (OT) is also being monitored since IT-1, now further developed with network traffic control using SACM and mitigation recommendations supported by EDC (Figure 46).



Figure 46: High level view of the three main nodes and streams of work affected by the WBP UC in FISHY

The two main systems explored in the three nodes from Figure 46– EDI and OT – also structure how the demos are displayed next. Clients and logistic partners are affected by EDI communications and are displayed in the following 3 types of attacks defined in detail in chapter 3.2:

Document name:	D6.4 IT-2 I	ISHY final release				Page:	50 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final





Figure 47: Priority threats identified and tested on FISHY for the EDI communications

Production monitorization is, as mentioned before, a continuation of the work done in IT-1 with the following 5 types of attacks being displayed:



Figure 48: Priority threats identified and tested on FISHY for the production monitoring

In every sequel piloted the intention was to generate alarms so that the factory has visibility on potential attacks/threats to their systems, based on known techniques.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	51 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



3.3.1 Demo script Sequel A and E

These sequels (representing attack type 2) intend to demonstrate how FISHY reacts and alerts the user on an attempt of denial-of-service of the Sap Web Dispatcher or the IoT Hub. This attack occurs in the Sap Web Dispatcher when a flood of requests is done to the machine in order to block the system and avoid the possibility of communications, in this case impacting the manufacturer by not allowing him to receive any purchase orders from the clients neither the communications from logistic partners for the transportation arrangements. The denial of service was also tested for the IoT Hub which can happen if an attack makes the IoT telemetry (e.g., sensor readings, device status) go higher than the licensed quota, disrupting the network correct functioning – this can happen if for instance he attacker creates or gains control over a large number of compromised IoT devices (be insecure IoT devices with weak or default credentials), forming a botnet.

Simulation of the denial-of-service attack

On Sap Web Dispatcher - The attacker tries to disrupt the system through a denial-of-service attack with a flood of requests. To simulate this a batch script was created invocating 102 requests of the CURL command in the Microsoft Windows environment calling a real URL from the web dispatcher – although in this case the call was only used from one singular machine, the exact same script could be used simultaneously from multiple machines in the internet therefore provoking a denial of service.

C:\te	mp\fishy\runcurl100.bat - Notepad++			- o x
Ele Edit	Search View Encoding Language Se	ttings Tools Macro Bun Plugins Window 2		+ 🔻
608	3 Q 💊 💊 🕹 🕹 🦓 🗋 🗩 C 1	n 🖕 🤏 👒 💁 🔂 1 🏋 🗉 🖏 🖏 🖉	📴 👁 🖲 🖻 🚰 🚰 🔍 🖬 4 🔸 🖬 🖷 🗶 🗑 🖼	G 😸 k K 4- 9- 2
runcu	rl100.bat 🖾			
58	curl -f https:/	.sonaearauco.com:	/ds.html	2
59	curl -f https:/	.sonaearauco.com:	/ds.html	
60	curl -f https:/	.sonaearauco.com:	/ds.html	
61	curl -f https:/	.sonaearauco.com:	/ds.html	
62	curl -f https:/	.sonaearauco.com:	/ds.html	
63	curl -f https:/	.sonaearauco.com:	/ds.html	
64	curl -f https:/	.sonaearauco.com:	/ds.html	
65	curl -f https:/	.sonaearauco.com:	/ds.html	
66	curl -f https:/	.sonaearauco.com:	/ds.html	
67	curl -f https:/	.sonaearauco.com:	/ds.html	
68	curl -f https:/	.sonaearauco.com:	/ds.html	
69	curl -f https:/	.sonaearauco.com:	/ds.html	
70	curl -f https:/	.sonaearauco.com:	/ds.html	
71	curl -f https:/	.sonaearauco.com:	/ds.html	
72	curl -f https://	.sonaearauco.com:	/ds.html	
73	curl -f https:/	.sonaearauco.com:	/ds.html	
7.4	curl -f https:/	.sonaearauco.com:	/ds.html	
75	curl -f https:/	.sonaearauco.com:	/ds.html	
76	curl -f https://	.sonaearauco.com:	/ds.html	
77	curl -f https://	.sonaearauco.com:	/ds.html	
78	curl -f https:/	.sonaearauco.com:	/ds.html	
79	curl -f https:/,	.sonaearauco.com:	/ds.html	
80	curl -f https:/	.sonaearauco.com:	/ds.html	
81	curl -f https:/	.sonaearauco.com:	/ds.html	
82	curl -f https:/	.sonaearauco.com:	/ds.html	
83	curl -f https://	.sonaearauco.com:	/ds.html	
84	curl -f https:/	.sonaearauco.com:	/ds.html	
85	curl -f https:/	.sonaearauco.com:	/ds.html	
86	curl -f https:/	.sonaearauco.com:	/ds.html	
87	curl -f https:/	.sonaearauco.com:	/ds.html	
8.8	curl -f https:/	.sonaearauco.com:	/ds.html	
8.9	curl -f https:/	.sonaearauco.com:	/ds.html	
90	curl -f https:/	.sonaearauco.com:	/ds.html	
91	curl -f https:/,	.sonaearauco.com:	/ds.html	
92	curl -f https:/	.sonaearauco.com:	/ds.html	
93	curl -f https:/.	.sonaearauco.com:	/ds.html	
94	curl -f https:/	.sonaearauco.com:	/ds.html	
95	curl -f https://	.sonaearauco.com:	/ds.html	
96	curl -f https:/	.sonaearauco.com:	/ds.html	
97	curl -f https://	.sonaearauco.com:	/ds.html	
98	curl -f https:/	.sonaearauco.com:	/ds.html	
99	curl -r https:/	.sonaearauco.com:	/ds.html	
100	curi -f https://	.sonaearauco.com:	/ds.html	
101	curi -r nttps://	.sonaearauco.com:	/ds.ntml	
102	curi =r nttps://	.sonaearauco.com:	(ds.ntml	
103				

Figure 49: Evidence of the 102 calls made using the batch script created for the simulation

On the IoT Hub: In order not to endanger real production environment by, for instance, provoking multiple devices to flood the server with overwhelming traffic, to test the correct reaction from FISHY, the telemetry threshold defined as alarming was lowered from 2000 to 1000 during a period of test.

Document name:	D6.4 IT-2	FISHY final release				Page:	52 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



mRemoteNG		- 0 >
Connect	- => RDP -	🚱 Elle View Jools Help
Connections	\$ ×	Cysteragent 61
🚯 😘 🗃 ģi		("count": 1074, "total": 1074, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0833C2B-41AF-4F41-5571-7FDC95706CBD/RESOURCEOROUPS/IOTINEM-P-HE-ROOI/PROVIDERS/HICROSOFT.
1.6		DEVICES/IOTHURS/IOTHURS/IOTHUR*, *time*: *2022-05-16T07:00:00.00000002*, *metricName*: *d2c.telemetry.ingress.success*, *timeGrain*: *PTIN*)
1000		("count": 1100, "total": 1100, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0033C1B-41AF-4F61-85F1-7FDC98709CBD/RESOURCEGROUPS/IOTIHDM-P-WE-RG01/FROVIDERS/HICROSOFT.
and the second second		DEVICES/IOTHUBS/IOTIMEM-P-WE-IOTHOL*, *time*: *2022-05-16T07:01:00.0000000Z*, *metricName*: *d2c.telemetry.ingress.success*, *timeGrain*: *FTIM*)
1.000		<pre>{ "count": 1117, "total": 117, "minimum": 1, "maximum": 1, "average": 1, "resource:d": "/SUBSCRIPTIONS/E0033CID-14Ar-4F61-89F1-7FC98709CBD/RESOURCEGROUPS/IOTINGA-P-WE-RGO1/VEOVIDERS/MICROSOFT. COUNTER/COUNDS/IOTUNALD-WE-TOTALD-100-100-00-01/020-000-00000000000000000</pre>
	1	<pre>detacd/dimode/ivitate**=bildet,imit: 1 *date="" date: " date:</pre>
		DEVICES/IOTHUBS/IOTINEM-P-WE-IOTHO1*, "time": "2022-05-16T07:03:00.0000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "PTIM")
		("count": 1012, "total": 1012, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0033C2B-41AF-4F61-89F1-7FDC90709CBD/RESOURCEGROUPS/IOTINEM-P-WE-RG01/PROVIDERS/HICROSOFT.
		DEVICES/IOTHUBS/IOTIMEM-P-WE-IOTHOL*, *time*: *2022-05-16T07:04:00.0000000Z*, *metricName*: *d2c.telemetry.ingress.success*, *timeGrain*: *PTH*)
	-	<pre>{ "count: 10%, "total": 10%, "minimum": 1, "average": 1, "resourceid": "/SUBSCRIPTIONS/E0033C28-61AY-64(-89Y)-TECS970%ED/RESOURCEGEOUPS/IOTINIA-P-WE-RG01/PROVIDERS/MICROSOFT. DEUTERS//COUNDS/LOWERS/DEUTERS. DAG. 2000.00.00000000000000000000000000000</pre>
		<pre>devices/strike====================================</pre>
	and a second	DEVICES/IOTHU85/IOTINEM-P-WE-IOTHOI*, *time*: *2012-05-16T07:06:00.0000002*, *metricName*: *dio.telemetry.ingress.success*, *timeGrain*: *FIN*)
	and the second second second	("count": 1091, "total": 1091, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0033C2B-41AF-4F61-89F1-7FDC90709CBD/RESOURCEGROUPS/IOTINUM-P-WE-RG01/PROVIDERS/HICROSOFT.
1000	the second second	DEVICES/IOTHUBS/IOTHUBS/IOTHUBS/FITHUE-P-WE-IOTHUS:, "time": "2022-05-16T07:07:00.00000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "FT1M")
	and the second second	<pre>(*count': liol, *cotal': liol, *minimum*: l, *maximum*: l, *average*: l, *average*: liol, *count': Liol, *cotal': liol, *minimum*: l, *maximum*: l, *maximum*: l, *maximum*: liol, *count': Liol, *</pre>
	-	<pre>det control interview = control = contro</pre>
		DEVICES/IOTHORS/IOTHORS/IOTHORS/.*time": "2022-05-16707:09:00.0000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "FTM")
	and the second se	("count": 1058, "total": 1058, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0833C28-41AF-4F61-89F1-7FDC98709CBD/RESOURCEGROUPS/IOTINDM-P-WE-RG01/PROVIDERS/HICROSOFT.
	and the second se	DEVICES/IOTHUBS/IOTHNE-P-WE-IOTHO1", "time": "2022-05-16T07:10:00.0000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "PTIM")
		<pre>("count": 1113, "total"; 113, "minimum": 1, "werage": 1, "resourceId": "/SUBSCRIPTIONS/E083SCIB-41AF-4F61-85F1-?FDC98705CB0RESORGUPS/IOTIHUM-P-WZ-RG01/PROVIDERS/HICROSOFT.</pre>
		UEVICES/UTHINDS/IDTERRE/=#E-TOTHUT, "IR#": 1/022/03-1610/11100.0000000, "RECTICARME": "GLO.564886FT, INFERS.BUCC88F, "INFERS.BUCC88F," INFERS.BUCC88F," INFERS.BUCC88F,
		OUVICES/IOTHORA-PURCTONOIT, "Ime": "2022-05-16T0712:100.00000002", "metricAme": "doc.elemetry.ingres.success. "timeGrain": "PIN"
		(*count*: 1076, *total*: 1076, *minimum*: 1, *maximum*: 1, *average*: 1, *resourceId*: */SUBSCRIPTIONS/E0833C2B-41AF-4F61-89F1-7FDC98709CBD/RESOURCEGROUPS/IOTINUM-P-WE-RG01/PROVIDERS/MICROSOFT.
		DEVICES/IOTHUBS/IOTINER-P-WE-IOTHOF", "time": "2022-05-16T07:13:00.00000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "PTH")
		<pre>("count: 1124, "total": 1124, "minimum": 1, "maximum": 1, "resourceId": "/SUBSCRIPTIONS/E083SC2B-41AF-4F61-89F1-7FDC98709CBD/RESOURCEGROUPS/IOTIHUM-P-WZ-RG01/PROVIDERS/MICROSOFT.</pre>
		UEVICES/LUTWIDS/IUTINE*-FE-IUTWUT, "LIME"1 "2022-05-1610/114100-10000000," metricement" "2020.562emetry.ingtess.success", "Limevrain"1 "FTHP" 1 Rourse: 1100 Francis: 1100 Francis: 1 Tarkingt, 1 Tarkingt, 1 Francisco, 1 February, 1 Fe
	an agent age	1 Control a large volume inter inter in a strange in a strange in the strange inter
and the second sec		{ "count": 1152, "total": 1152, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0833C1B-41AF-4F61-89F1-7FDC98709CBD/RESOURCEGROUPS/IOTINGM-P-WE-RG01/PROVIDERS/MICROSOFT.
		DEVICES/IOTHUBS/IOTHNE-P-WE-IOTHOF, "time": "2022-05-16T07:16:00.00000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "PTH")
		<pre>("count": 1122, "total": 1122, "minimum": 1, "maximum": 1, "average": 1/2US5CEPTIORS/E003SCEB-61AF-4F61-89F1-7TDC50F05CED/FE50 Development/option/schule_formation/schule_formation/schules/schu</pre>
1.1		DEVICES/IOTHORS/I
		1 Control 1, Control 1
- Search		("count": 1097, "total": 1097, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0833C2B-41AF-4F61-89F1-7FDC98709CBD/RESOURCEGROUPS/IOTINUM-P-WE-RG01/PROVIDERS/MICROSOFT.
Config	a ×	DEVICES/IOTHUBS/IOTIHEM-P-ME-IOTHO1", "time": "2022-05-16T07:19:00.00000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "PTH")
設24 回 山 岡 山	E •	("count: 1054, "total": 1054, "minimum": 1, "aximum": 1, "resourceId": "/SUBSCRIPTIONS/E0833C1B-41AF-4F61-89F1-7FDC9870%CBD/RESOURCEGROUPS/IOTINGM-P-WZ-RG01/PROVIDERS/MICROSOFT.
✓ Display		UEVICES/UTWIDS/IUTWID===E-IUTWIT, "IME" "2022-05-1810/120100.00000000," MECTICAMME" "2020.688##;"IMECESS", "IMECESS", IMECESS", IMECESS", "IMECESS", IMECESS", "IMECESS", IMECESS", IMECESS", IMECESS", IMECESS", IMECESS", IMECESS", IMECESS", IMECESS", IMECESS", IMECESS, IMECE
	the second second	DEVICES/(OTHURS/NEL/NUM-)-WEL/OTHOI, "LINE" 202-05-16707:21:00.0000002", "metric/ame" do.telemetry.ingras.success. "Clamber and Provide Provid
		{ "count": 1121, "total": 1121, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0033C28-41AY-4F61-89F1-7FDC90709CBD/RESOURCEGROUPS/IOTINIM-P-WE-RG01/PROVIDERS/MICROSOFT.
		DEVICES/IOTHUBS/IOTHNE-P-ME-IOTHO1", "time": "2022-05-16T07:22:00.00000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "PTIM")
		<pre>("count: 1123, "total": 1123, "minimum": 1, "maximum": 1, "resourceId": "/SUBSCRIPTIONS/E0033C2B-41AF-4F61-89F1-7FDC90709CBD/RESOURCEGROUPS/IOTIHEM-P-WE-RG01/PROVIDERS/HICROSOFT.</pre>
·		UEVICES/IGTNUSS/IGTNUSS/IGTNUSS/IGTNUSS/ITTNES/I 2022-05-16T07123100.000000000, "metrictame": "420.861emetry.ingress.success", "timeGrain": "471N")
	State of the local division of the local div	DEVICES/CONTRAS/IC INDEX-FACTORDI. TIME: ************************************
		E #count*: 1123, #otal*: 1123, *minimum*: 1, *maximum*: 1, *average*: 1, *resourceId*: */SUBSCRIPTIONS/E0833C28-41AF-4F61-8F1-7FDC98704CBD/RESOURCEGROUPS/IOTHEM-P-WE-RG01/PROVIDERS/MICROSOFT.
		DEVICES/IOTHUBS/IG ^{TINEM-P-WE-IOTHOL*, "time": "2022-05-16T07:25:00.00000002", "metricName": "d2c.telemetry.ingress.success", "timeGrain": "PTIN")}
		1 COMMAND 1 1394, "total": 1154, "minimum": 1, "maximum": 1, "average": 1, "resourceld": "/SUBSCEDFINS/E0033C2B-41AF-4F61-89F1-7FDC9870FCB07ESDORESGOORES/IDTIMEN-P-WE-R001/PROVIDERS/HICROSOFT.
-	-	uk zukszturnusztru inker-rekerturnut, cimert 1022-05-1670/126100.00000002, metrickimert 1020.cetemetry.ingress.success, "cimetrinis' "PIN" (Populati 1124, Francisch 1124, Englishert 1, Bartennest 1, Bartennest 1, Bartennest (PFR) Barten Professionen Profess
		<pre>t count i iii , count i iii , maximum i , maximum i , average i , isobiceto i /sobsectificms/bioSsich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ssich=iAr=fei=sfi=/fb/Ss</pre>
	-	("count": 1177, "total": 1177, "minimum": 1, "maximum": 1, "average": 1, "resourceid": "/SUBSCRIPTIONS/E0033C28-41AF-4F61-5971-7FDCATOSCBD/RESOURCEGROUPS/IOTINEM-P-WE-R001/FROVIDERS/HICROSOFT.
V Miscellaneous		DEVICES/IOTHUBS/IOTHUE-F-WE-IOTHU01*, "time": *2022-05-16T07:28:00.00000002*, "metricName": *d2c.telemetry.ingress.success", "timeGrain": *FIN*)
External Tool Before		("count": 1139, "total": 1139, "minimum": 1, "maximum": 1, "average": 1, "resourceId": "/SUBSCRIPTIONS/E0833C2B-41AF-4F61-89F1-7FDC98705CBD/RESOURCEGROUPS/IOTIMEM-P-WZ-RG01/FROVIDERS/MICROSOFT.
External Tool After		<pre>DEVICES/IOTHOBS/IOTHEM-P-WE-IOTHOL*, "time": "2022-05-16T07:29:00.00000002", "metricName": "d2d.telemetry.ingress.success", "timeGrain": "PTHM"}</pre>

Figure 50: Evidence of the IoT Hub telemetry being above 1000

FISHY reaction to the denial-of-service attack

XL-SIEM detects the attempted flood and raises an alarm (Figure 51), RAE increases the risk level (Figure 52), EDC provides information about the IP in question suggesting a proper reaction), Figure 53 Figure 54.

RU SIEM		SIE	N	Weicome admin Lo atos XL-SIEM	igout I		
L-SIEWI		auration Deports					
ACM	Plasitioalius Palem Pelaysis P com	ушавын Р Керонз	Next refi	esh in 281 seconds. Or click he	re to refresh now		0
AE	Pitters and Options						
lear	Ø View Grouped			(1-2)		Apply Ia	abel to selected alarms
	Signature	Events	Risk	Duration	Source	Destination	Status
	Denial of service	101	10	Friday 21-Jul-2023 [1	Delete	0.0.0.0.4NY	0080
	Malicious URL	2	6	0 secs	10.0.00	0.0.0.0 ANY	open
	Delete selected Close selected			(1-2)			Delete ALL alarms
	[Page loaded in 0 seconds]						

Figure 51: XL-SIEM alarm on the DoS

Document name:	D6.4 IT-2 I	ISHY final release				Page:	53 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final











FISHY		🧕 fishy_sva 💈
IRO Dashboard		EDC - Proposed remediations
	•	Filter ip and port on impacted node (recommanded)
Configurations Components	>	This remediation strategy configures one or more of the filtering security controls to prevent the attackers, identified by an IP, from reaching a victim service characterized by its IP and port.
		Filter payload on impacted node Accept Remediation Details Monitors traffic on impacted node
		Accept Remediation Details

Figure 54: EDC recommendation on the IRO dashboard to "filter ip and port on impacted node"

Document name:	D6.4 IT-2 I	FISHY final release	Page:	54 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



3.3.2 Demo script for Sequel B and G

These sequels (representing attack type 4) intend to demonstrate how FISHY reacts and alerts the user on an attempt of brute force attack on both the Sap Web Dispatcher server and the Windows Servers. This attack occurs when an attacker uses brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained [8].

Simulation of the brute-force attack for both cases

The attacker tries bypassing login by using excessively forceful attempts to gain access to a user account. To simulate this, a script was again used, via Postman, that did multiple requests to a known URL always with the wrong password, therefore getting a 401-error response code, meaning the lack of valid authentication credentials for the target resource.

=	Home Workspaces ~ Explore	Q Search	Postman		ය ^න හි Sign In	Create Account	- 6	;
	▲ Scratchpad is being deprecated. Re	ead more about this in o	our blog 🤊 Create a free ac	ount to experience all of Postman's cap	pabilities.			
3	POST Synchronous export c • POST https://idcs-0b6c2fe: • POST Synchronous export c • OET B	Brut force	+ •••			No Environment		~ 6
Po IO	Fishy / Brut force D					🖺 Save 🗸	/	6
2	GET ~ https:/ sonaearauco.com- /somewebservice.ht	tml					Send ~	Ę
5	Params Authorization Headers (9) Body Pre-request Script Tests Settin	ngs					Cookies	<
)	Type Basic Auth Username The authorization header will be automatically generated when you send the request. Learn more about authorization > Password		someuser somepassword	۵				G
	Body Cookies (1) Headers (10) Test Results			401 Unauthorize	1 Unauthorized Time: 534	ms Size: 582 B Sa	we Response	
	1 @frail version="1.0" encoding="UTF-8"} 2 cerror> 3 ccode>401/(code> 4 cersos=201/(code> 4 cersos=201/(code> 5 clogID>C000A0066932F050000040000025F/logID> 5 clogID>C000A0066932F050000040000025F/logID> 5 clogror>			Similar to 403 Forbidde when authentication is not yet been provided, include a WWW-Auther containing a challenge requested resource.	n, but specifically for use possible but has failed or The response must sticate header field applicable to the			I

Figure 55: Brute force login attempt simulation via Postman using a wrong password multiple times

Document name:	D6.4 IT-2 I	ISHY final release	Page:	55 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



FISHY reaction to the brute force attack

XL-SIEM detects the five multiple failed attempts and raises an alarm (Figure 56 and Figure 57), RAE increases the risk level (Figure 58), EDC provides information about the IP in question (internal or external) suggesting a reaction (Figure 59).

Tishy dashboard	× +						v - 1
. → C @	O A ↔ https://10.4.34.136:31001/main	html?session=eyJhbGciOiJS	Uzl1NilsInR5cClgOiAiSldU	liwia2lkliA6lC/pc015Y0hlWGVpa2l2	skiPTIVCb0s4RjExRU9pT1ZWUkQz5GlpUUI	YcWZVIn0.ey/leHAiOjE2ODk5MzU/	s in d
11	Di Tools - 🖞 Clear						S fishy_wa
FISHS							
	& XL-SIEM						
IRO			Welcome admin + Lo atos XL-SIEN	igout I			
XL-SIEM							
SACM	Dashboards	tion Reports					
RAE	 Fiters and Options 			Next refresh in 287 seconds. Or click h	ere to refresh now		MIC
Clear	Ø View Grouped			(1-2)			Apply label to selected alarms
	Signature	Events	Risk	Duration	Source	Destination	Status
				Friday 21-Jul-2023	[Delete]		
	Brute force	4		0 ма		0.0.0.0.ANY	open
	Brute force	4		0 secs		0.0.0.0 ANY	open
	Delete selected 🔒 Close selected			(1-2)			Delete ALL alarms
	[Page loaded in 0 seconds]						

Figure 56: XL-SIEM alarm on the brute force attack attempt





-		Average value return		
		Average value Low		
	Risk Model:	WRP101: Malware Attack	VERY LOW	
	Risk WRP101-R1:	Malware attack with loss of Availability	VERY LOW	
	Risk WRP101-R2:	Malware attack with loss of Confidentiality	VERY LOW	
	Risk WRP101-R3:	Malware attack with loss of Integrity	VERY LOW	
	Risk Model:	WRP102: Denial of service Attack	LOW	
	Risk WRP102-R1:	Denial of service attack with loss of Availability	LOW	
	Risk WRP102-R2:	Denial of service attack with loss of Confidentiality	LOW	
	Risk WRP102-R3	Denial of service attack with loss of Integrity	LOW	



Document name:	D6.4 IT-2 I	ISHY final release	Page:	56 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



FISHY		Se fishy_wa
IRO Dashboard INTERFACE		EDC - Proposed remediations
	3	Block malicious user (recommended) Accept Remediation Details This remediation strategy, starting from the information provided by the Threat Reports that characterize the Malicious User, configures all the proper security controls to prevent the Malicious User to the victim will be updated adding rules to deny the traffic. If the user is characterized by his IP address address, the filtering devices in the path from the Malicious User to the victim will be updated adding rules to deny the traffic. If the Malicious User is identified by its application-level data, like a username or a WalletD, the security controls able to prevent the user from performing operations are configured. Moreover, this strategy also filters MAC addresses whenever they are available. Filter ip and port on impacted node Accept Remediation Details Put impacted nodes into reconfiguration net Accept Remediation Details

Figure 59: EDC recommendation on the IRO dashboard to block malicious user IP

3.3.3 Demo script for Sequel C

This sequel (representing attack type 5) intends to demonstrate how FISHY reacts and alerts the user on an attempt to call a **malicious URL**. This attack occurs when the attacker makes an http request that is not one of the regular requests for the sap web dispatcher or when there is an attempt of access to an administration URL that does not come from an internal network – meaning, that it is an unknown IP address.

Simulation of the Malicious URL Attack

The attacker tries to gain access to the sap web dispatcher to inject malicious code. To simulate this the attacker makes a request with an URL path different from the "white-listed" ones.

Document name:	D6.4 IT-2 I	FISHY final release	Page:	57 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Home \	Workspaces v Explore			Q Search Postman		ල් 🕸 Sign In	Create Account	-	٥
		Scratchpad is being of	feprecated. Read more at	cout this in our blog > Create a free account	to experience all of Postman's capa	bilities.			
OST Synchro	onous export (• POST https://idcs-0b6c2fe;	POST Synchronous expo	ort c 😐 🛛 🕶 Brut force	POST https://jupiter.sonaea	+ ***		No Environment		~
https://	sonaearauco.com /thisurlisane	cploit.cgi					🖺 Save 🗸	/ 0	
POST	https:// sonaearauco.com;	thisurlisanexploit.c	gi					Send	~
Params	Authorization Headers (9) Body	Pre-request Script Te	sts Settings					Cookie	es
Туре	No Auth	~							
				This request does not use any au	uthorization. Learn more about authorization.	prization A			
ody Coo	kkies (1) Headers (5) Test Results				🚱 Status: 403	Forbidden Time: 266 ms	Size: 9.58 KB S	Save Response	• ~
ody Coo Pretty	kkies (1) Headers (5) Test Results Raw Preview Visualize HTT	n. v 🖘			😤 Status: 403	Forbidden Time: 266 ms	Size: 9.58 KB S	Save Response	a a
Pretty 1 Kht	kkies (1) Headers (5) Test Results Raw Preview Visualize HTT	nL × ⊒⊃			C Statur: 403	Forbidden Time: 266 ms	Size: 9.58 KB S	Save Response	~ Q "
Pretty 1 Ght 2	kies (1) Headers (5) Test Results Raw Preview Visualize HTT talls	n. ∨ 			🗞 Status: 403	Forbidden Time: 266 ms	Size: 9.58 KB S	Save Response	Q =
Pretty 1 Ont 2 Sche 4	Nies (1) Headers (5) Test Results Raw Preview Visualize HTT talg ead; cttle>Application Server Error//tit	tL ∨ =====			🗞 Status: 403	Forbidden Time: 266 ms	Size: 9.58 KB S	Save Response	Q =
Pretty 1 cht 2 3 che 4 5	Akies (1) Headers (5) Test Results Raw Preview Visualize HT tally call citle>Application Server Error/tit citle>Application Server Error/tit citle>Application Server Error/tit	tL ∨ ==> 140			🚷 Status: 403	Forbidden Time: 266 ms	Size: 9.58 KB S	Save Response	Q
Pretty 1 Coo 2 3 che 4 5 6	Hies (1) Headers (5) Test Results Raw Preview Visualize HTT talj (tille)Application Server Error/Tit (style) body (n. v ⇒ ⇒			🖏 Status: 403	Forbidden Time: 266 ms	Size: 9.58 KB S	Save Response	Q
Pretty 1 Coo 3 che 5 6 7	xkiss (1) Headers (5) Test Results Raw Preview Visualize אד العلي ختاب Application Server Error//tit <style></style>								



Document name:	D6.4 IT-2 I	FISHY final release				Page:	58 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



FISHY reacts to the malicious URL attack

XL-SIEM detects the invalid http request and raises an alarm (Figure 61 and Figure 62), RAE increases the risk level (Figure 63), EDC provides information about the IP in question suggesting a reaction (Figure 64).

Câ	O 🔒 ⊶ https://10.4.34.136/31001/main.html?tession=ey/hb	GoOiJSUzi1NilsInR5cCigO	iAiSidUlima2lkliA6K	Upd01SY0hIWGVpa2l2dlcePTIVC	b0s4RjExRU9pT1ZWUkQzSGlpUUIYcWZVIr	0.ey/leHAiOjE2O 130% 🏠	s in ed
	🗮 🖉 Tools 🗸 🖞 Clear						of fishy_wa
FISHY	& XL-SIEM						
20				Welcome admin > Lo atos XL-SIEN	ogout		
L-SIEM		CSIE	VI				
ACM	Dashboards Disk Dashboards Co	nfiguration F Reports	Next refr	esh in 285 seconds. Or click he	re to refresh now		0
AE	Filters and Options						hi. I 🖒
lear	Ø View Grouped			(1-2)		► Apply	label to selected alarms
	Signature	Events	Risk	Duration	Source	Destination	Status
	Malicious URL	2	6	Friday 21-Jul-2023 0 secs	Delete	0.0.0.0 ANY	open
	Denial of service	101	10	20 secs		0.0.0.0 ANY	open
	Delete selected 🔒 Close selecte	рd		(1-2)			Delete ALL alarms
	[Page loaded in 0 seconds]						

Figure 61: XL-SIEM alarm on the invalid URL request

- C @	O & ~ https://10.4.	34.136:31001/main.h	tml?session = eyInbGciOu5Uzi1NiIsInR5c	CigʻOlASidUliwa2ikliA6IC	pd015Y0hIWGVpa2l2dkiPTIVCb0	:4RjExRU9pT1ZWUkQzSGlp	UUN/cWZVIn0.ey/leHAiOjE2C	130% 🛱	CD /il ©
1	= .	ゆ Tools 〜 (j Clear					ć	2, fishy_wa ∨
FISHS	& XL-SI	IEM							
				M	Welcome admin > Logo atos XL-SIEM	ut			^
SACM	► D	ashboards > SIEN	Analysis Configuration Rep	orts				57	
RAE	E M	vent detail	mestive 100101)			1 0	\rightarrow	Ä	
		Event	Data Source Na	me	Produc	t Type	Data	Source ID	^
Clear			HTTP Requests 1	ND	Anomaly D	Detection	1	00101	
	1		Source Address	Source Port	Destination A	Address	Destination Port 0	TCP	
	9:0 里 P	eg	Unique Eve	nt ID#	Asset S + D	Priority	Reliability	Risk	
			27b711ee-a6f2-0242-ac1	1-0002e4040d54	5->5	5	0	8	
		SIEM	Method: POST	Net: 87 196	Request: HTTP/1.1	Response code: 403	Size: 9666	Machine:	2
	M So.		userdata7	userdata9					
			Message: /thisurlisanexploit.cgi	User: -					
		Context Ex	ent Context information not available						
			 Incident Response: Acces 	ss / Acl Permit [Taxo	nomy]				
	-								

Figure 62: XL-SIEM displaying details on the events that originated the malicious URL detection.

Document name:	D6.4 IT-2 FISHY final release Page: 59 of 120					59 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Fishy deshboard × +				~	-	σ
← → C @ O & ~ https://10	4.34.136:31001/main.html?session=eyJhbGciOiJSU	d1NilsInR5eClgOlAiSldUliwia2lkilA6lCJpc01SY0hlWGVpa2l2dkxPTIVCb0s4RjExRU9pT12WUkQzSC	SIpUUTYcWZVIn0.ey.lieHAiOjE2OI 130% 🏠		In CD	Ú
jộ: Fee	dback to OTX		Open Ticket	Close A	llarm	
						~
& RAE						
		Overall cyber-risk status:				^
		Average value VERY HIGH				
	Risk Model:	WRP101: Malware Attack	VERY HIGH			
	Risk WRP101-R1:	Malware attack with loss of Availability	MEDIUM			
	Risk WRP101-R2:	Malware attack with loss of Confidentiality	VERY HIGH			
	Risk WRP101-R3:	Malware attack with loss of Integrity	MEDIUM			

Figure 63: RAE risk increases due to the invalid URL request

FISHY FISHY	.❷ fishy_wa
IRO Dashboard	EDC - Proposed remediations
	Block malicious user (recommanded) Accept Remediation Details This remediation strategy, starting from the information provided by the Threat Reports that characterize the Malicious User, configures all the proper security controls to prevent the Malicious User from reaching the target of the attack. For instance, if the user is characterized by his IP address address, the filtering devices in the path from the Malicious User to the victim will be updated adding rules to deny the traffic. If the Malicious User is identified by its application-level data, like a username or a WalletD, the security controls able to prevent the user from performing operations are configured. Moreover, this strategy also filters MAC addresses whenever they are available.
	Put impacted nodes into reconfiguration net Accept Remediation Details

Figure 64: EDC recommendation on the IRO dashboard to react to the malicious URL risk

Document name:	D6.4 IT-2 FISHY final release				Page:	60 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



3.3.4 Demo script for Sequel D

This sequel (representing attack type 1) intends to demonstrate how FISHY reacts and alerts the user when there is a connection of an **unauthorized IoT device** to the network. This attack happens when an attacker tries to deploy an IoT device that is not validated and pre-registered in FISHY "white list" of devices for the factory, which might be used to acquire production metrics or alter their readings.

Simulation of a rogue device connection

The attacker tries to connect a new unregistered device. To simulate this, an actual new rogue device was connected to the network.



Figure 65: Cyberagent identifying the connection of an unknown new device with the Mac Address 74:fe:48:56:9d:21

FISHY reacts to the rogue device

XL-SIEM detects the new device Mac address received from the WIFI controller and compares it with the "white-list". Once it detects that the service is unknown, XL-SIEM and raises an alarm (Figure 66, Figure 67), RAE increases the risk level and (Figure 68), EDC provides information about the MAC Adress in question suggesting a reaction to block it (Figure 69).

Document name:	D6.4 IT-2 FISHY final release				Page:	61 of 120	
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



🗅 atos XL-SEM 🛛 🗙 🕒 Risk Report 🛛 🗙 🕂 +					- 0
-> C Q A Not secure https://37.48.101.248:18080/xl-siem/				A ⁴ Q	6 6 6 6
Test event detected for alarm	3	10 secs	bind 🐂	x M	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 Disects	ANY	NY	open
Unknown MAC address connected to server	2	10 0 secs	ANY	NY	open
Unknown MAC address connected to server	2	to O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	to O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	rr	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Test event detected for alarm	3	10 secs	bind 🐜	21 M	open
Unknown MAC address connected to server	2	10 0 secs	ANY	NY	open
Unknown MAC address connected to server	2	10 0 secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	t0 O secs	1997	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	488	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	to O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 0 secs	ANY	NY	open
Unknown MAC address connected to server	2	10 0 secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 O secs	ANY	NY	open
Unknown MAC address connected to server	2	10 Disecs	ANY	NY	open
Test event detected for alarm	3	10 secs	sind 🐜	20 M	open

Figure 66: XL-SIEM alarm on the unknown device from the WIFI Controller IP, the source of the signal

	Date		Event date		Sensor	Interface	
	2023-02-02 12:32:00 0	GMT+2:00	2023-02-02 11:32:00 GMT+	+1:00	SONAE [10.0.0.3]	eth0	
	Triggered Signat	ure	Event Type ID	Category	S	ub-Category	
lormalized	Signame Unknow	vn	4				
Event	Data Source	e Name	Product Typ	e	Data Sou	Irce ID	
	Client_Auth	enticated	Alarm		900	2	
	Source Address Source Port		Destination Addres	S	Destination Port	Protocol	
	172 1944 195	0	0.0.0.0		0 T		
	Unic	ue Event ID#	Asset S → I	D Priority	Reliability	Risk	
SIEM	35ed 11ee-b647-	0242-ac11-0003630bb00a	5->5			Us and the 7	
		Ilsernaria	Userdata5		Iserdatao		
	SSID: SA_WODILE WAC	Address. 7	Dase Radio MAC.	Usern	ame. unknown	p Address.	
Contoxt	Event received from Security Agent wi	h aliant id: amatu					
Context	Event received from Security Agent wi	in client_id. empty					
KDB I	No Documents Found						
1100	to boournerits round						

Figure 67: XL-SIEM displaying details on the device detected including the MAC Address

Document name:	D6.4 IT-2 I	FISHY final release				Page:	62 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



		t Laureb Dick	Accessment
			- Section of the sect
Risk Repor	n selected Data Processing Activity: data_share		
Qualitati	Quantitative Mitigations Risk History		
	,		
C.hu d	Table Conference		
Cyber-m	ans quanane		
	Overall cyber-	risk status:	
	Average value	VERY HIGH	
Risk Mo	WRP1: Denial of Service Attack	LOW	
Risk WRF	1: Hacker causes Service/s not available with risk of lo	ss of Availability of service LOW	
Risk Mo	WRP3: Bypass Login	LOW	
Risk WRP	1: Hacker reads application data with risk of loss of Co	Infidentiality of data	
Sisk Mo	WRP6: Session Fixation	VERY HIG	1
Risk WRP	1: Session hijacked with risk of loss of Confidentiality	VERY HIG	

Figure 68: RAE risk increase due to the unauthorized connection

FISHY FISHY	, P fr	shy_wa 🙎
IRO Dashboard	EDC - Proposed remediations	
& Configurations	Biock MAC address (recommended) Accept Remediation Details	
y configurations	This remediation strategy configures one or more of the filtering security controls to prevent the attackers identified by a MAC address, from communicating on the network.	
	Filter payload on impacted node Accept Remediation Details	
	Monitor traffic on impacted node Accept Remediation Details	

Figure 69: EDC recommendation on the IRO dashboard to react to the unknown device/asset by suggesting to block the MAC Address

3.3.5 Demo script for Sequel F

This sequel (type 3) intends to demonstrate how FISHY reacts and alerts the user on a **session hijacking** attempt. This attack occurs when the attacker takes over of an active session between a user and a server. The attacker gains control by exploiting vulnerabilities in the session management process, intercepting session tokens, or other means to impersonate a legitimate user.

Simulation of the session hijacking

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release				Page:	63 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



To simulate this event an attacker uses a valid session ID and password (i.e. obtained via network sniffing or malware infected devices) to log in another windows server immediately after the first genuine user logs in.

n na emoted 20 - cont Cana a mi -	- 0
Connect • + RDP • - File View Tools Help	
Connections 3 X D movement	4
(Ret)	Windows Security X Enter your credentials
	These oredentials will be used to connect to
-	Remember me More choices
listenti Conte 2011 - da 10 - da 10 - 0	OK Cancel
* Dayley	

Figure 70: Logging in to the SRVPT5004 server with a valid user ID

milemotelili - ceell, ons.mi -	- 0 X
Connect • +> RDP • 🚱 • File View Tools Help	
Connections 3 X Crow	x 49
	Windows Security X Enter upon readantials
E constantes	Enter your credentials
	These credentials will be used to connect to
and the second sec	
And a second sec	······
	Remember me
	Hereiter .
terra.	More choices
is Search	UK Cancer
1211 3 A 13 A E O	
✓ Display	
the second distance of	
and the second sec	
the second se	
and the second s	
100 mm	
the second se	
27 B	
All resulting the second	
the second se	
and the second s	
Notifications	

Figure 71: Logging in to the SRVPT5110 server with the same user ID from Figure 64 simultaneously

FISHY reacts to the attack

Document name:	D6.4 IT-2 I	ISHY final release				Page:	64 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



XL-SIEM detects the multiple login and identifies it as a possible session hijacking. Once it is detected the XL-SIEM raises the alarm (Figure 72), RAE increases the risk level (Figure 73Figure 116), EDC provides information about the user in question suggesting a reaction (Figure 74).

atos XL-S EM X D Risk Report X +							-
C A Not secure https://37.48.101.248:18080/xd-siem/					A	· @ @ D	•
	ronae) Logout L-SIEM						
Dashboards							
ers and Options	Next retresh in 296 seconds. Or cli	ck here to refresh now					M.C
View Grouped	(1-4)					Apply label to sele	icted alarms
Signature	Events	Risk 0	Duration	Source	Destination	Stat	us
	Wednesday 11-Ma	y-2022 [Delete]					
Log in with the same user in differents Servers	3	10	12 mins	0.0.0.0.ANY	0.0.0 0.ANY	ope	
Log in with the same user in differents Servers	3	10	9 mins	0.0 0.0 ANY	0.0.0.0 ANY	ope	m
Brute Force Windows	6	10	35 secs	0.000 ANY	0.0.0.0.ANY	ope	
Brute Force Windows	6	10	4 mins	0.0.0.0.ANY	0.0.0.0.ANY	ope	
Delete selected	(1-4)					Deleti	ALL alarms
Page loaded in 0 seconds 1							

Figure 72: XL-SIEM alarm on attempt to login in different servers with the same user ID

	Launch Risk Assessment		
Risk Reports in selec	ted Data Processing Activity: data_share		
Qualitative Qua	inflative Milligations Risk History		
Cyber-risk Status G	pualitative		
	Average value VERY HIGH		
Risk Model:	WRP1: Denial of Service Attack	HIGH	
Risk WRP1-R1:	Hacker causes Service/s not available with risk of loss of Availability of service	HIGH	
Risk Model:	WRP3: Bypass Login	MEDIUM	
Risk WRP3-R1:	Hacker reads application data with risk of loss of Confidentiality of data	MEDIUM	
Risk Model:	WRP6: Session Fixation	VERY HIGH	
Risk WRP6-R1:	Session hijacked with risk of loss of Confidentiality	VERY HIGH	

Figure 73: RAE displaying a risk increase due to the possible session hijacking

Document name:	D6.4 IT-2 I	5.4 IT-2 FISHY final release					65 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



FISHY FISHY		5 fishy_wa							
n IRO Dashboard		EDC - Proposed remediations							
INTERFACE									
🕸 Alerts	>								
la Conformation		Block malicious user (recommanded) Accept Remediation Details							
Configurations	ĺ.	This remediation strategy, starting from the information provided by the Threat Reports that characterize the Malicious User, configures all the proper security controls to							
© Components	>	prevent the Malicious User from reaching the target of the attack. For instance, if the user is characterized by his IP address address, the filtering devices in the path from the Malicious User to the victim will be updated adding rules to deny the traffic. If the Malicious User is identified by its application-level data, like a username or a WalletID,							
		the security controls able to prevent the user from performing operations are configured. Moreover, this strategy also filters MAC addresses whenever they are available.							
		Filter ip and port on impacted node Accept Remediation Details							
		Put impacted nodes into reconfiguration net Accept Remediation Details							

Figure 74: EDC recommendation on the IRO dashboard to block the user ID identified in the attempt of session hijacking

3.3.6 Demo script for Sequel H

This sequel (representing attack type 6) intends to demonstrate how FISHY reacts and alerts the user if the **network traffic of the IoT** goes bellow or above pre-defined thresholds, for multiple metrics, that match usual behavioral patterns, potentially indicating an attempt to tamper IoT readings. Much in the image of denial-of-service telemetry surpasses a certain value this sequel displays how SACM was introduced to the use case to further explore on the possibilities of the traffic control.

Simulation of traffic adulteration

To simulate a network traffic anomaly in this case we used a ICMP flood – ping flood. in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings [14].

PIN	IG 192	.168.2	2.33	(192	.168.2	2.33):	56 data	a bytes			
64	bytes	from	192.	168.	2.33:	seq=0	ttl=64	time=0.9	032	ms	
64	bytes	from	192.	168.	2.33:	seq=1	ttl=64	time=0.4	150	ms	
64	bytes	from	192.	168.	2.33:	seq=2	ttl=64	time=0.1	59	ms	
64	bytes	from	192.	168.	2.33:	seq=3	ttl=64	time=0.1	57	ms	
64	bytes	from	192.	168.	2.33:	seq=4	ttl=64	time=0.1	60	ms	
64	bytes	from	192.	168.	2.33:	seq=5	ttl=64	time=0.1	66	ms	
64	bytes	from	192.	168.	2.33:	seq=6	ttl=64	time=0.1	71	ms	
64	bytes	from	192.	168.	2.33:	seq=7	ttl=64	time=0.1	64	ms	
64	bytes	from	192.	168.	2.33:	seq=8	ttl=64	time=0.1	88	ms	
64	bytes	from	192.	168.	2.33:	seq=9	ttl=64	time=0.1	52	ms	
64	bytes	from	192.	168.	2.33:	seq=16) ttl=64	1 time=0.	164	ms	
64	bytes	from	192.	168.	2.33:	seq=11	ttl=64	1 time=0.	232	2 ms	
^ C	-										
	192.1	168.2	.33 p	ing	stati	stics -					
12	packet	ts tra	ansmi	tted	, 12	packets	receiv	/ed, 0% p	back	et loss	

Figure 75: Simulating an ICMP flood

FISHY reacts to the attack

Document name:	D6.4 IT-2 I	ISHY final release				Page:	66 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



For the SACM to be able to identify these threshold breaches there is a precondition which is the need to first configure the devices to be monitored in the tool. Once that is done the rule can be applied to the devices configurated, which will allow the tool to generate a certification of the system and inform the end user, in real time, for any violations or satisfactions regarding the IoT network traffic thresholds pre-defined.

FISHU	/ WPB SONAE ~ / Secu	rity Assurance / Create Hardware asset: Set trainmeters				9 0 4 0
🕐 Dashboard	Set hardware asset	parameters				
[] Admin 🤆						
Fish Management	Name*	IDT Device 1		Vendor*	Cisco	
🖞 Complence	Verson*	3		Category*	network.	~
🗄 Security Assurance 🔹	Status"	tnai				
🐼 Assets	Value	0	12	Currency	EUR	~
Assessments	Description	IOT Device of WPII use case to be manifored				
C Assessment Profiles						
Ø Assessment Criteria						
(b) Metrics / KPIs	Components					
Open Threat Intelligence	Companent Type*	Natwork				* +
B training & Avarances	MAC	00x0x9+8564/5		Connection Type*	Integrated	80
X AutoML (IPs41	192.168.178.10		Gateway*	192.168.178.1	
	IPv6					
	DHCP Server			DNS Server		
	Subnet Mask			ODR		10
<						Canal Provides Next

Figure 76: SACM configuration of a new asset/device to be monitored.

Fishe	/ WTB SONAE ~ / Security As	ursnoe / Edi Assessment Citierion 3			9 9 8 Ø
() Deshboard	Assessment Criterion Pa	rameters			
Atimin +					
Risk Management	Name*	101 Telemetry threshold	Assessment Model Type*	Monitoring Assessment	
🗅 Compliance	Tags	·	Language"	DRL	Ŷ
A Security Assurance -	Specification*	rule %ule%CRITIRIEN.ID Satisfaction*			1
G Annota		<pre>winter Happens (, of , o, 'cal' == etype, 'traffic == eagg(0), 'gg_instance' : eagg(1)threshod : eagg(2)], t1 : t, gg essure) enderstand the enderstand the enderst</pre>			
() Assessments		f2: Fuent (nome == Signate Rect #SCR/TERION_JD*) not instance == 41, f== 72, i == 112			
😣 Assessment Profiles		then			
Assessment Criteria		Prodicate predicate = new Prodicate() prodicate <u>antidiacent</u> #1;			
H Metros / KPIs	Assign Assessment Crite	rion			
Cyber Threat Intelligence					
₿ Intering to Avariate	Cirganisations*	FISHY V			
>C AutoML +					Gincel Update

Figure 77: SACM definition of rule specifications including every threshold value

Document name:	D6.4 IT-2 I	6.4 IT-2 FISHY final release					67 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



PISHU	WSP / RSWY - / Security Assumed / Assessm	ient Repults 97						a a 6	
(*) Dethboard	Basic Info - Assessment Group ID: 9	97							
G Admin (Organization	WEF			Creator	Agrie			
Ø Risk Management	Project	Paty			Let updated:	2025-08-2 12:55:04			
Compliance									
 Security Assume 	Teo /Service:	Monitoring Assessment			Status	Initialised	H Calsod		
G Accets	Propertien	Availability, Integrity, Confidentiality, Privacy			Accessment Profile	XXT Telensetry Threetro d			
C Assessments	Auda	View crosen Assets			Paramac	None			
C. Internet Conta	Assessment Results								
al version	Original Assets	1			Exploration	TC rule that checks the traffic of an XCP device. If traffic is over 15 then reports violation.			
Cyber Threat Intelligence	Discovered Assets	0							
3. Training & Awareness									
X AutoMa		Results Per Sev	stly			Me	nitoring Assets		
		0							
) follow: }44665			
	15 Clear Search keyword							8 column selected	
	Assessment ID 11 T	Assessment type 11 Y	Asset ID 11 T	Property 11 Y	Normalised Recificod 11 V	Initial detection 11 V	Last checked 11 V	Valid uncit 11 7	
	✓ 201	Maniforing assessment	15	integrity		2023-07-25 104649	2025-27-25 11:48:49		
	Processor Character (1) (2) Creation Descention (C) scients means the last Real Vorticity (Prant Basel Basel Context (C) (C) (C) (C) (C) (C) (C) (C) (C) (C)	it of an OT owner. I faulte to own Withow approximation							
,	> 278	Monitoring assessment	13	integrity		2023-06-23 1164905	2023-06-23 11:09:05		

Figure 78: SACM monitoring results regarding the satisfaction of applied rules

3.4 FISHY-enabled security enhancement in WBPTV supply chain

The wood-based panels trusted value-chain use case evolved consistently along the project to match FISHY developments and potential at the same time guaranteeing improvement of security and reliability their systems. Evolution also meant transformation and thus the involvement of new subsets such as the monitoring of electronic data interchange between company, clients and logistic partners, which made the use case more robust and complete regarding the scope and impact in the supply chain. New challenges demanded the integration of new modules, such as the EDC, so that FISHY could provide solutions - increasing on the already valuable monitorization and alarmistic – and SACM to improve network traffic control. The final list of integrations achieved for the pilots are detailed in the following table:

Table 11: FISHY Components integrated in the WBP UC

FISHY Component	Components	Used in F2F	NOTES					
SPI	Identity Manager	YES	WBP user is authenticated /authorized In FISHY platform					
	Data Management	YES	Transparent to the use case					
TIM	PMEM	NO	Incidents/attack detection on the IoT infrastructure and the SAP web dispatcher (via logging interpretation)					
	XL-SIEM	YES	Incidents/attack detection on the IoT infrastructure and the SAP web dispatcher (via logging interpretation)					
	RAE	YES	Risk analysis based on the detected incidents by SIEM in terms of loss of availability, integrity confidentiality					

Document name:	D6.4 IT-2 FISHY final release					Page:	68 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	VAT	NO	
	WAZUH	NO	
	Trust Monitor	NO	
	Zeek	YES	lot network traffic monitorization tool
	Smart Contracts	YES	Policies suggested to mitigate threats and attacks
SACM	Evidence Collection Engine	YES	Monitorization for any violations or satisfactions regarding the IoT network traffic thresholds
	Auditing Mechanism	YES	
IRO	Intent Manager	YES	Components, events and alarms visualization
	Knowledge Base	YES	
	Policy Configurator	YES	
	Dashboard	YES	
	Learning & Reasoning	YES	
EDC	Controller	YES	Policies suggested to mitigate threats and attacks
	Register & Planner	YES	
	Enforcer	YES	
SIA	IoT Gateway	YES	
FISHY appliance	LOMOS, PMEM	YES	

Returning to the attacks of interest for the use case presented in chapter 3.2, it is also relevant to highlight and detail the final set of rules defined for the pilot activities, which can be checked in following Table 12.

Document name:	D6.4 IT-2 FISHY final release					Page:	69 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Table 12: Rules defined for the detection of the attacks

Туре	RULE							
1	If an event of a connection and authentication occurs in the network (SSID) and is identified by the WLAN Controller (that monitors in real time the network, sending all events to FISHY), TIM compares with the list of validated IoT devices on the company, already pre-registered on FISHY, and checks if the "Client Mac Address" of the device is authorized to connect. If the address is unknown then:							
	• TIM tools (XL-SIEM and RAE) detect the anomaly and raise level of cyber-risk;							
	 FISHY notifies/alerts the operator on the potential rogue device; EDC suggests blocking the Mac Address as a mitigation action; 							
	 The operator must alert the cyber security administrator; 							
	 The administrator validates if it is an authorized device; If authorized, the new device is registered in the platform "white-list" and the incident is deleted; 							
	 If not authorized, Administrator asks to identify existing connections from/to this device and identifies potential impacts and countermeasures such as the blocking of the MAC address suggested by EDC 							
2	If a) the SAP web dispatcher server is flooded with 100 requests or more in less than 1 second or b) if Azure IoT Hub telemetry count is over the licensed quota of 2000, then:							
	• TIM tools (XL-SIEM and RAE) detect the anomaly as a denial-of-service attack							
	 and raise the level of cyber-risk; EISHY patifies (alerts the operator on the attempted DoS) 							
	 EDC suggests filtering IP and port on impacted node as a mitigation action; 							
	 Information is passed by the operator to the cyber security administrator; 							
3	If there is a login with same session ID in different windows servers (login with the same users in different IPs in less than 60 seconds) then:							
	 TIM tools (XL-SIEM and RAE) detect the possible session hijacking and raise the level of cyber-risk; 							
	 FISHY notifies/alerts the operator on the login bypass; EDC suggests blocking the malicious user ID as a mitigation action; 							
	 Information is passed by the operator to the cyber security administrator; 							
4	If (a) there is a tentative of bypass login by brute force with at least five failed login attempts to a) the OPC-UA windows server, or b) the Sap Web Dispatcher then:							
	• TIM tools (XL-SIEM and RAE) detect the brute force attack and raise level of							
	 Cyper-risk; FISHY notifies/alerts the operator on the failed login attempts: 							
	 EDC suggests blocking the malicious user IP as a mitigation action; 							
	 Information is passed by the operator to the cyber security administrator; 							
5	If the HTTP request registered in a log of the SAP Web dispatcher server does not include							
	one of the following strings in the UKL path							
	1/HttpAdapter/							

Document name:	D6.4 IT-2 FISHY final release					Page:	70 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	3/RESTAdapter/
	4/AS2/
	5/AdapterMessageMonitoring/basic
	6/AdapterFramework/ChannelAdminServlet
	Or if it is an access to an administration URL that does not come from an internal network – meaning, that has different lps from the following list:
	A 10.13.xxx.xxx
	B 10.208.xxx.xxx
	C 10.36.xxx.xxx
	D 10.30.xxx.xxx
	E 10.31.xxx.xxx
	Then it is a potential exploit attempt and in such case:
	 TIM tools (XL-SIEM and RAE) detect the malicious URL or unauthorized external IP and raise level of cyber-risk;
	• FISHY notifies/alerts the operator on unauthorized access;
	 EDC suggests blocking the malicious user IP as a mitigation action;
	 Information is passed by the operator to the cyber security administrator;
6	If IoTs network traffic fluctuation (being port-mapped off a switch and continuously read
	by a Zeek instance) crosses minimal and maximum thresholds specified and identified
	in four different metrics:
	 Data logs generated by Zeek are shipped to the SACM;
	 SACM analyzes data in order to match against pre-established network
	 behavioral patterns; SACM identifies the anomaly as a non-compliance of the network traffic
	certification:
	 FISHY notifies/alerts the operator on the non-compliance;
	• Information is passed by the operator to the cyber security administrator:

The data flows leading to the detection of the attacks are also represented in Figure 79, Figure 80, Figure 81.

սիսիս		Save Configuration (Fing Lagout Behavio
CISCO M	NITOR WLANI CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP ELEDBACK	🚺 Home
Monitor Tr Summary Access Points N Coso CleanAir N Statistics COP K Rogues Clients 1 Steeping Clients 2 Multicast 2 Applications 4 Local Profiling 5 0 1 1 1 1 1 1 1 1 1 1 1 1 1	An Logis Internet of Traps since last result 17838907 Internet of Traps Internet In	Chevr Log

Figure 79: Screenshot of syslog of WLAN Controller sending logs to TIM (XL-SIEM module) – use case scenario 1

Document name:	D6.4 IT-2 FISHY final release					Page:	71 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



General AVC Sta	tistics				
Client Properties			AP Properties		
MAC Address	00:d0:c9:e3:6d:f5		AP Address	00:fc.ba:c8:db:80	
IPv4 Address	172.16.0.13		AP Name	AP36_Buffer	
IPv6 Address			AP Type	802.11bn	
			AP radio slot 1d	0	
			WLAN Profile	Wi-Fi Industrial	
			WLAN SSID	SA_Industrial	
			Status	Associated	
			Association ID	13	
			802.11 Authentication	Open System	
			Reason Code	1	
			Status Code	0	
	and the second se	4	CF Pollable	Not Implemented	
Client Type	Regular		CF Poll Request	Not Employmented	
Chent Tunnel Type	Unavailable		Short Preamble	Implemented	

Figure 80: Registered IoT device information set from WLAN Controller to TIM (XL-SIEM module) – use case scenario 1

🔁 😳 🕂 srvpt521_WebDisp_DEV_QLT.tlp - wddadm@srvpt521.dcenter01.ind.sonae:22 - Bitvise xterm 📃 📃) ×
10.13.150.9 [20/Jul/2023:13:50:13 +0100] "GET /sap/wdisp/admin/public/default.html HTTP/1.1" 401 9578	~
10.13.150.9 [20/Jul/2023:14:00:13 +0100] "GET /sap/wdisp/admin/public/default.html HTTP/1.1" 401 9578	
195.23.102.188 [20/Jul/2023:14:09:49 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
195.23.102.188 [20/Jul/2023:14:10:05 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
195.23.102.188 [20/Jul/2023:14:10:07 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
195.23.102.188 [20/Jul/2023:14:10:09 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
195.23.102.188 [20/Jul/2023:14:10:10 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
195.23.102.188 [20/Jul/2023:14:10:12 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
195.23.102.188 [20/Jul/2023:14:10:13 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
10.13.150.9 [20/Jul/2023:14:10:13 +0100] "GET /sap/wdisp/admin/public/default.html HTTP/1.1" 401 9578	
195.23.102.188 [20/Jul/2023:14:10:15 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
195.23.102.188 [20/Jul/2023:14:10:25 +0100] "GET /maliciousurl.html HTTP/1.1" 403 9666	
139.59.147.204 [20/Jul/2023:14:15:50 +0100] "GET /thisurldoesnotexist.html HTTP/1.1" 403 9666	
64.227.21.251 [20/Jul/2023:14:16:58 +0100] "GET /thisurldoesnotexist.html HTTP/1.1" 403 9666	
10.13.150.9 [20/Jul/2023:14:20:13 +0100] "GET /sap/wdisp/admin/public/default.html HTTP/1.1" 401 9578	
64.227.21.251 [20/Jul/2023:14:21:37 +0100] "GET /thisurldoesnotexist.html HTTP/1.1" 403 9666	
10.13.150.9 [20/Jul/2023:14:30:13 +0100] "GET /sap/wdisp/admin/public/default.html HTTP/1.1" 401 9578	
10.13.150.9 [20/Jul/2023:14:40:13 +0100] "GET /sap/wdisp/admin/public/default.html HTTP/1.1" 401 9578	
10.13.150.9 [20/Jul/2023:14:50:13 +0100] "GET /sap/wdisp/admin/public/default.html HTTP/1.1" 401 9578	
195.23.102.188 - someuser [20/Jul/2023:14:53:52 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:53:55 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:53:56 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:53:57 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:53:59 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:00 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:01 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:02 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:03 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:04 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:05 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 170	
195.23.102.188 - someuser [20/Jul/2023:14:54:06 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:07 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:08 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 171	
195.23.102.188 - someuser [20/Jul/2023:14:54:09 +0100] "GET /RESTAdapter/somewebservice.html HTTP/1.1" 401 170	
More(66%)	~



3.5 Improvements compared to IT-1 and final assessment

Both the use case and its scenarios suffered considerable progress since IT-1 as reported along this section. The improvements we made allowed for the testing and validation of multiple components and its capabilities, matching the WBPTV needs and aspirations with the FISHY project.

The FISHY components that were validated in the WBPTV use case and the relevant experience to report is highlighted in the following list:

Validation of TIM: the integration and piloting of the TIM was done throughout the entire project development. On both scenarios developed by the use case a cyber-agent docker was deployed in the company network to receive logs from the IoT infrastructure and the SAP web dispatcher server. These logs are consumed by the XL-SIEM tool that recognizes and addresses potential security threats. This monitorization allows a second tool, the RAE, to do a comprehensive cyber-risk level assessment to

Document name:	D6.4 IT-2 FISHY final release					Page:	72 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final


the assets being monitored. Also, during IT-2 phase, Zeek was fully integrated to allow a complete monitorization of the IoT network traffic, giving a better understanding of telemetry expected patterns and potential events affecting the expected behaviour. Working as data collector Zeek also allowed to smoothly connect this information with SACM.

Validation of SACM: the use and validation of SACM was achieved only during IT-2 with the integration on the use case via connection to the Zeek data collector. While the Zeek was already able to monitor the IoT traffic network, SACM added the auditing mechanism functionality so that control thresholds could be established as certification rules, therefore creating the opportunity trough SACM dashboard to inform the end user on satisfactions or violations of such a threshold;

Validation of EDC: EDC was completely added and validated during IT-2. Although, as stated from the beginning, contrary to other use cases, the EDC was not integrated to automatically enforce policies into WBP IT infrastructure due to the high risks that would imply to the production environment, it has the relevant contribution of indicating to the human user – via IRO dashboard – mitigation measures to apply to the threats/attacks revealed by TIM and SACM tools, taking in consideration the specifics of the attack detected;

Validation of IRO/dashboard: The functionality of IRO/dashboard was successfully verified, as it compiled the findings and events identified by all the monitoring tools. This enabled the WBP operator to gain comprehensive insights into the infrastructure's operations, promoting a clear understanding of the system's activities. Specifically, during IT-2, SACM and EDC were added to the use case dashboard, and the TIM tools already present during IT-1 were improved.

3.6 KPIs satisfaction

Since D6.3 the final list of revised metrics we were to focus on the pilot evaluation activities, using Iteration 2 of the FISHY platform, were set. Although there was a small typo in the deliverable where all metrics were attributed to scenario 2, both scenarios were prescribed with specific metrics as seen in the following table:

Metric ID	Metric description	Туре	Target value	Achieved value
SC1_B1	Detect unregistered IoT devices in the network	Business	True	True
SC1_B2	Monitor IoT Hub telemetry sent from Edge	Business	True	True
SC1_T1	Detect unauthorised access – Windows system	Technical	True	True
SC2_B3	Monitor network traffic anomalies	Business	True	True
SC2_B4	EDI types of attack that can be detected and actuated	Technical	3	3
SC2_B5	EDI transactions real time monitoring	Business	True	True

Table 13: Business and Technical metrics defined in D6.3

In addition, both the KPIs defined in the *Description of Action* regarding the objectives of "Design, development and deployment of a functional platform for cyber resilience provisioning for supply chains of complex ICT systems, leveraging trust and security management" and the "deployment, validation and demonstration in heterogeneous, real world pilots" are considered successful achieved and well represented in the demo activities just described in the present document.

Document name:	D6.4 IT-2 I	ISHY final release	Page:	73 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4 FISHY validation in Securing Autonomous Driving Function at the edge (SADE)

4.1 Introduction

In this chapter, we focus on the validation of FISHY IT-2 in the SADE automotive supply chain. The structure of this chapter follows the one presented in section 1.4.

4.2 SADE vertical application and attack modelling

We are now briefly describing the architecture of the deployment of the SADE use case to give a general view of the whole system.

For the validation, we have several domains. Domain 1 and domain 2 are in our premises, where the SADE own modules are deployed. In addition, the L2SM and SIA NED modules are deployed to allow the inter and intra cluster communication in a secure way. An XL-SIEM agent is deployed in Domain 1 too, where logs are recorded. These agents are in charge of filtering all the logs, understand them and raise alarms to the central repository.

In the FRF all the rest of FISHY modules are deployed. Among them, the SACM, in charge of monitoring the SW versions of the connected vehicle; or the IRO, who must react to the different alarms raised by XL-SIEM.



Figure 82: SADE use case deployment.

During the deployment and integration of the use case, we have identified five different types of attacks:

- Type 1: Ghost vehicle: Not real vehicle sending data to manipulate vehicular traffic.
 - Metadata: {VIN(Vehicle Identification Number)}
 - Type 2: Unauthorized driver trying to start the vehicle with the facial recognition service.
 - Metadata: {VIN}

Document name:	D6.4 IT-2 I	FISHY final release	Page:	74 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



- Type 3: Unauthorized driver trying to start the vehicle with the PIN.
 - Metadata: {VIN, attempts left}
- Type 4: Malware, code injection by IoT devices software
 - Metadata: {VIN, Component: {manufacturer, model, version}}
- Type 5: Vehicle started two times or without previous authorization.
 - Metadata: {VIN}

With respect to **<u>attack modelling according to the ENISA model</u>** which has been introduced in chapter 1, for each type of attack we need to identify the following four elements:

- Attack Techniques Used to Compromise the Supply Chain
- Supplier Assets Targeted by the Supply Chain Attack
- Attack Techniques Used to Compromise the Customer
- Customer Assets Targeted by the Supply Chain Attack

These four components per attack are shown in the following Table 14. For example, in the first attack, we assume that someone could simulate a vehicle, activate it and send its hypothetical location. The vehicles use other vehicles' position data as a reinforcement for not collide with them. So, a simulated vehicle could control other ones by sending, for example, that it is in front of them. The vehicles will stop to avoid the collision. In this case, from the supplier point of view, the attacker targets the EDGE, the traffic data and data shared between connected cars. From the customer point of view, in this case, the car owner, the attacker targets the vehicle by trusted relationship techniques. The own vehicle, the traffic safety and the data flowing between vehicles and edge are compromised.

The second use case attaches the types 2 and 3 of attacks presented above. In this use case the car owner would act as a supplier, because is the one who offers to another person the possibility to drive the car, who would act as customer. With this scenario, two attacks could happen. In the first one, the attacker tries to power on the vehicle. If this individual manages to start the vehicle, there will be assets exposed such as the cameras and the data which the vehicle shares.

On the other possible attack, it is necessary to know that if the driver cannot be authorized with the face recognition service the system will ask him to input his personal PIN. In this attack we suppose that the not authorized attacker manages to get the PIN of an allowed driver by social engineering. At the time when he tries to authorize himself and the facial recognition fails, he could compromise some data stored in the central SADE databases introducing a valid PIN. In this case we see the relationship in a different way as the previous one. The supplier will be the dealer, because is the one who manages the credentials of the users and the ownership of the vehicles. And consequently, the supplier will be the users who own the vehicle.

So, as we have said, the data stored in the central SADE databases could be compromised, and this data is in the side of the supplier. In the side of the customer, the vehicle itself could be the compromised asset.

In the third and fourth use cases the type 4 attack is attached in which an attacker would try to inject malware into the IoT devices present in the vehicle. In this scenario, the manufacturer, and the dealer (as manufacturer of some IoT devices present in the vehicle) are the suppliers who give to the car owner, the customer, these devices. The suppliers' assets exposed are the own devices and the customer's asset in risk are the own vehicles and therefore their shared data and the traffic safety.

And finally, in the last scenario we attach the last attack, in which the attacker manages to activate a fake vehicle and with it, he would act as a man-in-the-middle and interact with many dataflows exposing them. In addition, it could interact with the other vehicles, so the traffic safety is at risk too. In this scenario will be two suppliers. The local operator, who offers connectivity through its infrastructure and the dealers, who manages the vehicles and user data. The customers will be the car owners who connects their vehicles sold by the dealer to the local operator infrastructure.

Document name:	D6.4 IT-2 I	ISHY final release	Page:	75 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	SUPPLIER		CUSTOMER			
Attack	Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack		
SADE – UC1 – Type 1	BruteForceGhostCarfortraffictampering(notauthorizedcarstarted)Supplier:LOCALEDGEOPERATOR	EDGE. The traffic data , and data shared between connected cars	Trustedrelationship(betweenthedriversandtheEdgeTrafficmanager)Customer:Allowed drivers	Vehicle, traffic safety Data (public data shared by the car)		
SADE – UC2 POWER ON – Type 1	Unauthorized Access/Code injection/malware Supplier: CAR OWNER	Vehicle cameras (Data)	Facial Recognition Spoofing Attack Customer: ALLOWED DRIVER	Vehicle, Data (public data shared by the car)		
SADE – UC2 – Type 3 (Not critical if no SADE – UC2 POWER ON – Type 1, because only can activate the FR)	Socialengineeringattacks(notauthorizeduserauthorizeduserstolencredentialstryingtoactivatefacialrecognitiontopowerpoweronthecarusingPIN)Supplier:DEALER	User credentials, User data	Trusted relationship (between the car, the Edge and the SADE On premise cloud) Customer: CAR OWNER	Vehicle		

Table 14: ENISA modelling of SADE use case attacks.

Document name:	D6.4 IT-2 I	ISHY final release	Page:	76 of 120			
Reference:	D6.4	D6.4 Dissemination: PU Version: 1.0				Status:	Final



SADE – UC3 SW Patch	Malware/code injection (not	Hardware component's pre-existing software	Trusted relationship	Vehicles, traffic
Certification UC4 SW Patch level correction Type 1	validated software) Suppliers: MANUFACTURER DEALERS (as main Manufacturers of the vehicle)	provided by the manufacturer	(between the drivers and manufacturer) CUSTOMER: Car Owners	safety Data (public data shared by the car)
SADE- UC5- - Type 1	Malware (car started two times) Suppliers: LOCAL OPERATOR DEALER	EDGE. The traffic data, and data shared between connected cars SADE Connected car system Possible traffic tampering attempt	Man-in-the- middle(carduplicatedtoreceive data)CUSTOMER:Allowed drivers	Vehicles safety Data (public data shared by the car)

With respect to the MITRE ATT&CK framework we are describing now how we can apply the asset/impact-centric approach step by step to the SADE pilot.

Step 1: System description

The system deployed in this automotive supply chain has already been presented above and thus here, we identify the main assets and their potential impact on security properties.

Table 15: Asset/Impact Synthesis

ASSET	EXPOSITION	IMPACT	Notes
EDGE nodes	Wireless	High	Type 1 and 5 of the previous list
Vehicles	Limited	High	Types 1 to 5 of the previous list
User credentials	Limited	Medium	Types 2, 3 and 4 from the above list.
HW's component SW	Limited	Medium	Type 4 attack from the above list.
User data	Internet	Low	Type 1 and 4 attack of the previous list

Step 2: Threat modelling

Threat modelling is an activity aiming to understand threats better and identify how the related attacks are deployed, the tools used, and the explored vulnerabilities. This is made easy by the MITRE ATT&CK Navigator.

In our use case, the main method to detect threats is by logs. The flow of all the use cases of the attacks starts by writing logs, so, if we select log as control element, we can see the set of attack that can be detected using logs, showing in blue colour in the figure.

Document name:	D6.4 IT-2 I	FISHY final release	Page:	77 of 120			
Reference:	D6.4	D6.4 Dissemination: PU Version: 1.0				Status:	Final



layer1 ×	+								selection contr	ols layer controls			nique controls	1 69	0
Initial Access	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques		no celor		
Dior-sy Composite Exploit Public-Faring Application Exploit Public-Faring Application Explored Remote Explored Remote Explored Remote Public Remote Services Remote Services Registerior Through Registerior T	Change Operating Mode Command-Line interface Execution through Original Controller Model Scripting Scripting User Execution	Intercoold Credentials Modify Program Modify Program Project File Infection System Filemare Valid Accounts	Exploration for provinge Escalation Hooking	Chunge Genating Munde Genating Indiator Strangel Indiator Removal on Host Maspared Resoluti Spool Reporting Message	Network Commetation Lower and Sector and Sec	Detail: Constraintia generative services remote services constraintia remote services regard Details Remote Services Wald Accounts	Advergary in the Middle Middle Collection Data Brown Data Strong Data Strong Data Strong Data Strong Data Strong Collegation State Collegation State Collegation State State Collegation State State Collegation State State Collegation State State Collegation State State Collegation State State Collegation State State Collegation State State Collegation State State Collegation State State Collegation States State	Commonly Used fort	Activate Firmane Update Mode Alam Suppression Book Company Message Book Sporting Bioks Serial COM Change Credential Davice Booke Credential Davice Booke UC Image Modity Alam Settings Rochit Service Stop System Firmane	Brate Serve UD Loddy Parameter Module Primare Secol Reporting Length of the Secol Unauthorized Command Mesage	Damage to Parejare to Penial of Control Loss of Availability Loss of Control Loss of Pareduchility Loss of Pareton Loss of Safety Loss of Vareton Loss of Vareton Loss of Vareton Control Manipulation of Damage Annotation Control Manipulation of Damage Annotation Control Manipulation of Damage Annotation Control Manipulation of Damage Annotation Control Manipulation of Control Manipulation	Search Settings anne ATT&CKID d d Techniques (46) Setted att Activate Firmware Update Mode Adversary-in-the-Middle	dess xiew select xiew select xiew select xiew select	ata source lect all deselec deselec deselec	

Figure 83: The attacks that can be detected based on logs shown/highlighted in Blue (53 out of 80, i.e. 66%)

From the selected threat we can select one by one the most important or more probable to our system. Once they are selected, the MITRE ATT&CK displays all the procedures that an adversary may follow, the mitigation measures identified and the detection alternatives. We can see some of the main examples in the following Figure 84, Figure 85 and Figure 86.

Marine Paritocon						Metrices * Tectics * Techniques * Data Dourses Mitigations *						
TECHNIQUES												
Enterprise	~	Parts - In	Children > 273 > 200214	Pressare.								
Mobile	*	Mod	ule Firmw	are								
105	^	Advensaries	i may install malicious o	r vultarable firmware o	nto modular hardware devices. Control system devices often contain modular hardware devices. These devices may have their corr set of firmware that is separate from the firmware of the main control system equipment.	IC: 70839						
Initial Access	×.	This taches	que le similar to System	Firmears, but is condu	end on other system components that may not have the same capabilities or level of imagity shadking. Although it results in a device re-image, malicious device fermears may provide pervicent access to remaining	Sub-techniques: No sub-rechniques						
Persistence		Devices.**				Tactics: Persistence, Impair Process Control Biaformer: Build Control (2010) Ender: Laster method former Remember Refer						
Hardcoded Gredentiels		accomplish	additional attacks, such	as the following. ^[1]	eg, which may have its own CPU, how, and operating system. The adversary may attack and usary expect the computer on an Ethernet Cart. Exploration of the Ethernet Card computer may enable the adversary to	Version: 1.1						
Modify Program		· Dalays	ed Attack - The adversar	y may stage an attack	in advance and choose when to learch it, such as at a particularly damaging time.	Created: 21 May 2020						
Project File Infection		 Brickt Rande 	the Ethernet Cerd - Malic Im Attack or Failure - Th	clous firmware may be a adversary may load r	programmed to result in an Ethernet card failure, requiring a factory return. natiolius firmware onto multiple field devices. Execution of an attack and the time it occurs is generated by a pseudo-random number generator.	Later Indentities of Nation and						
System Firmware		 A Field 	d Device Worm - The ad-	rereary may choose to	denofy all field devices of the same model, with the end goal of performing a device-wide compromise.	Version Permaink						
Valid Accounts		a Attack	CPU module.	d beide - Athough it i	a not the most important module in a field device, the Ethernet card is most accessore to the adversary and masware, compromise of the Ethernet card may provide a more direct route to compromising other modules, scon							
Evening Encaration	÷	a distant	lane									
Discovery	×	wiitiga	nions									
Lateral Movement	٣	0	Metgation		uengon							
Control and Control	*	ACCEPT	Access Management		An overces or systems charges, noticing at sommerance functions, endurreque extremication, consister using access management rectivologies to emote autoritation on an management rectivologies to emote autoritation on an management rectivologies of emote autoritation on an imagement rectivologies	mps, especially when the device does not interestly provide strong auteritication and automotion numbrions.						
Inhibit Response Function	v	10347	Audi		Parton integray precise of timesex before uppealing it or a device. Utilize cryptographic hashes to verify the timesex has not been tampared with by comparing it to a trusted hash of the timesex. This occurs be trust	trusted data souther (e.g., vendor and or through a throughty vertication service.						
Impair Process Control	*	MOJEO	Boot Pringhty		Check the integrity of the existing BIDS or on to determine it is is unreable to included on. Use Traded Platform Module technology, "" Move systems root of that to herdware to prevent tengening with the SM Team in	nemory, I'' technologies such as the Boot duard can assist with this, I''						
impact	v	M0945 Code Signing			Devices should verify that firmware has been properly signed by the vendor before allowing installation.							
		MORCE	Communication Authe	REEDY	Protocols used for device management ehouid authenticate all network messages to prevent unauthorized system changes.							
		MOSCE	Encrypt Network Traffi	¢.	The enclyption of himself and date considered to prevert adversion from Sectory og passible vulnerabilities within the formulae.							
		1109.61	Encrypt Senattive Infor	mation	The encopelion of formulae should be considered to prevent adversarias from identifying parable unleaved lines which the formulae.							
		M0937	Filter Network Traffic		Fiber for protocols and psyloads associated with foreware activation or updating activity.							
		MORON	Human User Authentic	Defice:	Devices that allow remote management of firmware should require authentication before allowing any changes. The authentication mechanisms should also support Account Use Pulicies, Password Pulicies, and User A	Account Management.						
		M0307	Network AllowEsta		Use host-based allowilitis to prevent devices from accepting connections from unauthorized systems. For example, allowilitis can be used to ensure devices can only connect with master stations or known management	tilangineering workstadons. III						
		M0930	Network Segmentation	9	Segment operational network and systems to restrict access to critical system functions to predetermined management systems. 🗮							
		MORIS	Software Process and	Device Authentication	Authenticate connections fromothware and devices to prevent unauthorized systems from accessing protected management functions.							
		Detec	tion									
		0	Oata Source	Data Component	Detects							
		050015	Application Log	Application Log Contwrtt	Monter device application logs for firmware shanges, although not all devices will produce such logs.							
		050001	Firmware	Ferrivare Modification	Nonter finnvær for unspected sharpes, Asen managemen systems should be onsubed to understand known god finnvære vesions. Durgs and neget BIOS images on vulnesble systems and compare against know against known pathing bekaris: Uleving ET mobiles an be collected and compared against a known olaw hit of ET executable brukers to direct partially malicious mobiles. The CHFISC framework can be used fi	vn good images ³⁰ Analyze differences to determine if malicious changes have socurred. Log attempts to readivirte to 8008 and compare to analyze to descrime if firminae modifications have bein performed. ²¹ NIR						
		090629	Network Traffic	Network Traffic Content	Monitor (55 messagement protocols / file transfer protocols functions inland to femvare changes.							
		090040	Operational Databases	Device Alem	Monter for femulare changes which may be observable via operational alarma from devices.							

Figure 84: Module firmware threat.

Document name:	D6.4 IT-2 FISHY final release						78 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Hume > 1	chrigues > ICS > Ad	Versary-in-the-Middle						
Adv	ersary-in	-the-Middle						
Adversarion that a	a with privileged net lversary has the abili	vork access may seek to mo ty to block, log, modify, or in	odly network traffic in nul time using adversary-in-the-middle (ATM) attacks. ¹¹ This type of attack allows the adversary to intercept traffic to und/or from a particular device on the network. If a ATM attack is established,	ID: TOESO				
An AiTM a Block Rep	task mey allow an a sting Message, Spor	dversery to perform the folio	taning media Informations, Unsubstand Cammund Message	But etchingues: Te sub-etchingues Testic Colorest Executions Testic Colorest Executions Testic Colorest Executions Controllators: Constantiants Controllators: Constantiants Controllators: Constantiants Constantian				
Proc	dura Evan	anles		Version Permaink				
n	Name D	ipies						
57010	VDMDhar 7	terrigener	a nonferenza the desired intelling to reduce all to En destruct for non 10 to include another latencies noncer 1000 Jan contains water an over 10 sea one internaned by salar and sas has internaned by the net module and	manin-land before being agons the leastmane LTTP agoing 1014				
-				nanganata anton bang ana managanata ara anganata.				
Mitig	ations							
ю	2 Milyahn Develoption							
1009.57	MORE? Audit Unit access to network infrastructure and resources that can be used to seehape traffic or otherwise produce AFMI conditions.							
M0802	100102 Communication Authenticity Communication authenticity will ensure that any messages tampered with through ATM can be determed. but cannot prevent assessing-program on these. In addition, printing communication authenticity around various discovery protocols, such as 2010, can be used to prevent various ATM procedures.							
M09.62	Disable or Remove	Feature or Program	Disable unnecessary legacy network protocols that may be used for ATTM if applicable.					
140931	Network Intrusion	Prevention	Network Intrusion detection and prevention systems that can identify traffic patterns indicative of ArTM activity can be used to mitigate activity at the network level.					
1/0930	Natoork Segments	ition	Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the access of ATM activity.					
M0810	Out-of-Band Comm	nunications Channel	Utilize out-of-band communication to validate the integrity of data from the primary channel.					
M0813	Software Process	and Davios Authentication	To protect against ATM, authentication mechanisms should not send oredentials across the network in plaintent and should also implement mechanisms to prevent replay attacks (such as nonces or timestamps). Challenge	response based authentication techniques that do not directly send oredentials over the network provide better protection from AITM.				
540814	Static Network Co	rfiguration	Statically defined ARP entries can prevent manipulation and aniforg of switched network traffic, as some ArTM techniques depend on sending spooled ARP messages to manipulate retwork host's dynamic ARP tables.					
Deter	tion							
10	Data Source	Data Component	Desics					
D/90015	Application Log	Application Log Content	Montor application logs for changes to settings and other events associated with network protocols and other services commonly abused for AITM.					
050029	Network Traffic	Network Traffic Network Traffic Content Monitor network traffic for anomalies associated with known ATM behavior. For Collection activity where transmitted data is not manipulated, anomalies may be present in network managem		P DHCP).				
		Network Treffic Flow	Monitor for network traffic originating from unknown/unexpected hoats. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be sub-techniques.	helpful in identifying hardware. For added context on adversary procedures and background see Adversary in the Middle and applicable				
050009	Process	Procese Creation	Host-based implementations of this technique may utilize networking-based system calls or network utility commands (e.g., (prables) to locally intercept traffic. Montor for relevant process oriention events.					
D50019	Service	Service Creation	Monitor for newly constructed services/Baemons through Windows event logs for event IDs 4907 and 7045.					
050024	4 Worken Reprov Microsoftware Statistica							

Figure 85: Adversary in the middle threat.

Brut	Brute Force I/O									
Adversarie manipulati values, the associated Adversarie	is may repetitively o e a process function e adversary may be a d with that particular is may use Brute For	r successively change I/O poin . The adversary's goal and the lible to achieve an impact withor point. cce I/O to cause failures within	ID: TOBOS Sub-techniques: No sub-techniques Tadito: Impair Process Control Platforms: Control Sarves, Faiel Controller/RTU/PLC//ED Version: 1:1 Created: 21 May 3020 Last Modified: 29 March 2023 Version Permalink							
Proce	Procedure Examples									
ID	Name Description									
S0604	Industroyer The industroyer EC 104 module has 3 modes available to perform its attack. These modes are range, shift, and sequence. The range mode operates in 2 stages. The first stage of range mode gathers information Object Addresses (IOA) and sends select and execute pacients to switch the state. The second stage of range mode has an infinite loop where it will switch the state of all of the previously discovered IOAs. Shift mode is similar to range mode, but instead of staging within the same range, it will add a shift value to the default range values.									
S1072	S1072 Industryer2 can iterate across a device's IDAs to modify the ON/OFF value of a given ID state. IRI									
Mitig	Mitigations									
ID	Mitigation		Description							
M0937	Filter Network Tra	ffic	Allow/denylists can be used to block access when excessive I/O connections are detected from a system or device during a specified time period.							
M0807	Network Allowlist	8	slize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.							
M0930	Network Segmen	tation	Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more cr	itical control and operational information within the control environment, $^{\left[4\right]}\left[5\right]\left[6\right]\left[7\right]$						
M0813	Software Process	and Device Authentication	Devices should authenticate all messages between master and outstation assets.							
Deteo	ction									
ID	Data Source	Data Component	Detects							
DS0015	Application Log	Application Log Content	Some asset application logs may provide information on U/O points related to write commands. Monitor for write commands for an excessive number of U/O points or manipulating a single value an excessive number of times.							
DS0029	Network Traffic	Network Traffic Content	Monitor network traffic for ICS functions related to write commands for an excessive number of I/O points or manipulating a single value an excess	ive number of times.						
DS0040	Operational Datab	ases Process History/Live Data	Monitor operational process data for write commands for an excessive number of UO points or manipulating a single value an excessive number of evidence that the technique has been used and may complement other detections.	times. This will not directly detect the technique's execution, but instead may provide additional						

Figure 86: Brute force threat

Document name:	D6.4 IT-2 I	ISHY final release	Page:	79 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Step 3: Impact assessment

In this final step, we assess the impact together with the success probability using the information provided by MITRE ATT&CK table. In more detail, for each row in the previous table, based on the information of the MITRE table, we check whether FISHY platform implements a detection technique and whether the mitigation identified (and recommended and/or enforced) in FISHY is aligned with the one suggested by MITRE table. Based on this information, we fill the following table:

ASSET	IMPACT	Success probability	Notes
EDGE nodes	High	Low	Type 1 and 5 of the previous list
Vehicles	High	Low	Types 1 to 5 of the previous list
User credentials	Medium	Low	Types 2, 3 and 4 from the above list.
HW's component SW	Medium	Low	Type 4 attack from the above list.
User data	Low	Low	Type 1 and 4 attack of the previous list

Table 16: Success probability assessment for potential attacks

4.3 Demo script

In this section, we present the script of the FISHY demonstrator for the SADE use case. We will break this down into the above use cases, which attempt to describe how FISHY would react to the different attacks identified above. The different use cases are independent between each other. We can see these use cases in the following Figure 87.



Figure 87: SADE use cases

Document name:	D6.4 IT-2 I	ISHY final release	Page:	80 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4.3.1 Demo script for Sequel A- Car activation

In this scenario we are seeing how FISHY can react to a traffic tampering attack. In addition, and due to the way we are going to show this case, we are also seeing how FISHY has the ability to activate or deactivate vehicles through SPI, IRO and FISHY dashboard.

At first, a dealer activates the vehicle using SADE API dashboard after selling it. That is, this vehicle is now allowed to be connected to the EDGE.

H								
FISHU	⊗ [SADE] Add Vehicle							
& Dealer workspace								
₿ IRO		Register vehicle 🖷						
€ SACM		VIN:						
∥ RAE								
ℬ TIM XL-SIEM		Model:						
		Manufacturer:						
🕆 Clear		Activation Country:						
		span						
		Submit						

Figure 88: Dealer's fishy dashboard workspace. With the add vehicle form (fishy_sb user is a dealer)

Then, let us suppose that a malicious agent tries to connect to the EDGE a not previously activated vehicle. It could be a ghost car, for traffic tampering. Without FISHY, it is not possible to monitor it, so the malicious agent could try many times to even take down the EDGE.

Nevertheless, we have FISHY. And we can see how this framework monitors the whole supply chain. In this case through logs. SADE API records the not activated car attempts to a log which is consumed and filtered by XL-SIEM. Furthermore, XL-SIEM raises an alarm saying that there have been five attempts to access an unauthorized vehicle.

[2023-07-18	12:38:56	+0200]	[44]	[ERROR]	[495]	No	existing	car.	Posible	attack:	22580005-4144-4085-bc3d-6cef407d6706	
Figure 89: Log row in SADE API logs												
		10										

	☰ 必 Tools ∨ 칍 Clear	r					C fishy_sb	~		
FISH9	& TIM XL-SIEM									
Dealer workspace	Today Last 24h Last 2 days Last	Ilmeline analysis Week Last 2 Weeks Last Month	a 🔊 a	ddresses: Destin Source estination	ution Port: TCP UDP	Product Types Categories	Unique IP links [FQDN] Unique Country Events	^		
₿ IRO							Custom Views			
& SACM	Displaying events 1-50 of about thousands matching your selection.									
	Signature	A Date GMT+2:00	Sensor	Source	Destinat	tion A:	⇒ D Risk			
₿ RAE	Not existing car	2023-07-18 14:38:56	CAPGEMINI	0.0.0.0	0.0.0.0) 5	->5 10			
2011 C C C C C C C C C C C C C C C C C C	Not existing car	2023-07-18 14 38:55	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5 18			
STIM XL-SIEM	D Not existing car	2023-07-18 14 38 55	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5			
	Not existing car	2023-07-18 14:38:54	CAPGEMINI	0.0.0	0.0.0.0	5	->5 18			
[SADE] Full Sade	Not existing car	2023-07-18 14:38:54	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5			
Api	Not existing car	2023-07-18 14:38:54	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5 18			
	Not existing car	2023-07-18 14:38:53	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5			
[SADE] Add Vehicle	Not existing car	2023-07-18 14 38 53	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5 18			
	Not existing car	2023-07-18 14:38:52	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5 18			
🕆 Clear	📝 🔲 Not existing car	2023-07-18 14:38:52	CAPGEMINI	0.0.0.0	0.0.0.0	5	->5 18			

Figure 90: Not existing car events in XL-SIEM dashboard.

Document name:	D6.4 IT-2 I	ISHY final release	Page:	81 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	© IIM.	XL-SIEN	Л								
Dealer workspace	8					, v	felcome > Logout				
RO					5IEN		tos XL-SIEM				
SACM	Þ	Dashboards	SIEM Analysis	Reports							
		PI S	ource		19	Destination		R Knowledge	e base		
♭ RAE	0.0.0). 0			0.0.0.0		volume, no	t their type: while a system single packet of data, b	m can be exploited with		
TIM XL-SIEM	📌 Location: Unknown				📌 Location:	Unknown	requires greater numbers to achieve. This presents a problem in determining the validity of a				
	0 01	IX: No			OTX: No		brute-force One system	attempt, as opposed to ju n repeatedly trying to log	ust a broken system. into the same account		
♭ [SADE] Full Sade pi	Ports Unknown			💻 Ports	Unknown	terror terring), over and over again, is visionity dimerent from a single system trying thousands of different accounts and passwords. Not all brute-force attempts will be about account credentials, any attempt to gain access to something through trail-and-care renetition is a hole force attempt for					
§ [SADE] Add Vehicle	► Sour	ce (1)	Destination (1)	• Event Det	ail						
j Clear	#		Alarm		Risk	Date	Source	Destination	Correlation		
	1	Brute force	attack against car		10	2023-07-18 14:38:52	0.0.0.0:ANY	0.0.0.0:ANY	2		
									-		
	2	Not existing	car		10	2023-07-18 14:38:52	0.0.0.0:ANY	0.0.0.0:ANY	1		
	2	Not existing Not existing	car car		10 10	2023-07-18 14:38:52 2023-07-18 14:38:06	0.0.0.0:ANY 0.0.0.0:ANY	0.0.0.0:ANY 0.0.0.0:ANY	1		
	2 3 4	Not existing Not existing Not existing	car car car		10 10 10	2023-07-18 14:38:52 2023-07-18 14:38:06 2023-07-18 14:38:06	0.0.0.0:ANY 0.0.0.0:ANY 0.0.0.0:ANY	0.0.0.0;ANY 0.0.0.0;ANY 0.0.0.0;ANY	1 1		
	2 3 4 5	Not existing Not existing Not existing Not existing	car car car car		10 10 10 10	2023-07-18 14:38:52 2023-07-18 14:38:06 2023-07-18 14:38:06 2023-07-18 14:38:05	0.0.0.0:ANY 0.0.0.0:ANY 0.0.0.0:ANY 0.0.0.0:ANY	0.0.0.0:ANY 0.0.0.0:ANY 0.0.0.0:ANY 0.0.0.0:ANY	1		

Figure 91: Brute force attack alarm.

These alarms are sent to central repository to be captured by IRO and it acts consequently. It will inform the local operator that an attack is being done by sending a POST call to a SADE API endpoint.

Alarm	reported by Fishy IRO from XL-SIEM 🛛 🕙 🗸	€, ∨					
a a t	raducir mensaje a: Español Nunca traduzca de: Inglés						
S	send.secure.mail.fishy@gmail.com©©<	→ … 3/2023 11:25					
*****This mail has been sent from an external source. Do not reply to it, or open any links/attachments unless you are sure of the sender's identity.*****							
	Possible brute force attack.						
	\leftarrow Responder \rightarrow Reenviar						

Figure 92. Mail received by Local Operator.

Document name:	D6.4 IT-2 I	FISHY final release	Page:	82 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4.3.2 Demo script for Sequel B - Power on

In the second scenario we see how FISHY monitors the vehicle power on against two different types of attacks.

Firstly, a phishing attack in which the malicious agent tries to impersonate one of the allowed drivers for the vehicle and secondly a social engineering attack, in which someone has been able to steal a vehicle driver credentials.

Unauthorized access

Assuming a well-known driver is correctly allowed to use a vehicle and that the vehicle has a face recognition (FR) module to power on the vehicle. We can see in the following image how a car owner can allow new drivers through its workspace of the FISHY dashboard.

k	😑 🖉 Tools 🗸 📋 Clear		$\stackrel{\circ}{\frown}$ fishy_sc \checkmark
FISHS	⊗ [SADE] Allow new driver		
بھ IRO		Register driver 🖻	
ℬ SACM		To register a new driver you need a user registered by the dealer.	
₿ RAE		ID:	
多 TIM XL-SIEM			
[SADE] Allow new driver		Allowed VIN:	
		Driver's image:	
🖞 Clear		Examinar No se ha selegún archivo.	
		Submit	

Figure 93: Allow new driver form. Only available for car owner (fishy_sc)

Let us imagine that an attacker manages to sit in the driver's seat and tries to start the vehicle. The FR module must authorize it through the dashboard camera. And the result is an unauthorized driver event. SADE API, as in the previous scenario, records this attempt and XL-SIEM will capture it and generate and event.

[2023-07-18 13:50:16 +0200] [44] [ERROR] [490] Unauthorized driver for car: 22580003-4144-4085-bc3d-6cef407d6706

Figure 94: Unauthorized driver log row.

Document name:	D6.4 IT-2 FISHY final release					Page:	83 of 120
Reference:	D6.4	D6.4 Dissemination: PU Version: 1.0				Status:	Final



	📕 🖉 Tools 🗸 📋 Clear						C fishy_sc
FiSH9	& TIM XL-SIEM						
🖉 Car Owner	Real Time Trend Graph by GMT+2:00 d	lates					_
vorkspace	Search Clear	Back 🔁 Refres	ih 🔥 🛛 Cu	rrent Sear	ch Criteria [Clear	r All Criteria])	Show full criteria
Ø IRO	Search term	IP Signature Pay	M	ETA	PAYLOAD	IP	LAYER 4
		in origination (ray		any	any	any	none
3 SACM	Sensor Data Source xlsiem-server	es Risk	~		Summai	ry Statistics	
	More Filters	Taxonomy and Reputation F	ilters Ev	ents 🛃 💽	Unique Events	Sensors	Unique Data Sources
₿ RAE Ø TIM XL-SIEM	Time frame selection GMT+2:00: 🛅 Today Last 24h Last 2 days Last Week	Timeline analysi	s: 📆 ac	Unique Idresses: Source estination	Source Port: TCP UDP Destination Port: TCP UDP	Taxonomy Product Types Categories	Unique IP links (FQDN) Unique Country Events
3 [SADE] Allow new							► Custom Views
river	Displaying events 1-50 of about thousands matched and the second seco	ching your selection.					14,385 total events in database.
	Signature	▲ Date GMT+2:00 ▼	Sensor	So	urce Des	stination	Asset S → D Risk
· · · · · · · · · · · · · · · · · · ·	🦻 🔲 Unauthorized Driver	2023-07-18 15:50:16	CAPGEMINI	0.0	.0.0 0	0.0.0.0	5->5
ר Clear	D Not existing car	2023-07-18 14:38:56	CAPGEMINI	0.0	.0.0 0	0.0.0.0	5->5
	Not existing car	2023-07-18 14:38:55	CAPGEMINI	0.0	.0.0 0	0.0.0	5->5 10

Figure 95: Unauthorized driver event.

Car Owner workspace © Car Owner workspace © Ra © RaC © RAC © RAC © TIM XL-SIEM © SADE[Allow new driver © SADE[Allow new driver © SADE] Insert PIN © SADE] Insert PIN © Car		🗮 🖉 Tools 🗸 📋 Clear					C fishy_sc
An error occured. Given file does not exist. Please make sure the logfile is present in the given directory. Warning: session_start(): Cannot send session cockie - headers already sent by (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent by (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers already sent (output started at Just/share/ossim/include/dasses/Security.inc.255) in Just/share/xd-siem/index.php on line 8 Warning: session_start(): Cannot send session cockie - headers Not reflexin in 297 seconds. Or click here to reflexin now Filters and Options View Grouped (1.38) Papity label to selec	FISHY	⊗ TIM XL-SIEM					
R AE	𝒫 Car Owner workspace	An error occured: Given file does not exist. Please make Warning: session_start(): Cannot send session cookie -	sure the logfile is present in headers already sent by (ou	the given directory. Iput started at /usr/share/oss (output started at /usr/share)	sim/include/classes/Security.ir	nc:255) in /usr/share/xl-siem/	index.php on line 8
 	∮ IRO		nitor - Hoadors diready sent	(ouput seared at /ds//shale/ Weld	come > Logout	y.nv.2557 in MSI/Share/Ai-Sie	mendex.php on me
	₿ SACM	🧐 XU	SIEM	ato	os XL-SIEM		
Image: Sade plane with the same of Options Image: Sade plane with the sade plane with the same of Options Image: Sade plane with the sade p	ß RAE	Dashboards SIEM Analysis Repo	rts Next refresh in :	297 seconds. Or click here to	o refresh now		0
Image: Sade Sade Sade Sade Sade Sade Sade Sade	Ø TIM XL-SIEM	Filters and Options					hi.] 🗳
Signature Events Risk Duration Source Destination Status SADE] Insert PIN	SADE] Allow new SADE] SADE] SADE] SADE]	Ø View Grouped		(1-38)		Apply label to	selected alarms
Image: SADE Insert PIN Image: Facial recognition failure 2 5 0 secs 0.00.0 ANY 0.00.0 ANY open Image: Clear Image: Brute force attack against car 6 10 49 secs 0.00.0 ANY 0.00.0 ANY open	river	Signature	Events	Risk Duration	Source	Destination	Status
Facial recognition failure 2 5 0 secs 0.000 ANY 0.000 ANY In Clear Brute force attack against car 6 10 49 secs 0.000 ANY 0.000 ANY 0.000 ANY	A ISADEL Incort DIN			Tuesday 18-Jul-2023 [Del	lete]		
Clear Brute force attack against car 6 10 49 secs 0.00.0.ANY 0.00.0.ANY open	[SADE] INSERT PIN	Facial recognition failure	2	5 0 secs	0.0.0.0:ANY	0.0.0.0:ANY	
							open

Figure 96: First unauthorized driver alarm.

For now, it could have been an error of the FR module due to poor lighting or the driver wearing a mask, for example. The vehicle does not power on and the thief tries it again. In case the FR fails again, the system understands that the person is not allowed to drive this vehicle. The FR will be blocked and XL-SIEM will raise a PIN blocked alarm.

Document name:	D6.4 IT-2 FISHY final release					Page:	84 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	=	🖉 Tools 🗸 📋 Clear						S fishy_sc
CIPUIU								
FISHS	⊗ TIM X	XL-SIEM						
ar Owner	An error occur Warning ses	red: Given file does not exist. Please make sur sion_start(): Cannot send session cookie - hea	e the logfile is preser iders already sent by	nt in the giv (output sta	en directory. arted at /usr/share/os	sim/include/classes/Security.i	nc:255) in /usr/share/xl-siem/	/index.php on line 8
orkspace	Warning: ses	sion_start(): Cannot send session cache limiter	r - headers already s	ent (output	started at /usr/share/	/ossim/include/classes/Secur	ity.inc:255) in /usr/share/xl-si e	em/index.php on line
9 IRO	8				Web	come ▶ Loqout		
SACM				Λ	ato	s XL-SIEM		
GAGIN								
RAE	►c	Dashboards IN SIEM Analysis IN Reports	Next refrest	n in 204 sec	ronds. Or click bere to	refrech prov		0
RAE	► Filters a	Aashboards > SIEM Analysis > Reports	Next refrest	n in 294 sec	conds. Or click here to	refresh now		
RAE TIM XL-SIEM [SADE] Allow new	► Filters a	Aushboards SIEM Analysis Reports and Options ew Grouped	Next refrest	n in 294 sec (1-4	conds. Or click here to	refresh now	► Apply label to	lil. C selected alarms
RAE TIM XL-SIEM [SADE] Allow new ver	 Filters a Ø Vi 	Aushboards SIEM Analysis Reports and Options ew Grouped Signature	Next refrest	n in 294 sec (1-4 Risk	conds. Or click here to 40) Duration	refresh now	► Apply label to Destination	c ki,i C selected alarms Status
RAE TIM XL-SIEM [SADE] Allow new ver	 Filters a Ø Vi I 	ew Grouped Signature	Next refrest	n in 294 sec (1-4 Risk Tuese	conds. Or click here to 40) Duration day 18-Jul-2023 [Del	refresh now Source ete]	► Apply label to Destination	II.IC selected alarms Status
RAE TIM XL-SIEM [SADE] Allow new /er [SADE] Insert PIN	> Filters a	eshbaards > SIEM Analysis > Reports and Options ew Grouped Signature Facial recognition failure Input: PIN	Next refrest Events 3	n in 294 sec (1-4 Risk Tues 10	40) Duration day 18-Jul-2023 (Del 2 mins	refresh now Source etej 0.0.0.0.NY	Apply label to Destination 0.0.0.0 ANY	selected alarms
RAE TIM XL-SIEM [SADE] Allow new ver [SADE] Insert PIN Clear	> Filters a	eshbaards SIEM Analysis Reports and Options ew Grouped Signature Facial recognition failure Input: PIN Facial recognition failure	Next refrest Events 3 2	n in 294 sec (1-4 Risk Tuese 10 5	40) Duration day 18-Jul-2023 (Del 2 mins 0 secs	refresh now Source etel 0.0.0.0.ANY 0.0.0.0.ANY	Apply label to Destination 0 0 0 0.0 ANY 0 0 0 0.0 ANY	selected alarms Status open open

Figure 97: Second unauthorized driver alarm à Pin blocked alarm

In this case we can see the RAE reaction too. It analyses the qualitative and quantitative risk associated with different alarms. Now, with the second facial recognition failure. We can see the assets exposed in this case, the risk they are exposed to and the potential economic cost that will suppose in the case of the attack was not prevented.

	≡ & Too	ls ∽			⊖ fishy_sc ∨
FISHY	& RAE				
₿ RAE		Risk Model:	WRP101: Session hijacking Attack	VERY HIGH	^
윤 XL-SIEM		Risk WRP101-R1:	Sensitive data exposed to unauthorized users	VERY HIGH	
			Sade car server (10.0.0.2)	VERY HIGH	
		Risk WRP101-R2:	Service disrupt	HIGH	
			Sade car server (10.0.0.2)	HIGH	
		Risk WRP101-R3:	Transmitted data alteration	VERY HIGH	- I
			Sade car server (10.0.0.2)	VERY HIGH	- 1
		Risk Model:	WRP102: Bypass Login Attack	VERY LOW	- 1
		Risk WRP102-R1:	System disrupt or data deletion	VERY LOW	- 1
		Risk WRP102-R2:	Unauthorized acc ^{[hg} s to private data	VERY LOW	
		Risk WRP102-R3:	Unauthorized data alteration or corruption.	VERY LOW	

Figure 98: Qualitative risk analysis.

Document name:	D6.4 IT-2 FISHY final release						85 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



11	🔳 🖉 Тоо	ls ∨ 🖞 Clear			\circ fishy_sc \checkmark
FISHY					
	& RAE				
₿ RAE					î
₿ XL-SIEM		Cyber-risk Status Qu	antitative		
🖞 Clear			Overall cyber-risk status:		
			Typical Loss:		
			Worst Case:		
		Risk Model:	WRP101: Session hijacking Attack	Typical Loss:	
		Risk WRP101-R1:	Sensitive data exposed to unauthorized users	Typical Loss:	
			Sade car server (10.0.0.2)	Typical Loss: 3,050.00 EUR -	
		Risk WRP101-R2:	Service disrupt	U Typical Loss: •	
			Sade car server (10.0.0.2)	Typical Loss: 1,450.00 EUR 💌	
	CRAE v1.3	Risk WRP101-R3:	Transmitted data alteration	Typical Loss: •	

Figure 99: Quantitative risk analysis.

IRO has seen the alarm in the central repository and makes a new call to another SADE endpoint to advise all the allowed drivers that if are they who are trying to power on the vehicle, they must enter their personal PIN though the FISHY dashboard to try the facial authentication again.

New r	not authorized power on try - PIN blocked car $\ \ \ \ \ \ \ \ \ \ \ \ \ $
a a	raducir mensaje a: Español Nunca traduzca de: Inglés
S	send.secure.mail.fishy@gmail.com⋮Image: Compare: ['miguel.juaniz-lopez@capgemini.com']Para: ['miguel.juaniz-lopez@capgemini.com']Mié 02/08/2023 9:54
	*****This mail has been sent from an external source. Do not reply to it, or open any links/attachments unless you are sure of the sender's identity.******
	You must introduce your PIN in your SADE API dashboard.
	\leftarrow Responder $ ightarrow$ Reenviar

Figure 100: Mail telling the allowed drivers to input its PIN.

Unauthorized PIN

Presuming the FR module is blocked. As we have said, the user must use the FISHY dashboard to insert its personal PIN. To do it, it needs to identify itself with its ID, tell FISHY the FR of which vehicle wants to reactivate (Using the vehicle ID) and insert the PIN.

Document name:	D6.4 IT-2 FISHY final release					Page:	86 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	≡ 🖉 Tools ∨ 🖞 Clear		$\stackrel{\circ}{\sim}$ fishy_sc \checkmark
FISHU	⊗ [SADE] Insert PIN		
Car Owner workspace			
₿ IRO		SELECT YOUR CAR 🖻	
B SACM		Select car: 22580003-4144-4085-bc3d-6cef407d6706	
ℬ RAE		Insert PIN:	
₿ TIM XL-SIEM			
[SADE] Allow new driver		Submit	
[SADE] Insert PIN			
🖞 Clear			

Figure 101: Insert PIN form in the car owner workspace in FISHY dashboard.

If the PIN is not correct, a new event will be generated the same way as previously.

	E Sols V Clear		o fishy_sc ∨
CICLUU			
FISHS	⊗ [SADE] Insert PIN		
🔑 Car Owner		8	
workspace		PIN is wrong. 5 attempts	
₿ IRO		left. Please try again.	
₿ SACM		<u>Go back</u>	
₿ RAE			
₿ TIM XL-SIEM			
[SADE] Allow new driver			
🕆 Clear			
2022 07 18 12-55-21 10200	1 [44] [EPROP] [402] Unauthorized P	TN for care JIEQ0003 1111 1085 bodd Conf10746706 and	TD: 721/2600Y Attomate laft. 5

Figure 102: Unauthorized PIN error

Document name:	D6.4 IT-2 I	FISHY final release				Page:	87 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



									C fishy_s	SC
FISHY	⊗ TIM XL-SIEM									
Car Owner	Search Clear	I	Back 💫 R	efresh 秒	Current	t Searc	h Criteria [Clear	All Criteria] 🕨	Show full criteria	
Inspace	search term	IP	Signature	Pavload	META		PAYLOAD	IP	LAYER 4	
10.0			orginataro	, aj loud	any		any	any	none	
RO	Sensor Data Sou	urces		Risk						
	xlsiem-server V		~	~			Summar	y Statistics		
SACM	More Filters	Taxonon	ny and Reputa	tion Filters	Events 🛛	2 🖻	Unique Events	Sensors	Unique Data Sources	
RAE	Time frame selection GMT+2:00: 🛐 Today Last 24h Last 2 days Last We	ek Last 2 W	Timeline ar /eeks Last N	nalysis: 📆 Ionth All	Uniqu address Source Destinat	ue ses: e tion	Source Port: TCP UDP Destination Port: TCP UDP	Taxonomy Product Types Categories	Unique IP links [FQDN] Unique Country Events] s
TIM XL-SIEM									Custom Views	
[SADE] Allow new	Displaying events 1-50 of about thousands m	natching your se	election.					1	4,387 total events in database	5e
er	Signature	• 5	Date GMT+2:0	0 v Sen	isor	Sou	rce Des	stination	Asset S → D Risk	
	🍺 🔲 Unauthorized pin	202	23-07-18 15:55	31 CAPG	EMINI	0.0.0	0.0 0	0.0.0.0	5->5 6	
SADEJ Insert PIN	Unauthorized Driver	202	23-07-18 15:52	36 CAPG	EMINI	0.0.0	0.0 0	0.0.0.0	5->5	
	Unauthorized Driver	202	23-07-18 15:50	16 CAPG	EMINI	0.0.0	0.0 0	0.0.0.0	5->5	
Clear	S Not existing car	202	23-07-18 14:38	56 CAPG	EMINI	0.01	0 0	000	5->5	

Figure 103: The evant of unauthorized PIN error as shown in the dashboard.

There are five attempts, at the fifth failed PIN, the vehicle will be completely blocked. A new alarm will be raised, and the IRO will have to call to a new endpoint. This call will notify all the allowed drivers for this car that the dealer has to be asked to unlock the vehicle.

	=							$\stackrel{\rm O}{\frown}$ fishy_sc \checkmark
FISHY	⊗ TIM	XL-SIEM						
Car Owner workspace	An error occ Warning: se 8	sured: Given file does not exist. Please make sure assion_start(): Cannot send session cache limiter	e the logfile is preser r - headers already se	t in the giv ant (output	ren directory. started at /usr/sha	re/ossim/include/classes/Securi	y.inc:255) in /usr/share/xl-sie	m/index.php on line
₿ IRO			SIEN	Λ	a	tos XL-SIEM		
₿ SACM		Dashboards	ation Reports	-				_
& RAE	Filters	s and Options	Next refresh	in 295 see	conds. Or click here	e to refresh now		
ℬ TIM XL-SIEM	Ø	View Grouped		(1-	41)		Apply label to	selected alarms
[SADE] Allow new		Signature	Events	Risk	Duration	Source	Destination	Status
driver				Tues	day 18-Jul-2023 [[Delete]		
		Car Blocked	2	10	0 secs	0.0.0.0:ANY	0.0.0.0:ANY	open
ℬ [SADE] Insert PIN		Facial recognition failure Input: PIN	3	10	2 mins	0.0.0.0:ANY	0.0.0.0:ANY	open
A Clear		Facial recognition failure	2	5	0 secs	0.0.0.0:ANY	0.0.0.0:ANY	open
		Facial recognition failure	2	5	0 secs	0.0.0.0.ANY	0.0.0.0.ANY	open

Figure 104: Car blocked alarm.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	88 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4.3.3 Demo script for Sequel C and D - Software patch certification and correction

In this new scenario a main well-known weak link in the automotive supply chain will be addressed, the software patch certification.

The vehicle has IoT devices, and they have a software running on them. Here appears the opportunity for an attacker to introduce malware or make a code injection into these IoT devices. We are seeing how FISHY is preventing it.

The vehicle is sending continuously their IoT devices sw versions to a RabbitMQ queue located in the SADE Domain 1, which is connected to the whole FISHY through SIA. And the current software versions of the devices can be managed by its manufacturer through SADE API. It cans update, revoke and add certifications.

H							⊖ fishy_sa ∨
FISHY	⊗ [SADE] Add Certification						
Manufacturer workspace		Add Ce	ertifica	tion (ţ		^
₿ IRO		Device manufactu	urer:				
₿ SACM							
[SADE] Add Certification		Device model:					
		Firmware version:					
		Checksum:					
🖞 Clear							
		🗌 Online update					
1	🗮 🖉 Tools 🗸 📋 Clear						o fishy_sa ∨
FISHU	⊗ [SADE] Revoke Certification						
Manufacturer workspace							
₿ IRO		Re	evokab	ole			
& SACM		Cert	ificatio	ns 🕅			
[SADE] Add Certification		Manufacturer	Model	Versions	Revoke		
ℬ ISADE1 Revoke		Capgemini	Remotis ECU	1.0 1.0	1.0 1.0	x	
Certification		Sekonix	SF3324-100	2.0.0	2.0.0	×	
		Sekonix	SF3324-105	0.5.0	0.5.0	×	
🖞 Clear							

Figure 105: Certification management in the manufacturer workspace.

The SACM module is constantly comparing both certifications. The ones installed on the car and the ones published by the manufacturer through SADE API. This comparison results in a monitoring of the SW certifications of the vehicle.

Let us suppose that the manufacturer has found a vulnerability in one of its devices and it launches a new software patch and revokes the vulnerable one. SACM will realize and it cans notify to dealer

Document name:	D6.4 IT-2 I	ISHY final release				Page:	89 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



and/or vehicle owners about insecure software or even notify to the owners for a recall to the dealer or for an Online update if it is possible.

[Manu	ıfacturer] Certification issue detected by Fishy. $\ \ \textcircled{G} \ \lor \qquad \qquad \ \ \textcircled{\oplus} \ \lor \qquad $	
≣aj∎ T	raducir mensaje a: Español Nunca traduzca de: Inglés	
S	send.secure.mail.fishy@gmail.comImage: Image: I	
	******This mail has been sent from an external source. Do not reply to it, or open any links/attachments unless you are sure of the sender's identity.*****	
	The SF3324-100 model of Sekonix (serial number ABCD-ABCD-ABCD-0001) is not updated. Latest version: 2.0.0. Current version: 1.0.0 Please update the following cars: ['22580003-4144-4085-bc3d-6cef407d670']	
	\leftarrow Responder \rightarrow Reenviar	

Figure 106: Mail asking manufacturer to update an IoT device online.

[Dealer] Certification issue detected by Fishy. $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	€, ~
្នីភ្នំ Traducir mensaje a: Español Nunca traduzca de: Inglés	
send.secure.mail.fishy@gmail.com	 ≪ → … • 02/08/2023 13:17 ✓ to it, or • intity.****** CD-0001) is • ipdate, please 3d-
$\leftarrow \text{Responder} \qquad \overrightarrow{} \text{Reenviar}$	

Figure 107: Mail asking dealer to schedule a recall to update components offline.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	90 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4.3.4 Demo script for Sequel E - Vehicle compromised

Let us suppose that someone has taken the control of the vehicle. That someone has been able to power-on the vehicle bypassing the authorization. The vehicle, each time it is started, it generates an event pointing its VIN.

As is logical, in a normal situation, the driver identifies itself and then can start the vehicle. This will generate two consecutive events, an authorized driver for the X vehicle and this X vehicle started.

1							on fishy_sb ∨
FiSHY	⊗ TIM XL-SIEM						
	Dashboards > SIEM Analysis > Re	ports					^
ß IRO	Real Time Trend Graph by GMT+2:00 data	tes					0
Ø SACM	Search Clear	Back	esh 🚷	Current Sear	rch Criteria [Clear	All Criteria] 🕨	Show full criteria
6 OAOM	Search term	IP Signature P	ayload	META	PAYLOAD	IP	LAYER 4
Ø RAE	Sensor Data Source	Piel		any	any	any	none
0.00	xlsiem-server v	· · · · · ·	~		Summary	Statistics	
ℬ TIM XL-SIEM	More Filters	Taxonomy and Reputation	n Filters	Events 🛃 📰	Unique Events	Sensors	Unique Data Sources
	Time frame selection GMT+2:00; Today Last 24h Last 2 days Last Week	Timeline analy	ysis: 📆 th All	Unique addresses: Source Destination	Source Port: TCP UDP Destination Port: TCP UDP	Taxonomy Product Types Categories	Unique IP links [FQDN] Unique Country Events
(SADE) Add Vehicle							Custom Views
	Displaying events 1-50 of about thousands match	ing your selection.				14	,836 total events in database.
🖞 Clear	Signature	Date GMT+2:00	Senso	or Sour	rce Desti	nation A S	sset Risk
	Car_started	2023-07-23 14:26:40	N/A	0.0.0	0.0 0.0	0.0 5	->5
	Authorized_driver	2023-07-23 14:26:38	N/A	0.0.0	0.0 0.0	.0.0 5	->5 7

Figure 108: Normal workflow of a vehicle power on.

If someone bypass the authentication, the started vehicle event will be raised alone. So we can suppose that the vehicle is dangerous. XL-SIEM will understand that and will raise a compromised car alarm.

	▶ Dashboards ► SIEM Analysis ► Rep	ports				
ACM AE	Car started with malware (Direct	ive 100115) 2 Open Events	9 Risk →	t 52 secs 2 hour	s ago	
MXLSIEM	► Source	I Destination		R Knowledg	e base	
IN AL-SIEW	0.0.0.0	0.0.0.0	do not direc assets critic	do not directly indicate malicious activity, they reference assets critical to your business processes, and may indice		
SADE] Full Sade	📌 Location: Unknown	📌 Location: Unknown	failures, mis processes.	sconfigured systems or no	oncompliant business	
	OTX: No	OTX: No				
	Ports Unknown	Ports Unknown	Documer	nt Summary		
SADE] Add Vehicle			Read More	Articles (1)		
Clear						
	Source (1) Destination (1)	rent Detail				
	# Alarm	Risk Date	Source	Destination	Correlation	
	1 Car started with malware	9 2023-07-23 14:26:40	0.0.0.0:ANY	0.0.0.0:ANY	2	
	2 Car_started	5 2023-07-23 14:26:40	0.0.0.0:ANY	0.0.0.0:ANY	1	

Figure 109: Possible malware alarm.

That alarm will be received by the IRO and it will react deactivating that vehicle by a SADE API call.

Document name:	D6.4 IT-2 FISHY final release					Page:	91 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



[Man	ufacturer] Certification issue detected by Fishy. $\ \ \ \ \ \ \ \ \ \ \ \ \ $							
∎ð,	Fraducir mensaje a: Español Nunca traduzca de: Inglés							
S	send.secure.mail.fishy@gmail.com Para: Juaniz Lopez, Miguel Mié 02/08/2023 12:30							
	*****This mail has been sent from an external source. Do not reply to it, or open any links/attachments unless you are sure of the sender's identity.******							
	The SF3324-100 model of Sekonix (serial number ABCD-ABCD-ABCD-0001) is not updated. Latest version: 2.0.0. Current version: 1.0.0 Please update the following cars: ['22580003-4144-4085-bc3d-6cef407d670']							
	\leftarrow Responder $ ightarrow$ Reenviar							

Figure 110: Mail asking manufacturer to update an IoT device online.

[Dealer] Certification issue detected by Fishy.	Ð, ~							
ង្វី Traducir mensaje a: Español Nunca traduzca de: Inglés								
 send.secure.mail.fishy@gmail.com Send.secure.mail.fishy@gmail.com Para: Juaniz Lopez, Miguel ******This mail has been sent from an external source. Do not reply to it, o open any links/attachments unless you are sure of the sender's identity.*** The SF3324-100 model of Sekonix (serial number ABCD-ABCD-ABCD-000⁻ not certified. Latest certified version: 2.0.0 Not possible an online update, p schedule a recall for the following cars: ['22580003-4144-4085-bc3d-6cef407d670'] Responder	 → …)23 13:17 r **** is blease 							

Figure 111: Mail asking dealer to schedule a recall to update components offline.

Document name:	D6.4 IT-2 FISHY final release					Page:	92 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4.4 FISHY-enabled security enhancement in SADE pilot

As presented in deliverables D6.1 and D6.3, in the Securing Autonomous Driving Function at the Edge supply chain, to protect information about software and prevent software vulnerabilities detected throughout time, we have implemented the components that deliver information from the deployed SADE platform to the FISHY platform. Data are consumed by the FISHY platform asking via REST/RabbitMQ.

For all the following rules/scenarios to be validated the following components are involved:

TIM: detects and checks whether the condition is satisfied, (attacks, failures in the infrastructure or data, unauthorized power on in the vehicle, etc).

DASHBOARD: presents to the FISHY user the detected security events and allow dealers to register vehicles, personal data about owners and certifications included by OEMs.

IRO: Create intents to match what is happening in the environment infrastructure with policies to be enforced to mitigate attacks, threats, etc. In addition, it can perform action policies against SADE API using REST.

SPI: Allows access to the information about existing vehicles, and personal data. It also controls who can access, and the type of access by using Role based model.

SIA/NED: Allows a secure communication between different domains: EDGE, Cloud, and control services. SADE Platform will be allocated into the Cloud but some specific services of the vehicle are deployed into the EDGE. Interconnection of services in the cloud with the FISHY control services will be needed perform mitigation and operations. [2][6]

Returning to the subject of the above attacks, we are seeing how the system acts against them. For example, starting with the type 4 attacks, the code injection or malware injection through the IoT hardware's software.

The following table shows an example of information that OEMs add using FISHY dashboard to certify its software versions. This information is stored in the data base.

Model	TempMeterXXX
SW Version	1.1235
Safe Update Link (optional)	https://company.com/updates/TempMeterXXX/1.1235/firmware.bin
Update checksum (optional)	5a000ca5302b19ae8c7a66149f3e1e98

Table 17: Example of information OEMs add using the FISHY dashboard to certify their software versions

Data from vehicles will be sent to FISHY in the form of a JSON object which will include: UUID (Unique Universal ID, Timestamp (UTC timestamp) and Metadata.

FISHY Component	Components	Used in F2F	NOTES
SPI	Identity Manager	YES	WBP user is authenticated /authorized In FISHY platform

Document name:	D6.4 IT-2 FISHY final release					Page:	93 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	Data Management	YES	Transparent to the use case				
TIM	PMEM	NO	Incidents/attack detection on the IoT infrastructure and the SAP web dispatcher (via logging interpretation)				
	XL-SIEM	YES	Incidents/attack detection on the IoT infrastructure and the SAP web dispatcher (via logging interpretation)				
	RAE	YES	Risk analysis based on the detected incidents by XL- SIEM in terms of loss of availability, integrity or confidentiality				
	VAT	NO					
	WAZUH	NO					
	Trust Monitor	YES					
	Zeek	NO	lot network traffic monitorization tool				
	Smart Contracts	YES	Policies suggested to mitigate threats and attacks				
SACM	Evidence Collection Engine	YES	ELK and RABBITMQ deployed and SADE API. deployed in domain 1.				
	Auditing Mechanism	YES					
IRO	Intent Manager	YES	Components, events and alarms visualization				
	Knowledge Base	YES					
	Policy Configurator	YES					
	Dashboard	YES					
	Learning & Reasoning	YES					
EDC	Controller	YES	Policies suggested to mitigate threats and attacks				
	Register & Planner	YES					
	Enforcer	YES					
SIA	IoT Gateway	YES					
FISHY appliance	LOMOS, PMEM	YES					

Document name:	D6.4 IT-2 FISHY final release					Page:	94 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



```
{
"metadata": {
        "sw_data": [{
                    "manufacturer": "Capgemini Engineering",
                    "model": "TempMeterXXX",
                    "sw version": "1.1235",
                    "serial number": "sensor ht:257d0001XXXX",
                  },
                  {
                    "manufacturer": "Capgemini Engineering",
                    "model": "CamSensorXXX",
                    "sw version": "0.1",
                    "serial_number": "sensor_cam:1d101s",
                  }
                 ],
        "vin": "0000-0000-0000-0001",
        "timestamp": "1624003974",
},
"UUID": ""
}
```

Figure 112: JSON object including vehicle data in SADE use case

As previously explained in D6.1, D6.2 and D6.3, SADE will send this information to a RabbitMQ exchange, deployed in the Sandbox of the FISHY domain 1 as a k8s POD.

- SACM must get JSON messages and parses the received information.
- SACM compares with SW certification versions provided by OEMs that can be recovered from the SADE API using REST.

RULES

- There is one rule that checks if one version received is not certified:
 - FISHY notifies/alerts users related to the compromised vehicle.
 - FISHY enforces Update* policy against SADE Service (REST API module)

* If an updated version model is certified and contains a safe link for an update, that link must be provided; if not, our service will start a recall notification. FISHY just does not send any link in the POST request.

On the other hand, with the rest of attacks we can follow the same flow. Data collectors send logs to XL-SIEM. XL-SIEM in turn sends elaborated events and alarms to RAE that can calculate in real-time the cyber risk exposure. IRO filters these logs and, depending on the policies, acts consequently.

An agent of the XL-SIEM is deployed as part of the FISHY appliance and sends logs for the XL-SIEM to detect those attacks. This agent is in charge of obtaining the log files from a number of services related to SADE use case and will make them available to the RAE.

Log files collected are from:

- RabbitMQ server.
- NGINX + gunicorn SADE API
- NGINX + gunicorn DB connector API

Document name:	D6.4 IT-2 FISHY final release					Page:	95 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



The agent will be deployed in the same CLOUD infrastructure (same domain) as the other services of the use case, allowing access to the logs by mapping volumes to a common directory, which is accessible by the agent. These logs, once collected, are sent to the central repository.

From the central repository, the IRO can get those logs in a common format which unifies all the pilots. For those logs it will have some policies and depending on them, it will react in some way. In the case of SADE, and due to complications with other modules, IRO will react against SADE API directly through REST calls.

These calls depend on the different use cases:

- UC1. Several access attempts with non-activated vehicle.
 - o RULE:
 - 5 x not existing car log \rightarrow send mail to local operator.
 - [POST] <u>https://192.168.0.103:5000/api/actions/report_local_operator</u> {'subject':", 'message': "}
- **UC2.1.** Attempt to power on by unauthorized driver.
 - RULE:
 - 2 x unauthorized driver log \rightarrow send mail to owner.
 - [POST] <u>https://192.168.0.103:5000/api/actions/send_mail</u> {'VIN': 'vin_number[uuid4]', 'subject':'', 'message': ''}
- UC2.2. Too many PIN input attempts failures. Car blocked.
 - RULE:

- 1 x unauthorized PIN. Car blocked → Send mail to owner.
 - [POST] <u>https://192.168.0.103:5000/api/actions/send_mail</u> {'VIN': 'vin_number[uuid4]', 'subject':'', 'message': ''}
- **UC5.** Duplicated behicle for traffic tampering.
 - o RULE:
 - 2 x vehicle started with the same vin in a short period of time, or 1 x started vehicle without previous authorized driver in a short period of time. → Deactivate car.
 - [DELETE] https://192.168.0.103:5000/api/actions/vehicles/{vin}

4.5 Improvements compared to IT-1 and final assessment

As far as the use case is concerned, we have solved some integration difficulties due to the situation we are in and the fact that the components are still in the development phase. However, the great work of the partners has facilitated the deployment of the components and the integration with the use case. Also, the definition of the flows has allowed to consolidate the architecture of the use case solution.

In the first iteration, the state of the integration could only allow us to see the monitoring function of FISHY. That is, the secure communication thanks to the SIA-NED integration and the logging monitoring thanks to XL-SIEM integration.

Until now, the previous integrations have been advanced and there have been new ones. For example, the IRO. Until now, as we said, we only were taking advantage of the monitoring functionality of FISHY. Nevertheless, with the addition of IRO we could complete the cycle. The system was monitored and if something dangerous occurs, it can react and solve it or suggest some solutions.

Document name:	D6.4 IT-2 FISHY final release					Page:	96 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



4.6 KPIs satisfaction

Since D6.3 the final list of revised metrics we were to focus on the pilot evaluation activities, using Iteration 2 of the FISHY platform, were set. The metrics and the achieved values are seen in the following table:

Metric ID	Metric description	Туре	Target value	Achieved value
SC3_T1	Detect unauthorized access to the vehicle.	Technical	1	1
SC3_T2	Integrate inside SIA – secure biometric function	Technical	True	True
SC3_T3	Integrate inside SIA – Software update function	Technical	True	True
SC3_B1	Reduce recall operation to the car's dealer	Business	True	True

Table 18: Business and Technical metrics defined in D6.3

Document name:	D6.4 IT-2 I	FISHY final release				Page:	97 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



5 FISHY IT-2 overall evaluation

Based on the description of the piloting activities, it becomes evident that the IT-2 version of the FISHY platform is significantly enhanced compared to the IT-1 both with respect to functional capabilities and with respect to user friendliness. The activities have led to a set of important messages:

- <u>Key message 1.</u> FISHY platform protects the considered supply chain IT systems from the attacks of interest to their operators: In all supply chains, the operators defined attacks of interest and demos showcasing that FISHY protects against these attacks have been produced and are described in detail in chapter 2, 3 and 4. These attacks includes among others unauthorised user access attacks, unauthorised devices access attempt attacks, brute force attacks, Denial of Service Attacks and DDoS attacks, network-relevant and end-point specific attacks and more sophisticated blockchain specific attacks.
- <u>Key message 2.</u> FISHY platform protects the considered supply chain IT systems against additional attacks: After internal discussions, the consortium agreed that a number of additional attacks can be demonstrated with these attacks being of wide interest. Thus, for example, in the F2F use case, the protection of specific end points (thanks to VAT component) has been demonstrated and other network level attacks have been protected based on PMEM components which employs Machine Learning algorithms. This proves that the FISHY platform is capable of detecting additional attacks upon appropriate configuration of the components through the dashboard.
- <u>Key message 3.</u> FISHY platform can protect against 80% of the identified supply chain attacks based on the employed components: FISHY platform integrates components that implement techniques which according to the MITRE@Attack framework can be used to detect and mitigate 80% of the currently defined attacks. More precisely, 81% in the F2F supply chain and 66% in the other two, as discussed in the individual chapters (2, 3 and 4). Apart from configuration of the components, in certain cases, some development of the appropriate mechanism to provide FISHY with the required supply chain platform details and data may be needed but this is considered minor once the components and their UI to the administrators is ready.
- <u>Key message 4.</u> FISHY platform- IT-2 has efficiently addressed the feedback collected up to M18. In the individual chapters, it is stated that the updated version satisfies the targeted KPIs overvoming the deficiencies point out in D6.2.
- <u>Key message 5.</u> All the components of the FISHY platform have been evaluated in at least two use cases. The table of components per use case is shown below. The evidence of this involvement has been presented in chapters 2-4. There are few components like PMEM, Trust monitor, VAT and ZEEK that were added in the 2nd half of the project to test and showcase that FISHY framework is flexible enough to integrate additional detection tools as they appear in the market. This way FISHY -IT-2 can be considered a version of the platform with sufficient tools to detect high number of attacks and it is very easy to enrich it to move to the 100% of identified attacks.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	98 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



FISHY Component	Components	F2F	WBP Trust	SADE
SPI	Identity Manager	YES	YES	YES
	Data Management	YES	YES	YES
тім	PMEM	YES	NO	NO
	XL-SIEM	NO	YES	YES
	RAE	NO	YES	YES
	VAT	YES	NO	NO
	WAZUH	YES	YES	NO
	Trust Monitor	NO	NO	YES
	Zeek	NO	YES	NO
	Smart Contracts	YES	YES	YES
SACM	Evidence Collection Engine	YES	YES	YES
	Auditing Mechanism	YES	YES	YES
IRO	Intent Manager	YES	YES	YES
	Knowledge Base	YES	YES	NO
	Policy Configurator	YES	YES	YES
	Dashboard	YES	YES	YES
	Learning & Reasoning	YES	YES	NO
EDC	Controller	YES	YES	YES
	Register & Planner	YES	YES	YES
	Enforcer	YES	YES	YES
SIA	IoT Gateway	YES	NO	YES
FISHY appliance	LOMOS, PMEM	YES	YES	YES

Table 19: FISH	Y components	used in each	of the three	pilot cases

- <u>Key message 6.</u> FISHY platform IT-2 is user friendly: During this final round of piloting, special emphasis was placed on the assessment of the user interface. The evaluation was carried out in the F2F use case by people from SYN and Entersoft a) involved in the FISHY project and b) outside the FISHY project. The results show that this has significantly been improved reaching the value of 4.2 (in 5-points Likert scale) in the F2F case where this was quantified.
- <u>Key message 7.</u> The flexible deployment of the FISHY platform is well appreciated. The end users showed interest in the different deployment options that were presented based on D2.4. Thus, FISHY consortium decides to keep this into consideration during the commercialisation phase.

Document name:	D6.4 IT-2	FISHY final release				Page:	99 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



6 Conclusions

In this document we have described the FISHY IT-2 deployments in the infrastructures of the threepilot premises and the results from the validation of the capability of FISHY to meet the user requirements reported in D2.3, i.e. to detect and mitigate the set of attacks of interest to the pilot partners. Additionally, we have evaluated the capability of FISHY platform to detect attacks outside this predefined set. To make sure that FISHY platform focuses on supply chain attacks, we have modelled these attacks according to the ENISA model for supply chain attacks Furthermore we have used the MITRE@ATTACK navigation tool, to examine whether the adopted detection techniques and mitigation measures are aligned with those captured by MITRE. The analysis of the evaluation results from the three different supply chain systems has allowed us to capture a set of key messages that will guide the consortium in the commercialization phase of FISHY. **These messages reveal that FISHY platform is capable of detecting and mitigating a large number of supply chain specific attacks, while providing deployment flexibility (on premise or on cloud) and providing adequate control to the operators of the supply chain systems. Additionally, the introduction of machine-learning based modules maximises its potential to detect unknow (today) attacks.**

Document name:	D6.4 IT-2 I	ISHY final release				Page:	100 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



7 References

- [1] FISHY, D6.2 "IT-1 FISHY release validated", 2022
- [2] FISHY, D6.3 "Use cases settings and demonstration strategy Use cases settings and demonstration strategy", 2022
- [3] FISHY, D5.2 "IT-2 FISHY release integrated", 2023
- [4] FISHY, D2.4, "Final Architectural design and technology radar", 2023
- [5] FISHY, D7.4, "Report on dissemination, standards and exploitation (Y3)", 2023
- [6] FISHY, D6.1, "Use cases settings and demonstration strategy (IT-1)", 2022.
- [7] <u>https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks</u>
- [8] https://attack.mitre.org/
- [9] https://attack.mitre.org/
- [10]https://mitre-attack.github.io/attack-navigator/
- [11]Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., Loukas, G.: Sok: The MITRE ATT&CK Framework in Research and Practice (2023). https://doi.org/10.48550/ARXIV.2304.07411
- [12]Santos, H.M.: Cybersecurity: a practical engineering approach. CRC Press (2022)
- [13]Ahmed, M., Panda, S., Xenakis, C., Panaousis, E.: MITRE ATT&CK-driven Cyber Risk Assessment. pp. 1–10. ACM (8 2022)

[14]https://www.imperva.com/learn/ddos/ping-icmp-flood/

Document name:	D6.4 IT-2 I	FISHY final release				Page:	101 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



8 Annex: User Manual

The FISHY dashboard is currently located in the FISHY Reference Framework (accessible through VPN) in <u>https://10.4.34.136</u>. For login we have to fill the login and password.

FISHY	
Login Signup	
fishy ••••• Forgot password?	
Signin	

Figure 113: Accessing FISHY dashboard

When accessing, the main page is the IRO.

Alience Alience Alience Ordepurations Output alientities Alience Alience Output alientities Alie			
BO Dashboard Dashboard Dashboard Write your Intents Too the or or			0
Aress Confurcions Confurcions <td>Dashboard</td> <td></td> <td></td>	Dashboard		
Configuration Usage : fro commando cargos Usage : fro commando cargos Usage : recettar register reset usage : reports cargos ifor reports from a tool	Write your Intents Text he	Result	
	usage : fro (command) sargs) add "intent" read new intent/vules intents show intent register tatus pub solutions in the same to convolute and same to reset reset intent register usage : reports (args) show regorts summary 'tool name' show regorts from a tool		
		Deshboard Write your intents Teath Urite your intents Teath Uritege : fro comments argst Marger : fro comments argst Marger : read new intent register status and intent register status controller means : reports : drags: Marger : reports : drags: Marger : thor reports summary 'teal name'	Vertrees vertrees

Figure 114: Main page in FISHY dashboard

Document name:	D6.4 IT-2 I	FISHY final release				Page:	102 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Depending on the tools deployed for each case, in the dropdown menu we can see the different tools. In the next figure we see all the possible tools in FISHY.



Figure 115: FISHY tools in FISHY dashboard

8.1 XL-SIEM

XL-SIEM is the ATOS Security Information and Event Management system, which detects and raises alarms based on the security events generated by the system. It can be initiated from the FISHY control panel.

NO NUMBER NUMBER NUMBER	🗏 🔉 Fishy 🖉	Tools ~ 🕆 Clear	A fishy_wa ∨
Conductation Dashboard Dashboard Dashboard Dashboard Mitte your intents Test in: or created: creates usage : Incorrect creates abox intent register usage : reports sealary test in solution		o Sister Kom Ke	40 ×
Aurie	IRO Dashboard	Dashboard	
Configuration sugger : From Consequence Composition def : Televent** - read was intensited intensite status : status intensite intensite status : status : status : status unager : registres : registres unager : registres : status submer prest : from a total	INTERFACE	Write your Intents Test he Q Result	
	/ Configurations	<pre>usge::Dury:Comment() Serges add "Intent", "read and Determination intent in the interference of the intent intent intent register status public controlling "reast" controlling "reast" controlling "intent register intent intent register intent intent register intent intent register intent register "intent ender intent register "intent ender intent register intent "intent ender intent register intent intent ender intent register intent ender "intent ender intent ender intent ender "intent ender intent ender intent ender "intent ender intent ender intent ender "intent ender intent ender intent ender "intent ender intent ender intent ender "intent ender intent ender intent ender intent ender "intent ender intent ender intent</pre>	

Figure 116: Through the FISHY dashboard, we are able to select the XL-SIEM.

The main dashboard displays graphics indicators summarising the overall status of the system; the highest risk level of the events and alarms generated, the distribution of events over time, and the number of events and alarms grouped by type.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	103 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final





Figure 117: Main view [1] At first glance, we can observe a threat level based on the events and alarms generated in the recent hours and we also have a summary of the alarms and statistics generated in the last few hours.



Figure 118: Statistics on the detected attacks are provided.

Over the main view, there is a navigation bar that allows access to the different sections of the tool. After the *Dashboard*, which shows the summary status of the system (described above), there is the *Analysis* menu, where it is possible to view the details of the analysis such as the list of the events or alarms and their details.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	104 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



E > Fishy > Tools - Clear				A fishy_wa ∨
	Petiume atmos k logist atos XL-SIEM			
Alama A	Consist Thread Local	P -	Auron Torol Lood	7
	Last Security Events		Monitoring Engine: Last Alarms	2



A Fishy & Tools	✓ ☐ Clear							A fishy_v
L-SIEM								
(LSIEM	Welcome admin > Logout atos XL-SIEM						
Real Time Trend Graph by GB	▶ Configuration ▶ Reports							
Search Clear	Back 📮 Refresh 🎨			Current Search Criteria [Clear	All Criteria]		Show full of	riteria 🔝
search term	IP Signature Payload			META	PAYLOAD	IP	LAYER 4	
inter Da	fa Sturras Risk		time >= [07 /	17 / 2023] [any time]Clear	any .	any	none	
lsiem-server v	v v			Summar	Statistics			
More Filters	Taxonomy and Reputation Filters	Events 📓 🔯		Unique Events	Sensors	Uniq	e Data Sources	
ime frame selection GMT+2:00: 🚞	Timeline analysis: 😽	Unique addresses: Source Destination		Source Port TCP UDP Destination Port: TCP UDP	Taxonomy Product Types Categories	Uniqu Uniqu	e IP links (FQDII) e Country Events	
loday Last 24h Last 2 days 🖬	It Week Last 2 Weeks Last Month All						► Custo	m Views
Displaying events 1-50 of about hunde	eds matching your selection.						14,836 total eve	nts in database
	Signature	* Date GMT+2:00 *	Sensor	Source	Destinati	ion	Asset S + D	Risk
Car_started		2023-07-23 14:28:40	NA	0.0.0.0	0.0.0	i	5->5	5
Authorized_driver		2023-07-23 14:28:38	NA	0.0.0.0	0.0.0.0	1	5->5	7
Car_started		2023-07-23 14:25:48	NA	0.0.0.0	0.0.0.0	I	5->5	- 1
Authorized_driver		2023-07-23 14:25:47	NA	0.0.0.0	0.0.0	1	5->5	7
Car started		2023-07-23 14:25:32	NA	0.0.0.0	0.0.0.0		5->5	

Figure 120: Events List

Fishy P Tools V 🗅	Clear						A fishy_w
KL-SIEM							
M KL	SIEM	Welcome admin ► Logout atos XL-SIEM					
Real Time Alarma SiEM Analysis Colory Alarma SiEM Analysis Colory Alarma SiEM Events Network Traffic	juration ▶ Reports Fales						
Search Cle Intruders Datection Vulnerabilities	Back 📮 Refresh 裬			Current Search Criteria [Clear /	All Criteria]	> Show f	Il criteria 🔝
C search term	IP Signature Payload			META	PAYLOAD	IP LAYE	R 4
Sensor Data Source	n Risk		time >= [07 /	17 / 2023] [any fime]Clear	847	any non	•
xisiem-server v	v v			Summary	Statistics		
More Filters	Taxonomy and Reputation Filters	Events 🛅 🖸		Unique Events	Sensors	Unique Data Sources	
Time frame selection GMT+2:00: 🚞	Timeline analysis: 😒	Unique addresses: Source Destination		Source Port: TCP UDP Destination Port: TCP UDP	Taxonomy Product Types Categories	Unique IP links (FQDII) Unique Country Events	
Today Last 24h Last 2 days <mark>Last Week</mark>	Last 2 Weeks Last Month All					+ C	ustom Views
Displaying events 1-50 of about hundreds match	hing your selection.					14,836 total	events in database
	Signature	* Date GMT+2:00 *	Sensor	Source	Destinati	on Asset 5 + D	Risk
Car_started		2023-07-23 14:28:40	NA	0.0.0.0	0.0.0	S=>S	5
Authorized_driver		2023-07-23 14:20:38	NA	0.0.0.0	0.0.0.0	5-25	7
Car_started		2023-07-23 14:25:48	NA	0.0.0.0	0.0.0.0	5->5	5
Authorized_triver		2023-07-23 14:25:47	NA	0.0.0.0	0.0.0.0	5+>5	7
C O Orac standard		2023-07-23 14:25:32	NA	0000	0000	5-25	5

Figure 121:We use the navigation menu of the XL-SIEM to view the list of alarms.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	105 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



-SIEM						
📎 XLSIEM	Welcome admin > Lopout atos XL-SIEM					
Daviboards SIEM Analysis Configuration Player Player		Next refre	sh in 291 seconds. Or click here to refresh now			MQ.
ø View Grouped			(1-9)			Apply label to selected alarms
Signature	Events	Risk	Duration	Source	Destination	Status
			Sunday 23-Jul-2023 [Delete]			
Car started with mahware	3	9	52 secs	0.0.0.0.ANY	0.0.0.0 ANY	open
Brute force	4	1 A A A A A A A A A A A A A A A A A A A	2 days	10.13.150.9.ANY	0.0.0.0.ANY	open
Malicious URL	2	6	0 secs	10.13.150.9.ANY	0.0.0.0 ANY	open
			Friday 21-Jul-2023 [Delete]			
Malicious URL	2	4	0 seos	10.13.150.9-ANY	0.0.0.0.ANY	open
Brute force	4	8	17 mins	87.196.80.90 ANY	0.0.0.0 ANY	open
Denial of service	101	10	18 mina	87.195.80.90.ANY	0.0.0.0 ANY	open
Malicious URL	2	6	0 seos	87.195.80.90 ANY	0.0.0.0 ANY	open
Maticious URL	2	4	0 secs	87.198.80.90 ANY	0.0.0.0 ANY	open
Denial of service	101	10	20 5605	87.190.80.90 ANY	0.0.0.ANY	open

Figure 122:Alarms List

1	≡ .	ß Tools ∨	🖞 Clear					2	S fishy_wa
FISHY	& XL-SI	IEM							
RO KL-SIEM			» ····································	M	Welcome admin > Lo atos XL-SIEM	ogout I			
ACM	► Di	ashboards > SiE	EM Analysis Configuration Repo	rts					
-Com	+= M:	alicious URL	(Directive 100101)		Ð	1 6	11	X	
AE	E	ivent detail							
	1000	Event	Data Source Nar	ne	Prod	uct Type	Dat	a Source ID	^
ear			HTTP Requests W	D	Anomal	ly Detection		100101	
	1		Source Address	Source Port	Destinatio	n Address	Destination Port	Protocol	
	1 1 L	Þ	87 196 80 90 📰	0	0.0	0.0	0	TCP	
	- p		Unique Even	t ID#	Asset S +	D Priority	Reliability	Risk	
			27b711ee-a6f2-0242-ac11	-0002e4040d54	5->5	5	8	8	
			userdata1	userdata2	userdata3	userdata4	userdata5	userdata6	
		SIEM	Method: POST	Net: 87.196	Request: HTTP/1.1	Response code: 403	Size: 9666	Machine: srvpt521 wdisp	
	M.Sor		userdata7	userdata9					
			Message: /thisurlisanexploit.cgi	User: -					- 17
		Context	Event Context information not available						
			▼ Incident Response: Access	s / Acl Permit [Taxo	nomy]				

Figure 123:Alarms details

Document name:	D6.4 IT-2 I	ISHY final release				Page:	106 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



8.2 RAE

The Risk Assessment Engine (RAE) evaluates the risk of different assets based on alarms, generated by the XL-SIEM, and infrastructure information, such as the architecture or software version of the different components, to obtain a risk score for each individual asset.



Figure 124: RAE selection from the landing page

Several different mathematical models can be used to assess the risk score. In this example, there are two risk models: one for *Malware Attack* and other for *Denial of Service*.

≡ & Fishy	/ Dools - 🖞 Clear		⊖ fishy_wa ∨
& RAE			
CRAE (soane@sonae	e.demo) User Profile Legal Entities Configuration	Data Processing Activities Configuration Models Configuration Risk Report	
	Models Configuration -> Risk Model Selection	n for Data Processing Activity:processing	
	Suggested Risk Models for processing:	Malware Attack (WRP101) - (Threats: Malicious code/ software/ activity)	
	Other Risk Models: Cancel Submit	☐ Denial of service (WRP102)	
CRAE v1.3			
shy project 2023			CRAAX Lab dashboard powered by AV

Figure 125. The user can choose a risk model

Document name:	D6.4 IT-2	D6.4 IT-2 FISHY final release				Page:	107 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



From the User Profile tab, the risk evaluation can be launched (Launch Risk Assessment button).

RAE		
CRAE (soane@sona	e.demo) User Profile Legal Entities Configuration Data Processing Activities Configuration Models Configuration Risk Report	
	🏚 Launch Risk Asse	essment
	User Profile	
	Username: doctor	
	Name: Sonae	
	Last name: Web dispatcher	
	email: soane@sonae.demo	
	Legal Entity: Sonae (I Department)	
	Update user profile	
RAE v1.3		

Figure 126: Main RAE view with basic info.

Then, the tool generates a qualitative report with a summary score for each risk model and a score for each specific risk in the models.

(1012				
		Overall cyber-risk status:		
		Average value MEDIUM		
	Risk Model:	WRP101: Malware Attack	LOW	
	Risk WRP101-R1:	Malware attack with loss of Availability	VERY LOW	
	Risk WRP101-R2:	Malware attack with loss of Confidentiality	LOW	
	Risk WRP101-R3:	Malware attack with loss of Integrity	VERY LOW	
	Risk Model:	WRP102: Denial of service Attack	MEDIUM	
	Risk WRP102-R1:	Denial of service attack with loss of Availability	LOW	
	Risk WRP102-R2:	Denial of service attack with loss of Confidentiality	MEDIUM	
		Sonae Web Dispatcher (10.0.0.2)		
RAE v1.3	Risk WRP102-R3:	Denial of service attack with loss of Integrity	MEDIUM	

Figure 127. RAE qualitative risk assessment

Likewise, RAE generates an economic report with the worst and typical loss for each risk.

Document name:	D6.4 IT-2 FISHY final release					Page:	108 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final


(NAL				
		Typical Loss: 11,575.00 EUR		
		Worst Case: 47,475.00 EUR		
	Risk Model:	WRP101: Malware Attack	Typical Loss: 8,200.00 EUR 💌	
	Risk WRP101-R1:	Malware attack with loss of Availability	Typical Loss: 3,250.00 EUR 👻	
		Sonae Web Dispatcher (10.0.0.2)	Typical Loss: 3,250.00 EUR ·	
	Risk WRP101-R2:	Malware attack with loss of Confidentiality	Typical Loss: 1,700.00 EUR 🝷	
		Sonae Web Dispatcher (10.0.0.2)	Typical Loss: 1,700.00 EUR 💌	
	Risk WRP101-R3:	Malware attack with loss of Integrity	Typical Loss: 3,250.00 EUR -	
	Risk Model:	WRP102: Denial of service Attack	Typical Loss: 3,375.00 EUR 💌	
	Risk WRP102-R1:	Denial of service attack with loss of Availability	Typical Loss: 1,475.00 EUR ▼	
RAE v1.3		Sonae Web Dispatcher (10.0.0.2)	Typical Loss: 1,475.00 EUR 💌	-

Figure 128. RAE quantitative risk assessment

Document name:	D6.4 IT-2 I	FISHY final release	Page:	109 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



8.3 WAZUH

Wazuh tool allows the user to set rules and receive alarms when these are violated. An example of the Wazuh dashboard is shown in the following figure, where the detected events are shown.

😔 Elastic														۵
	even	ts												
Security events (0)														
Dashboard Events														() Explore agent
🖭 🗸 Search									KQL	l ∨ Last:	24 hours		Show dates	C Refresh
manager.name: localhost.localdomain + Add filter														
wazuh-alerts-* 🗸 🤤								226 hits						
Q Search field names						Jun 22, 2023	@ 13:51:12.698 - Ju	n 23, 2023 @ 13:51:12.6	Auto	\sim				
Filter by type O		200												
Selected fields		150												
t agent.name	ount	100												
t rule.description	0	50												
t rule.id		0												
rule.level		0	15:00	18:00	2	1:00	00:00	03:00	0	0	6:00	09:00	12:00	0
Available fields							tim	estamp per 30 minutes						
t agent.id		Time	· ·	agent.name	rule.descripti	on							rule.level	rule.id
t data.command		Jun	23. 2023 0 13:51:08.795	localhost.localdo	Synelixsis	unauthorized dev	ice. DID level.	9XFFSoI1t7ehKPARh8X	cNt. name: A	AberonIoT.	token: evJBeXA1	01JKV101LCJhbGc101JIUzI1	3	300004
t data.dstuser	l í			main	N1J9.eyJzdW	I101IweDk5MjQ1YT	kyOTAyOUQ4YjVGNki	MxMmI3ZDgwMTU4ZjcxZ	kFDMTkx0Tgif	fQ1YM8auw	-Ewq32MFSW11F5C	9651JNLIY75mcCD9Dc34		
t data.gid		Jun	23. 2023 @ 13:51:03.792	localhost.localdo	Synelixsis	unauthorized use	r. IP level. use	r from 163.23.164.1	66				3	300006
data borne				main										
data metadata attacker did	>	Jun	23, 2023 0 13:50:58.791	localhost.localdo	Synelixsis	unauthorized dev	ice, DID level.	njjls34UQxVdvxEETyM	hLD, name: A	AberonIoT,	token: eyJBeXA1	01JKV1Q1LCJhbGc101JIUzI1	3	300004
 data matadata davia, sama 				main	NiJ9.eyJzdW	I101IweDk5MjQ1YT	ky0TAy0UQ4YjVGNkI	MxMmI3ZDgwMTU4ZjcxZ	kFDMTkx0Tgi1	fQ1YM8auw	-Ewq32MFSW11F5C	9651JNLIY75mcCD9Dc34		
Gata metadata device_name	>	Jun	23, 2023 0 13:50:53.789	localhost.localdo	Synelixsis	unaüthorized dev	ice, DID level.	njjls34UQxVdvxEETyM	hLD, name: A	AberonIoT,	token: eyJ0eXA1	01JKV1Q1LCJhbGc101JIUzI1	3	300004
i casta metadata ip				main	NiJ9.eyJzdW	I101IweDk5MjQ1YT	ky0TAy0UQ4YjVGNkI	MxMmI3ZDgwMTU4ZjcxZ	kFDMTkx0Tgi1	fQ1YM8auw	-Ewq32MFSW11F5C	9651JNLIY75mcCD9Dc34		
 data.metadata.token 	>	Jun	23, 2023 0 13:50:48.792	localhost.localdo	Synelixsis	unauthorized dev	ice, DID level.	njjls34UQxVdvxEETyM	hLD, name: A	AberonIoT,	token: eyJ0eXA1	01JKV1Q1LCJhbGc101JIUzI1	3	300004
@ data.metadata.user				main	N1J9.eyJzdW	I101IweDk5MjQ1YT	KYOTAYOUQ4YjVGNki	MxMmI3ZDgwMTU4ZjcxZ	KFDMTKx0Tg11	TQ1YM8auw	-Ewq32MFSW11F5C	9651JNLIY75mcCD9Dc34		
t data.pwd t data.sca.check.command	>	Jun	23, 2023 0 13:50:43.786	localhost.localdo main	Synelixsis NiJ9.eyJzdW	unauthorized dev IiOiIweDk5MjQ1YT	ice, DID level. kyOTAyOUQ4YjVGNk	njjls34UQxVdvxEETyM MxMmI3ZDgwMTU4ZjcxZ	hLD, name: A kFDMTkx0Tgif	AberonIoT, fQ1YM8auw	token: eyJ0eXA1 -Ewq32MFSW11F5C	01JKV1Q1LCJhbGc101JIUzI1 9651JNLIY75mcCD9Dc34	3	300004
t data.sca.check.compliance.cis	,	Jun	23, 2023 0 13:50:38.784	localhost.localdo	Synelixsis	unauthorized use	r, IP level. use	r from 163.23.164.1	66				3	300006

Figure 129: Printscreen from the dashboard of Wazuh

🥪 Elastic		0 0
WAZUH ~ / Modules / Security	events	
Security events (0)		
Dashboard Events		(n) Explore agent
t data.dstuser	in Uz1N8J.9.eyJz0811011w66K9Kj01YTky0TAy0UQ4YjV0A6K9H3Z20geHTU4ZjcxZ8F0HTkx0Tg1f01YHBauw-Ewq129F0H1F50665L34L1Y75ecC09 Dc34	
t data.gid t data.home data.metadata.aftacker_did	Jun 23, 2023 @ 13:52:23.834 localbext.localdoma Synelixsis unauthorized device, DD level. mjliAHUQvdevEETyMKLD.mame: Adversion.ft token: eyJMexLiDLXVTGULCADGCIDLIT 3 UVITULA.p.ejzGMIDD11wGKM9D[17ThyOTAyOD[47]YOBARGHII2DgwHTuZ]zeZZVEHTkoTfp10IVMBuw=Exp22WEHTJP5CM51_MLTYTBeCCD9 DC14	300004
 data.metadata.device_name data.metadata.ip 	Jun 23, 2023 @ 13:52:18.426 localboxt.localdoma Synelixsis unauthorized user, IP level. user from 163.23.164.166 in	300005
data metadata token	Jun 23, 2823 0 13:52:13.824 localhost.localdoma Symelixis: Device AberonIoT has tried to log in 10 times in 2 hours in	e 30005
data metadata user data pwd	C Expanded document View surrounding doc	cuments View single document
t data.sca.check.command	Table JSCN	
data.sca.check.compliance.cis data.sca.check.compliance.cis_csc data.sca.check.compliance.cis_csc data.sca.check.compliance.attrr.fV	f sgent.1d 000 b	
t data.sca.check.compliance.gpg_13	③ data.metadata.attacker.did mjjki#uQxvdvxEETyMbLD	
t data.sca.check.compliance.hipaa t data.sca.check.compliance.	© data.metadata.device_name AberonIoT	
nist_800_53	data.metadata.token eyJ@eXX101.KVTQ1LC./hb0c101.JTU2TINLJ9.eyJzdWI101Iwe6KMJQ1YTKy0TAy0Uq4YJY00KH.Mm12ZDgwWTu4ZjcxZkFEWTkx0Tg1fQ1YMBauw-Ewq2HFBW1FS	C9651JNLIY75mcCD9Dc34
t data.sca.check.compliance.tsc	data.timestamp Jan 26, 2022 0 11:59:36.000	
(t) data.sca.check.description	r data.type 2	

Figure 130: Printscreen from the dashboard of Wazuh that detects a brute force attack

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					110 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



8.4 SACM

SACM tool allows the user to set rules and receive alarms when these are violated. An example of the SACM dashboard from the IRO is shown in the following figure, where the detected events are shown (and also whether these have been registered and verified by the blockchain is indicated).

FISHY						B fishy, fa
IRO Dashboard	Detailed Reports					
	DataTables containing all information received fro	m monitoring tools				
	DataTable					
	Show 10 • entries					Search:
	ID é	Description	Full Text		Smart Contracts Verification	
	0d05c337-17a3-4ce9-ab90-c0a83b0d8fa0	Source: SACM	pilot: F2F Sender: AuditingComponent	Sender	Outcome	Verified
			upateg_at:2023-06-30101021212.507762 Description: AssessmentResultD:27 Receiver:AuditIngModule Severity:75 AssessmentExecutionD:79 AssetD:11 Source:EventCollectionEngine Event:27Etype 1 attack: WalletID Action:('Action.type': bha.uid', '%id': '0x10078a9f2dfe8665007038b9682f0b7Be6050f')	AuditingComponent	Satisfaction	
	1a8fc697-3105-4036-94aa-67534f9315a9	Source: SACM	pilot: F2F Sender: AuditingComponent undated at: 2023.03.30110-02:32 9077762	Sender	Outcome	Pending
			Description: Outcome: Satiafaction Arguments: [*] AssessmentResultID: 24 Receiver: AuditIngModule Severity: 75 AssestmetExecutionID: 79 AssetID: 11 Source: EventCollectionEngine Event: 525 type 1 attack: WalletID Action: (*action_type': 'ban_wid', 'wid': "aci3067Bam972Arede60007038b962f067BedD566f')	AuditingComponent	Satisfaction	

Figure 131: Printscreen from the dashboard of SACM that detects the wallet ID attack

	=					A admin	E Locout
Tuchnology	-					2 evinin	-D color
J 2) Solutions	Home / Project: SONAE /	Create Asset 1/3: Choose Asset Type / Create Asset 2/3: Hardware Asset Parameters					
Home	Version*	1					
Organisations	Category*	network	~	Status*	final		~
Projects	Value	0	\$	Currency	EUR		~
Assessment Profiles	Description						
Assessment Criteria	Description						. A.
	Components						
Create User	Component Type*	Network			× .		
	MAC*	00.d0.c9.e3.6d.f5		Connection Type*	Integrated		~
	IP _V 4*	192.168.178.10		Gateway*			
	IPv6						

Figure 132: Printscreen from the dashboard of SACM on configurating new assets to monitor

Document name:	D6.4 IT-2 I	FISHY final release	Page:	111 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



M STATUS	=				& admin	Logout
Solutions	Home / Assessment Crite	ria / View Assessment Criterion				
Home						
Organisations	Assessment Crit	terion Parameters				
Projects	Name*	IOT Telemetry threshold	Assessment Model Type*	Monitoring Assessment		¥
Assessment Profiles	Tags		Language*	DRL		*
Assessment Criteria		rule 'Rule\$CRITERION_ID_Satisfaction'				1
End-Users	1.000	when Huppens [_e1: e, "call" == e.type , "traffic" == e.args[0] , "	iot_instance" : e.args[1], _,threshold : e.args[23], t1 : t. src:	e.source)		
Create User	Specification*	eval(onp.compare_threshold, 80') = true) 12 : Fluent (name = = "SatisfactionFluent_RSCRITERION_D	D*)			
		not instates, $e = - (e_1, t = t_2, t = t_1)$ then				
		Predicate predicate = new Predicate(): predicate.addEvent(.e1);				
						4

Figure 133: Printscreen from the dashboard of SACM on configurating new rules to monitor the assets

Document name:	D6.4 IT-2 I	D6.4 IT-2 FISHY final release					112 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



8.5 VAT

VAT functionality is used to check the vulnerability of nodes hosting the supply chain platforms. To do so, we first configure VAT tool of the FISHY platform providing the IP address of the node as has been done in the F2F case and is shown Figure 134.

📮 🌲 беланд 🗸
NI CONFIGURATION > NEW SCAN
SELECT SCAN TYPE
SELECT CONFRC SUITE TYPE
BASIC TARGET CONFIGURATION TARGET*
TASK DETALS
RUN OPTIONS
SCAN SUMMARY
Back Next
SC/ 1 2 3 4 5 6

Figure 134: Configuration of VAT to scan a specific platform

Once the scan has been executed, a screen appears indicating the level of the detected risk vulnerability and providing information on ways to mitigate it, as shown in the Figure 135.

SCAN SCAN Download JSON	PORT			×	Lo OBMUT ~
	 Vulnerability 	0	Scanner		
Medium (75)	Click-Jacking vulnerability		W3af	^	
desc solution	The application has no protect Clickjacking (User Interface re Web user into clicking on som revealing confidential informat pages. The server didn't retur clickjacking attack. The 'X-Fra browser should be allowed to attacks, by ensuring that their	ion against Click-Jacking attacks. dress attack, UI redressing is a using different from what the user perceives they on or taking control of their computer while click an "X-Frame-Options" header which means that me-Options "HTTP response header can be used ender a page inside a frame or iframe. Sites can content is not embedded into other sites.	a malicious technique of tric v are clicking on, thus potent ng on seemingly innocuous t this website could be at risk t to indicate whether or not at use this to avoid clickjacking	king a ially web k of a a g	
-		*		Close	
STATUS	ione -	COUNT	1		
STARTED 23.	96.2023 13:45:19	INTERVAL	1		
FINISHED 23.	06.2023 13:47:33	START AFTER	1		
LAST RUN 23.	06.2023 13:47:33	UPDATED	1		
NEXT DUN /					

Figure 135: Results of the VAT scan of the F2F platform

VAT is also used to monitor the availability of all the nodes comprising the supply chain platform as shown in the Figure 136 below:

Document name:	D6.4 IT-2 I	FISHY final release				Page:	113 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Starteu	Finished	Result		Output uris
13.06.2023 16:22:	4 13.06.2023 16:22:33	Report		container_output_1686662552146.txt cscan-log.txt genscan-out.json
13.06.2023 16:19:	4 13:06:2023 16:19:56	Report		container_output_1686662394373.txt cscan-log.txt genscan-out.json
12.06.2023 17:12	7 12.06.2023 17:13:49	Report		container_output_1686579228491.txt cscan-log.txt genscan-out.json
× 1 ×				
< 1 > RUN DETAILS	50HF			1
c 1 > RUN DETAILS	5041 13.06.2023 16:22:14		COUNT	1
x 1 , RUN DETAILS STATUS STARTED EINISJEED	13.06 2023 16:22:14 13.06 2023 16:22:14		COUNT	1 / /
< 1 > RUN DETAILS STATUS STARTED FINISHED LAST RUN	13.06.2023 16:22:14 13.06.2023 16:22:33 13.06.2023 16:22:33		COUNT INTERVAL START AFTER UPDATED	

Figure 136: VAT monitors the availability of nodes

Document name:	D6.4 IT-2 I	FISHY final release				Page:	114 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



8.6 PMEM

PMEM tool can be used to provide the protection against different attacks, such as the DDOS attack at the endpoints. The PMEM front end shows three different screen/views. First of all, it keeps tracks of the real time traffic of the last 24 hours traffic to provide an analysis and a better overview to detect the anomalies (Figure 137 left part). Also it gives the distribution of the protocols present in the last scan (see Figure 138 right part), the third screen provides a summary of the events detected in the last 24 hours (Figure 138). Finally, the tool also allows to see the last scan as well as all the previous scans results (Figure 139), to reach this screen user must click on the Reports Tab. These reports can also be downloaded in form of CSV, Excel or PDF files.



Figure 137: PMEM front end showing different status



Figure 138: PMEM showing events detected in the last 24 hours.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	115 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



	XX PMEM											
	di tracta											
		Showin	to to 1 g	Pentries								
.M							History of	All Scan Results				
ZUH		CSV	Excel	POF							Search	
		1.1	Pilot	Timestamp	Source.IP	Destination.IP	Protocol	Frequency	Predictions	Description	Traffic.Share	Severity
		1	126	26/07/2023 01:45:06	8.6.0.1	8.0.6.4	0	1	Denign	Benign Traffic is detected	0.0208333333	Low
M		2	125	26/07/2023 01:45:06	193.145.14.195	192.168.190.240	17	1	Denign	Benign Traffic is detected	0.0208333333	Low
or .		3	#2F	26/07/2023 01:45:06	192.168.190.240	8444	17	40	Denign	Benign Traffic is detected	0.833333333333	High
		40	F2F	26/07/2023 01:45:06	192.168.190.240	192.168.169.189	- 28	1	Benigs	Benign Traffic is detected	0.0208333333	Low
		5	F2F	26/07/2023 01:45:06	192.168.190.145	192.168.190.240	- 56	1.1	Benigs	Benign Traffic is detected	0.0208333333	Low
		6	F2F	26/07/2023 01:45:06	192,568,190,20	192.168.190.240		1	Benigs	Benign Traffic is detected	0.0208333333	Low
		7.1	F2F	26/07/2023 01:45:06	83.235.169.221	192.168.190.240	6	3	Denign	Benign Traffic is detected	0.0625000000	Low
			121	26/07/2023 01:55:13	0.8.0.0	245.129.128.0	<u>_</u> 0	1	Betign	Benign Traffic is detected	0.0001488982	Low
		9	125	26/07/2023 01:55:13	8.6.0.1	8.0.6.4	0	1	Benign	Benign Traffic is detected	0.0001488982	Low
		10	F2F	26/07/2023 01:55:13	193.145.14.196	192.168.190.240	17	ī	Benigs	Benign Traffic is detected	0.0001488982	Low
				Se.007/3039-01-68-1.8	1973.168.196.344		19	34	and the second	Bankes Treffic is detected		1.000
		Stewin	g 1 to 16 c	f 16 entries								
		9 10 -11 Showin	F2F F2F E1E g1 to 16 o	26/07/2023 01:55:13 26/07/2023 01:55:13 36/07/2023 01:55:13 36/07/2023 01:65:13 125 embles	86.0.1 193.145.14.196 193.168.186.366	8.0.6.4 192.168.190.240 4.4.4.4	0	I I M	Benign Benign Boolee	Benign Traffic is detected Benign Traffic is detected Resides Traffic is detected	0.0001489982 0.0001488982 0.0001488982	

Figure 139: PMEM showing different scan results reports.

8.7 IRO

When a user access to the FISHY Dashboard in the FRF with credential of any pilot user, a personalized IRO Dashboard appears in the first place, where a user is able to create new intents to configure how to react to certain attacks or alerts. On the left side of the IRO, the user can check the different alerts received from different heterogeneous tools.

IRO X.SLOM ACCOMPTING A IND Dushbard Configurations Confi	RO XLSUM SACM RC RC RC RC RC RC RC RC RC RC	E A Fishy Prools	Clear	පු fishy_wa
SACM RE Dashboard O Doubhoard Dashboard Vitro Doubhoard Vitro compando family service to the last of the company status sub or later register status pub sub controller reset reset later register status pub sub register stat	SACM Ref SACM Ref INDUMANT Dashboard INDUMANT INDUMANT INDU	O XL-SIEM		
Robadad Robadad Robadad Dashboard Configuration Configurati	Configuration C	SACM		0
Mars Configurations Configurations Usage : fro command> darges add "intent": read where figurations status show reports summary "tool name" show reports from a tool Result Result	Mars Conformations Conformations <td>IRO Dashboard</td> <td>Dashboard</td> <td></td>	IRO Dashboard	Dashboard	
Configurations Usage : from commands carges U	Configurations Usage:::fro:ccomand::dergs3 add "Intent":::read:rea:Intent:/rules Intents::::read:rea:Intent:/rules Intent::::read:rea:Intent::register: reaet::::reaet::::read:rea:Intent:register: usage:::reports::caregs3:	TERFACE	Write your Intents Text he	esult
		f Configurations 3	usage : fro <command/> <args> add "intent" read new intents/rules intents show the list of intents status show intent register tatus push solve conflict and send to controller reset reset intent register usage : reports <args></args></args>	
		34 136-31001/main html?cossion		

Figure 140: IRO in the main FISHY Dashboard

Document name:	D6.4 IT-2	FISHY final release				Page:	116 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



IRO shows all the important alerts received from different tools, and assure their integrity by verifying the received information with the help of Smart Contracts. In the following figure, an example of a report from SACM is received and verified with Smart Contracts.

FISHY						AB fuby, fa 💈
IPO Distriction (INDAcc) Alerts Configurations (Detailed Reports DataTables containing all information record DataTable Strow 10 • entries	ived from monitoring tool	ς.			Search:
	ID	+ Description	Full Text	Additional info		Smart Contracts Verification
	0d05c337-17a3-4ce9-ab90-c8a83b0	d8fa8 Source: SACM	pilot: F2F Sender: AuditingComponent	Sender	Outcome	Verified
			updated_at: 2823-08-00710:02:32.0077762 Description Outcome: Satisfaction Arguments: ['1] AssessmentResultID: 27 Receiver: AuditInpdoUule Severity: 75 AssetsmettResultIon1D: 79 AssetSentExecution1D: 79 AssetSentExecution1D: 79 AssetSentExecution1D: 79 AssetD: 11 Source: EventCollectionEngine Event: F2F type 1 attack: WalletID Action: ("action.type': "basyf24res065007038bbe82fbb7Be0050f")	AuditingComponent	Satisfaction	
	1a8fc697-3105-4036-94aa-67534f5	315a9 Source: SACM	pilot: F2F Sender: AuditingComponent	Sender	Outcome	Pending
			upateg_at: 2023-03-00710:02:32.9677762 Obecription Outcome: Satisfaction Arguments: ['1] AssessmentEsoultID: 24 Receiver: AuditingNdoUule Severity: 75 AssessmentExecutionID: 79 AssetID: 11 Source: EventCollectionEngine Event: F2F type 1 attack: WalletID Action: ('action_type' 'backsdop7038bbed0566f') 'buid': '0x310678a99f24fe8665007038bbed0566f')	AuditingComponent	Satisfaction	
	2ad4b562+ee5b+429b+a415+b26231	df0e1 Source: SACM	nilot: E2E	2		Condinat

Figure 141:List of alerts on the dashboard from different tools (e.g.SACM detects wallet ID attack)

The IRO Dashboard also integrates a frontend for interfacing with the EDC Remediation Module. This can be done by selecting the EDC from the dropdown list, which is shown after clicking on the "Components" button on the navigation bar on the left side of the dashboard.

The EDC will respond to incoming new Threat Intelligence Reports. As soon as a new report associated with a detected attack or suspicious behavior is received from the EDC, it will present a set of proposed remediations. Final users or administrators with the required levels of authorization can then visualize these proposals through the EDC interface, which is accessed through the IRO GUI.

The EDC interface, as shown in Figure 142, presents a view with the list of remediations proposed by the EDC when a new report has been received. Otherwise, it will simply state that no remediation proposals are available. Each remediation element on the list presents two buttons. The first is used to "Accept" the given remediation, meaning that the remediation will be applied to the operational environment. This is done by leveraging the Central Repository asynchronous message broker (based on RabbitMQ) for intercommunication between the different components, regardless of where they are located. The "Details" button, instead, it will open a drop-down window with a high-level description of that remediation.

This interface keeps track of incoming remediation proposals and can be refreshed by simply clicking on the title at the top of the interface.

Document name:	D6.4 IT-2 I	FISHY final release				Page:	117 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



FISHY FISHY	. I fishy_wa
n IRO Dashboard	FDC - Proposed remediations
Configurations	Block malicious user (recommended) Accept Remediation Details
	This remediation strategy, starting from the information provided by the Threat Reports that characterize the Malicious User, configures all the proper security controls to prevent the Malicious User from reaching the target of the starts. For instance, if the user is characterized by his Paddress address, the filtering devices in the path from the Malicious User to the victim will be updated adding rules to deny the traffic. If the Malicious User is dentified by its application-level data, like a username or a WalletD,
	the security controls able to prevent the user from performing operations are configured. Moreover, this strategy also filters MAC addresses whenever they are available. Filter ip and port on impacted node Accept Remediation Details
	Put impacted nodes into reconfiguration net Accept Remediation Details

Figure 142: EDC recommendation on the IRO dashboard

8.8 Trust Monitor

The Trust Monitor component allows to verify the integrity of the entity that constitutes the infrastructure. It permits to be integrated with several Remote Attestation frameworks and technologies, abstracting them and the objects managed.

This purpose of this tool is producing periodic reports about the trustworthiness of the entities involved in the Remote Attestation process. The Trust Monitor can interact with the underneath Remote Attestation frameworks gathering information about the status of the entities and aggregating them into a report, which can be consumed by every tool that needs to know about the trustworthiness of the infrastructure.

Figure 143 is shown the main page of the web graphical interface and how entities are represented. From this interface is possible to start a Remote Attestation process on a specific entity or on a set of entities, and it will be possible to see if an attestation process is running on a specific object.

The fields reported are:

- Entity UUID: This is the primary key of the table and it is an internal identifier for the single object to attest. It is assigned by the outside at the moment of the registration of the entity and it will be used for all the operations exposed by the TM on entities;
- Infrastructure ID: This attribute allows to identify the infrastructure to which the entity belongs;
- Attestation tech: This attribute is a list of attestation technologies that will be used to verify the integrity of the specific entity. This permits to be able to use more than one attestation technology for each object;
- Name: This field represents the name of the object. It is assigned at the moment of registration and it has no impact on the logic of the TM, but it can be useful for quicker identification of entities;

Document name:	D6.4 IT-2 I	FISHY final release				Page:	118 of 120
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



- External ID: It is an identifier of the entity external to the TM. It is assigned at registration time by the outside and it permits to define an identifier that can be used for example by an attestation technology;
- Type: This attribute represents the type of the entity, such as node, VM, container, etc;
- Whitelist UUID: This value is an external reference to the whitelist database, in order to link an entity to a whitelist, which will be used during the attestation process;
- Child: This attribute is a list of entity_uuid values, which permits to know the objects contained in another one. For example, a physical node can have a list of containers running on it;
- Parent: This value has the opposite meaning of the previous one. In this case, it represents the entity_uuid of the entity that contains the represented object;
- State: This value represents the state of the entity in the TM in order to be able to understand which process is running related to the specific entity. Here is also present a button which permits to start or stop the attestation process on that specific entity;
- Metadata: This is an important field because it represents in some way the flexibility of the TM. Inside this field can be stored custom information, that the TM interprets as a blob, so this data is not relevant for the primary logic of the TM, but they can be used by attestation technologies, which could need some additional information to properly work;
- Actions: This field provides some action on the entity like modifying it or deleting it.

🞸 Trust M	Ionitor GUI										
Entities											
Verifiers	1										
Whitelist	ts										
Status											
			En	tities							
Entity UUID	Infrastructure ID	Attestation tech	Name	External ID	Туре	Whitelist UUID	Child	Parent	State	Metatdata	Actions
1	1	keylime_v6_3_2	attester	90e71d86-13e0-4bd3- 9ec4-1521f10a5194	node	1	2,3,4,5,6,7		registered	Show	/#
2	1	keylime_v6_3_2	local	9be621ca-7746-4217- 8a28-eab90077ac33	pod	2		1	registered	Show	2 8
3	1	keylime_v6_3_2	coredns	16d0eaea-a9d8-4998- bf22-475799067645	pod	3		1	registered	Show	×#
4	1	keylime_v6_3_2	metrics	a94e4991-a53f-4952- 87ee-6a2b0269e3bf	pod	4		1	registered	Show	/1

Figure 143: Trust Monitor listing the monitored nodes

Figure 144 instead shows the actual status of the entities which a Remote Attestation is running on

Document name:	D6.4 IT-2 I	FISHY final release	Page:	119 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final



Trust Mon	nitor GUI				
Entities					
Verifiers					
Whitelists					
Status					
			Status		
Loaded	Adapters				
Loaded A	Adapters				
Loaded A keylime	Adapters _v6_3_2 tion processes				
Attesta Loaded A keylime	Adapters _v6_3_2 tion processes Attestation tech	Name	External ID	Trust	Action
Attesta 20	Adapters _v6_3_2 tion processes Attestation tech keylime_v6_3_2	Name test_node_1	External ID	Trust	Action
Attesta Entity 20	Adapters _v6_3_2 tion processes Attestation tech keylime_v6_3_2	Name test_node_1	External ID	Trust True	Action
Attesta Entity UUID 20	Adapters _v6_3_2 tion processes Attestation tech keylime_v6_3_2	Name test_node_1	External ID	Trust	Action
Loaded / keylime Attesta Entity UUID 20	Adapters _v6_3_2 tion processes Attestation tech keylime_v6_3_2	Name test_node_1	External ID	Trust True	Action

Figure 144: Trust Monitor during a Remote Attestation execution

Document name:	D6.4 IT-2 I	FISHY final release	Page:	120 of 120			
Reference:	D6.4	Dissemination:	PU	Version:	1.0	Status:	Final