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.

(*) 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

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

Table of Contents

List of Tables

List of Figures

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	*Pods* 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

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.

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

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

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

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.

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.

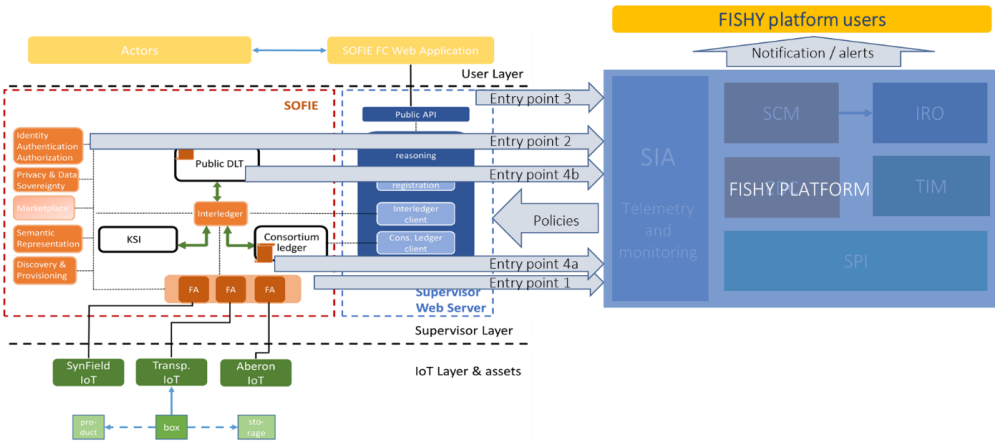


Figure 2: The F2F platform and its interconnection with the FISHY platform

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 **attack modelling according to the ENISA model** 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

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.

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

	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)

With respect to the MITRE ATT&CK framework [9], 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

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.

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

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)

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.

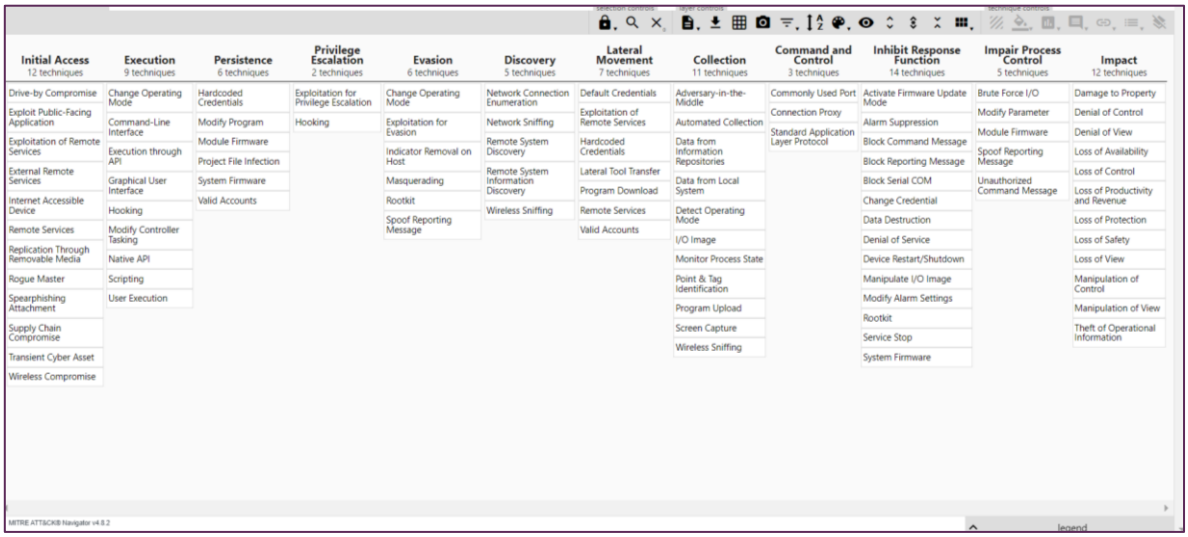


Figure 3: Overview of the MITRE ATT&CK navigator

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.

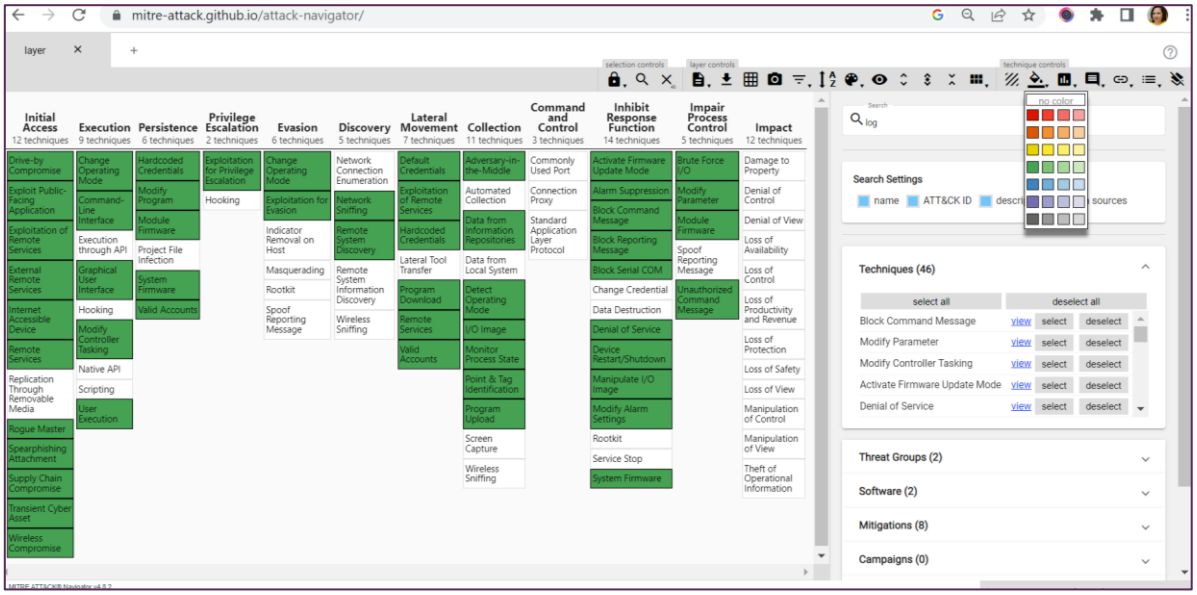


Figure 4: The attacks that can be detected based on logs shown/highlighted in green

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.

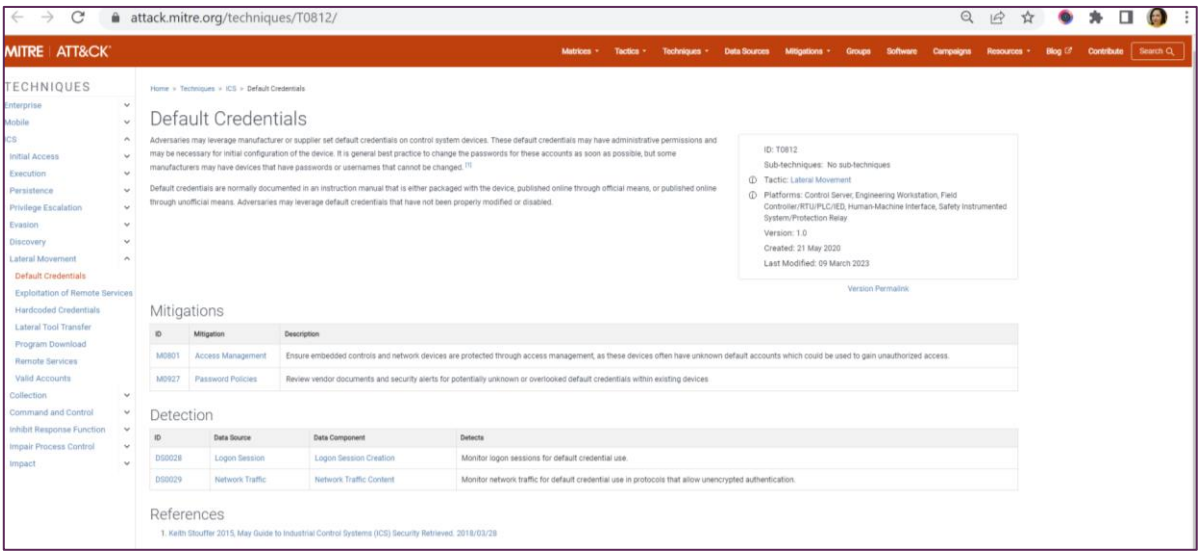


Figure 5: The ATT&CK information provided of the “default credentials” threat

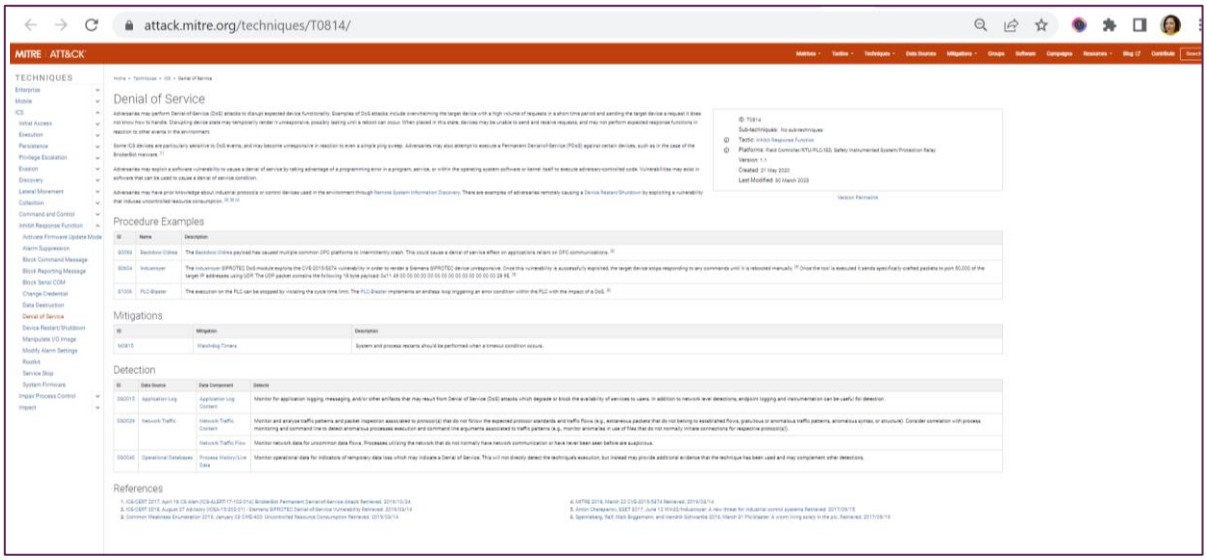


Figure 6: The ATT&CK information provided of the "Denial of Service" threat

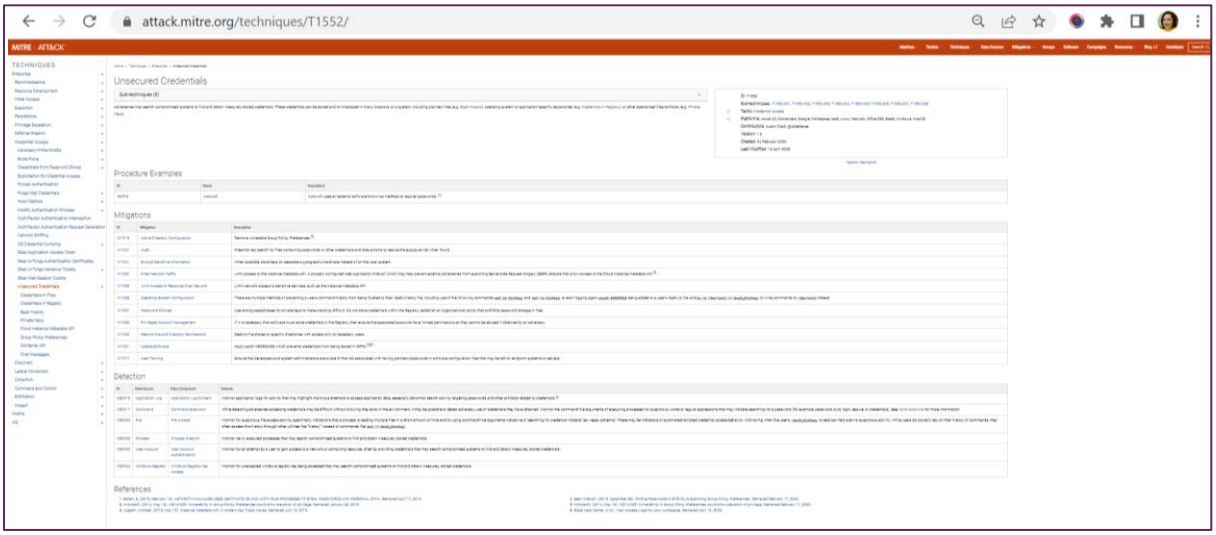


Figure 7: The ATT&CK information provided of the "Unsecured credentials" threat

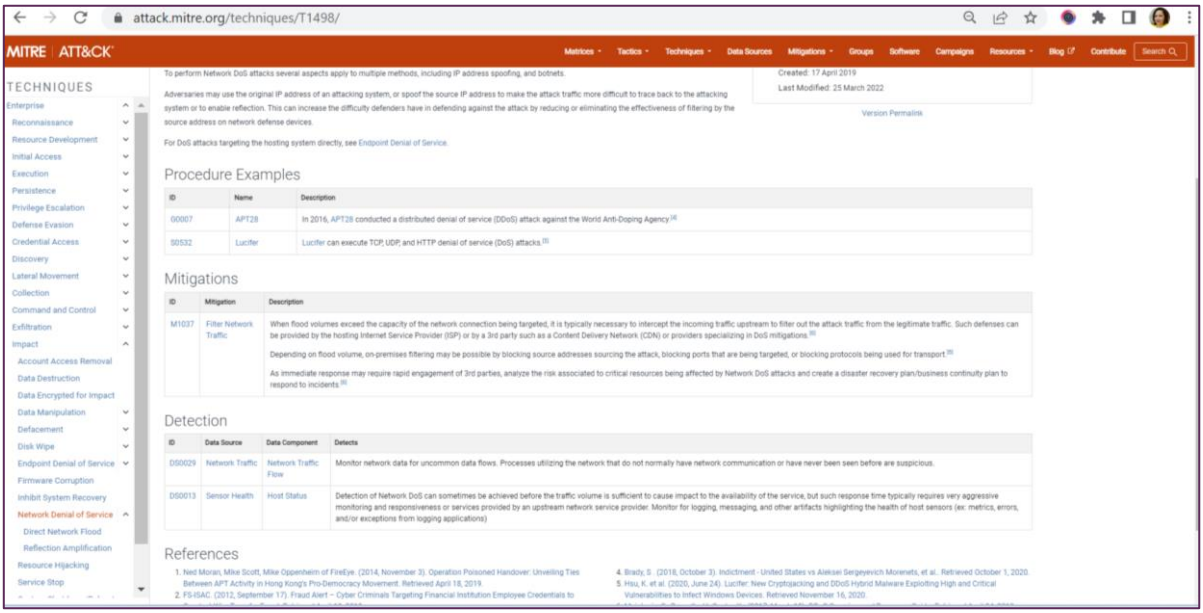


Figure 8: The ATT&CK information provided of the "Network Denial of Service" threat

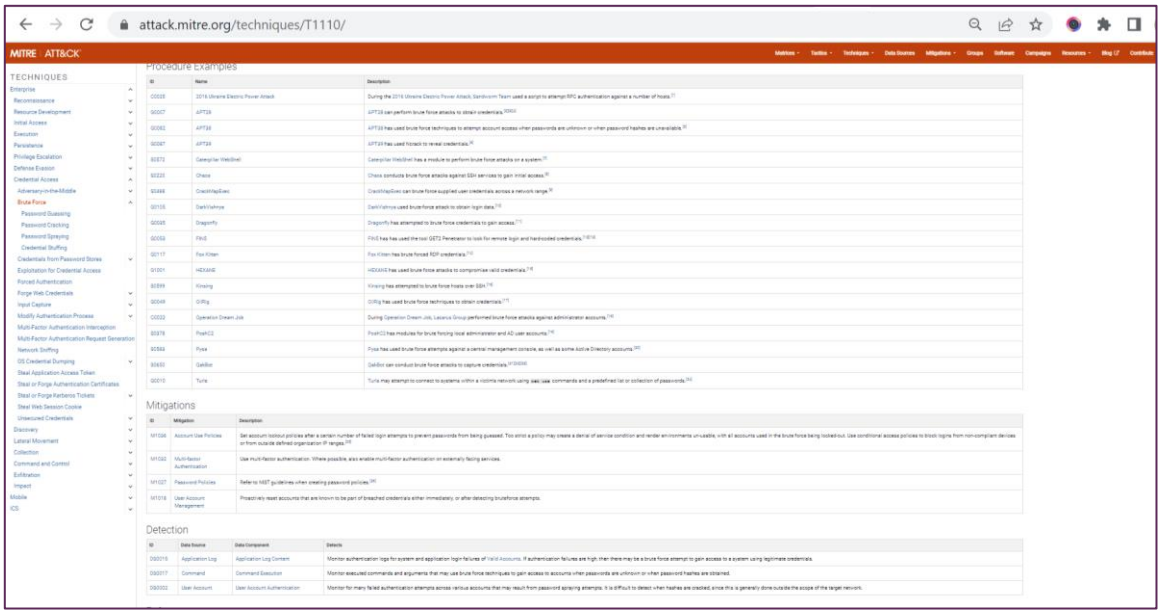


Figure 9: The ATT&CK information provided of the "Brute force" attack

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:

Table 3: Success probability assessment for potential attacks

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)

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).

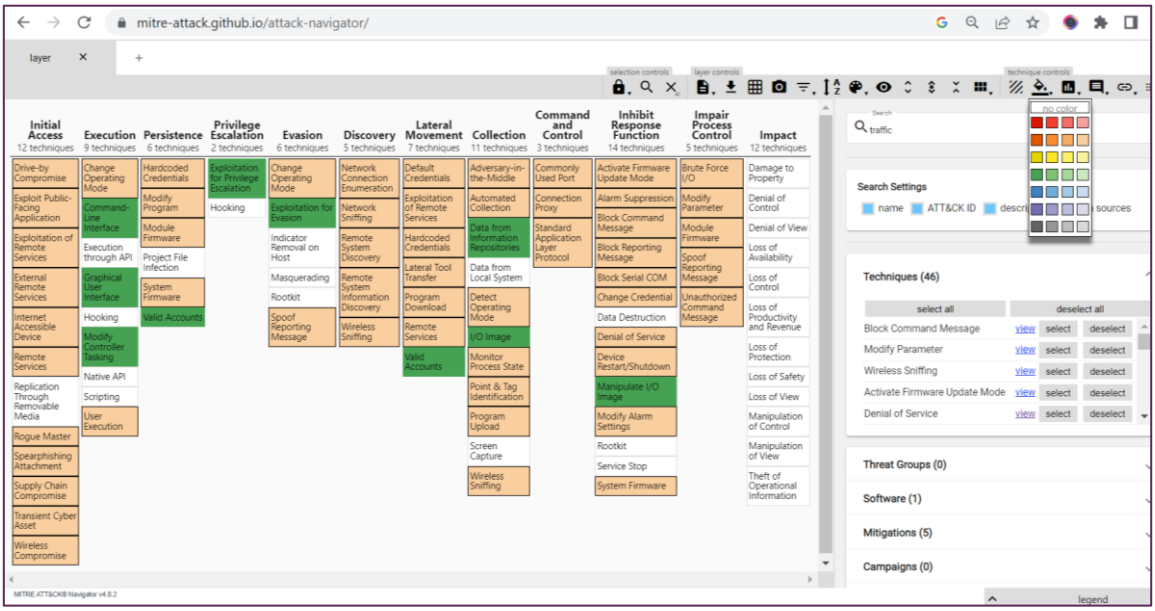


Figure 10: The threats that can be detected based on logs and traffic analysis information are coloured (65 out of 80, i.e. 81%)

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).

Figure 11: The "sequels" of demonstration of the FISHY operation in the Farm to Fork use case

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.

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.

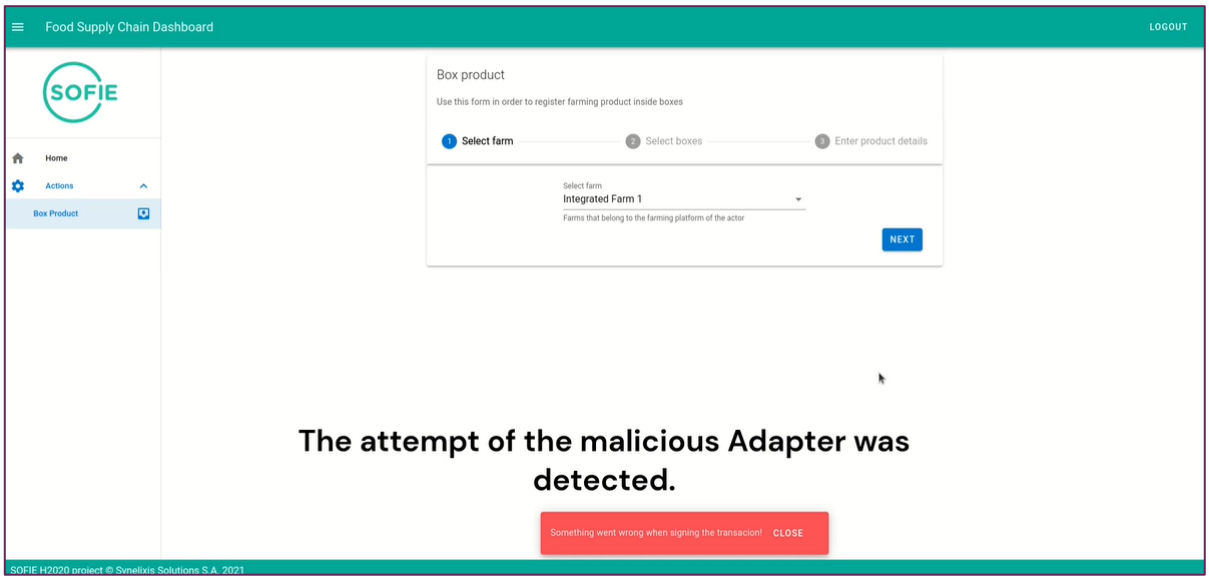


Figure 12: Malicious farmer attempts to register fake information through a device (with unauthorised wallet ID)

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.

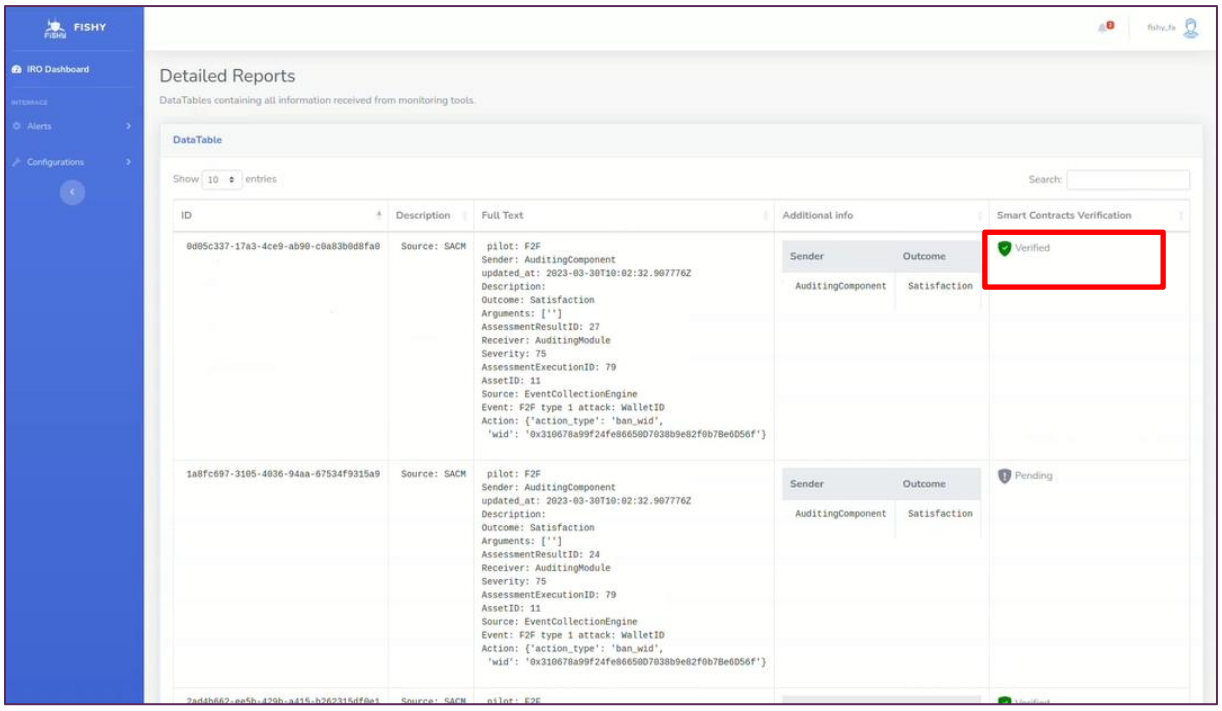


Figure 13: Screenshot from the dashboard of SACM that detects the wallet ID attack

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

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.

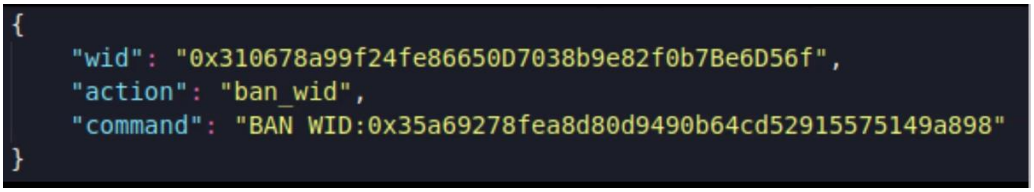


Figure 14: Screenshot from the FISHY platform capturing the defined policy.

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.

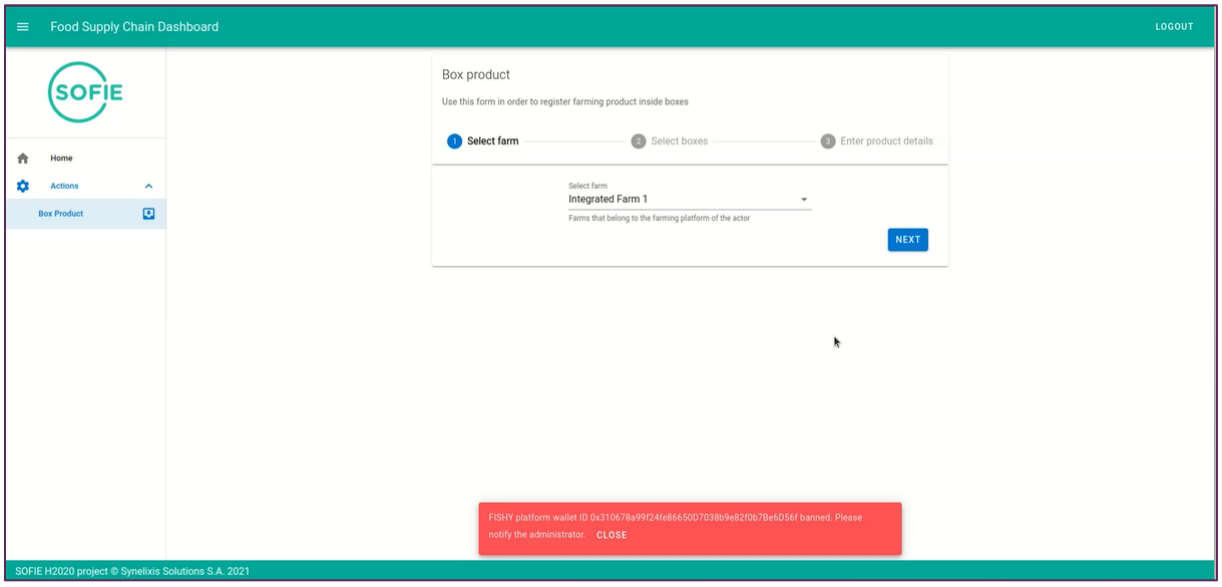


Figure 15: Screenshot from the F2F platform where the inability of the malicious user to enter information is shown.

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.

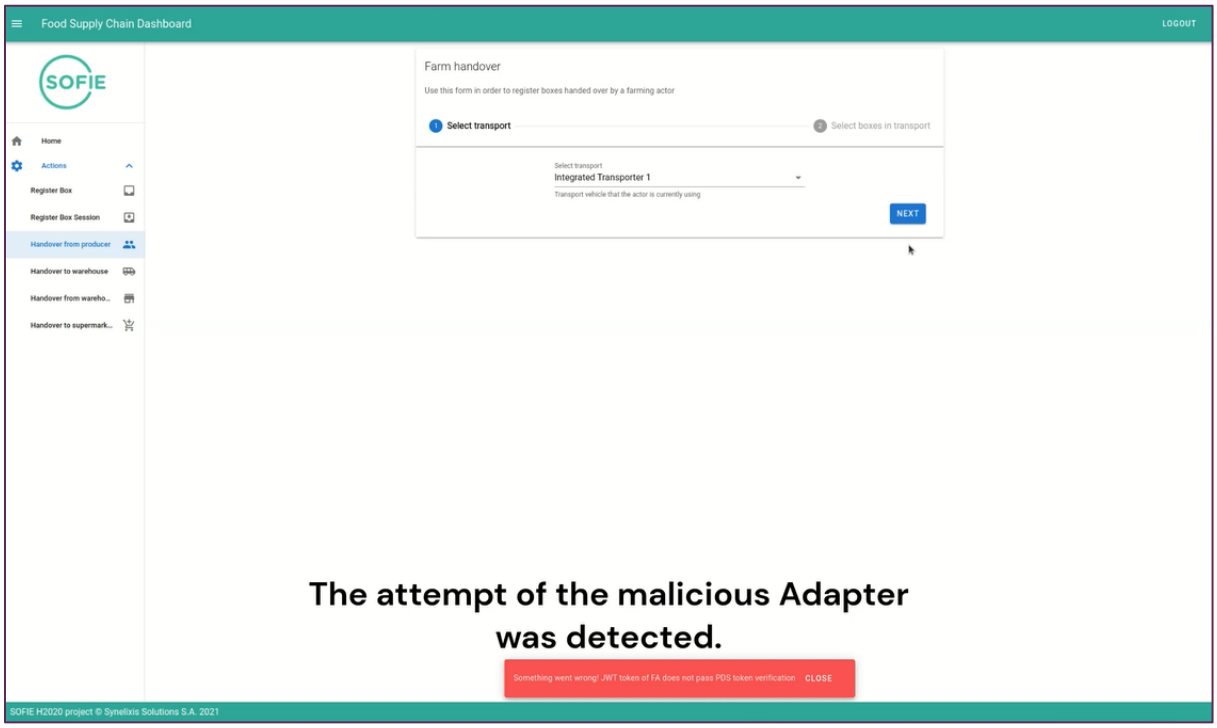


Figure 16: The adversary (transporter) attempts to register fake information through a device (with Distributed Identified that has not been assigned by the F2F platform)

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.

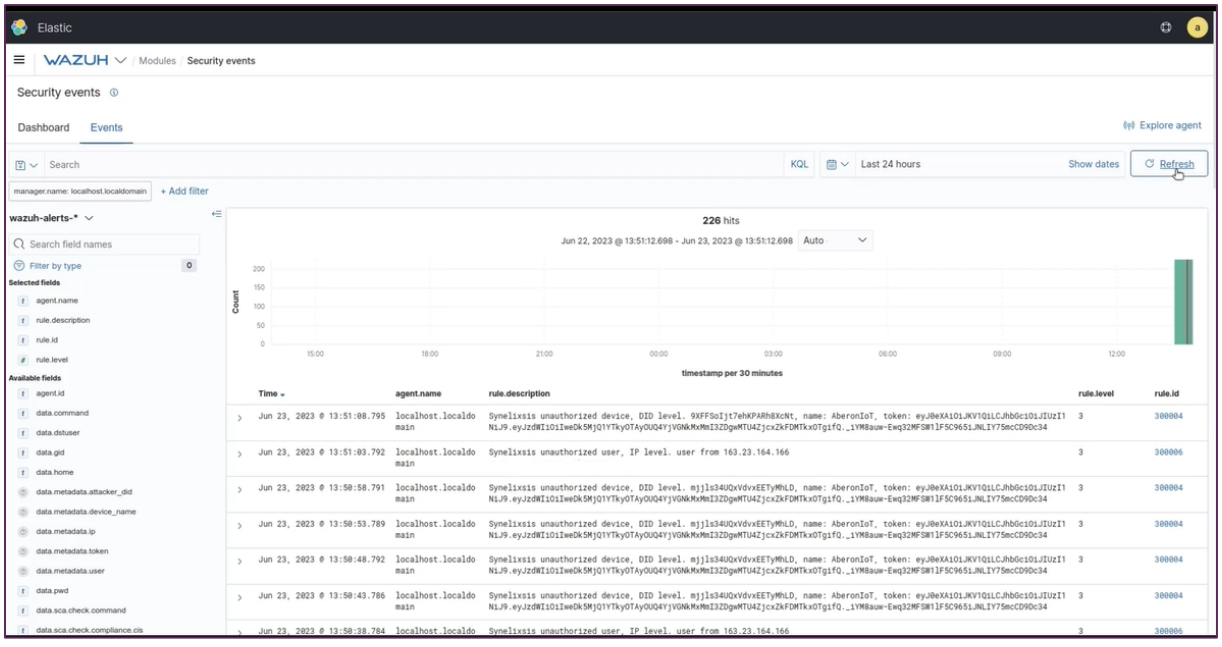


Figure 17: Screenshot from the dashboard of Wazuh that detects the DID attack

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 18.

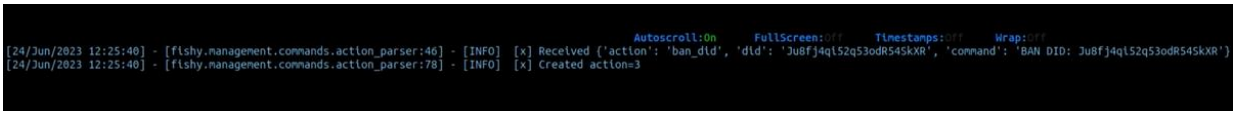


Figure 18: Screenshot from FISHY where the defined policy to protect against the DID attack is presented.

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

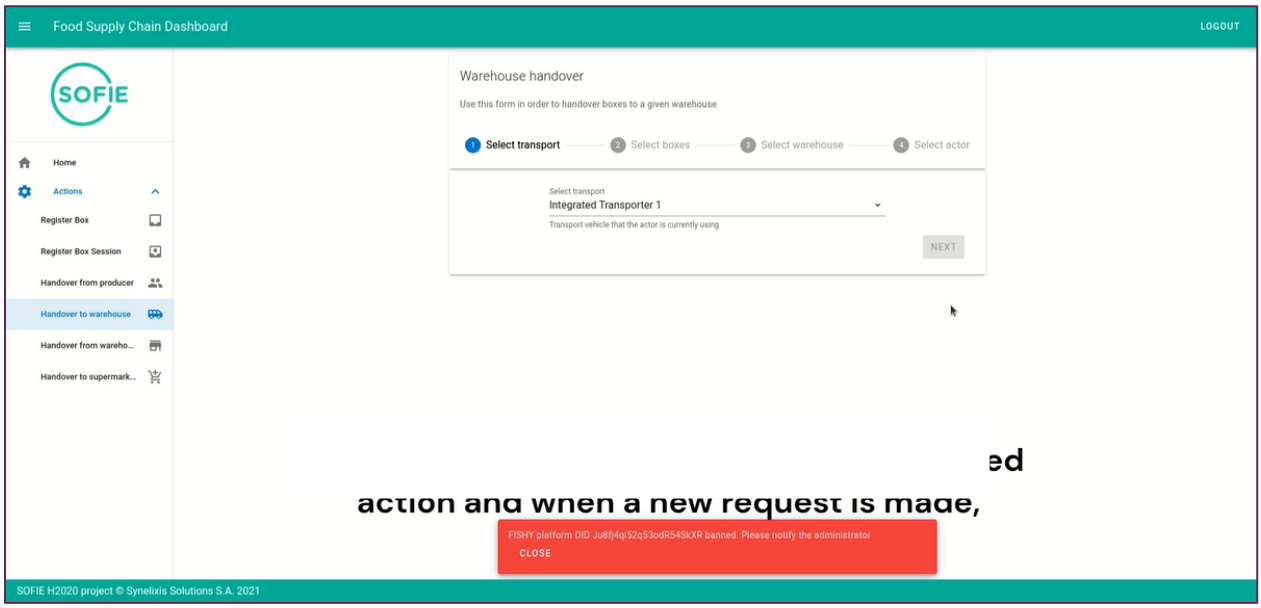


Figure 19: Screenshot from the F2F platform where the inability of the malicious user to enter information is shown

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.

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.

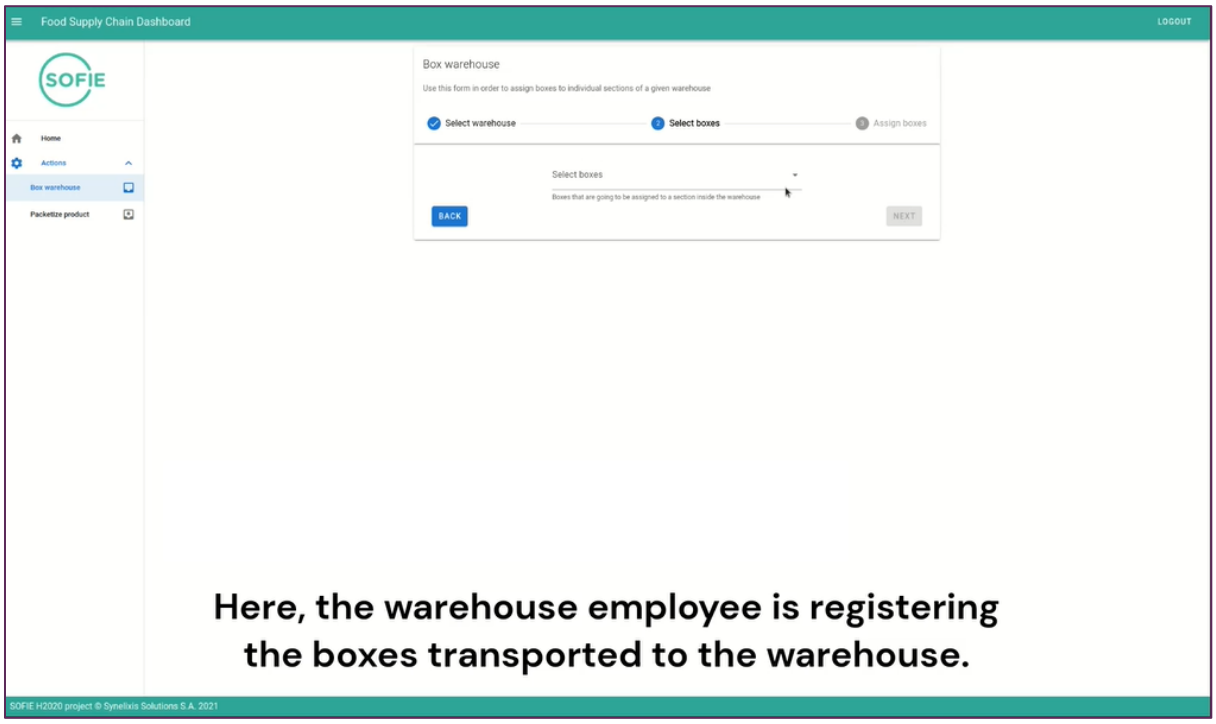


Figure 20: Malicious warehouse operator attempts to register fake information through a device (with unauthorised wallet ID)

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.

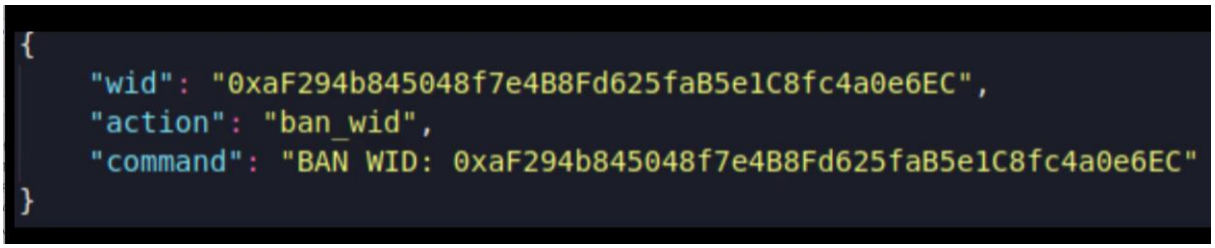


Figure 21: Screenshot from the dashboard of FISHY where the defined policy is presented.

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

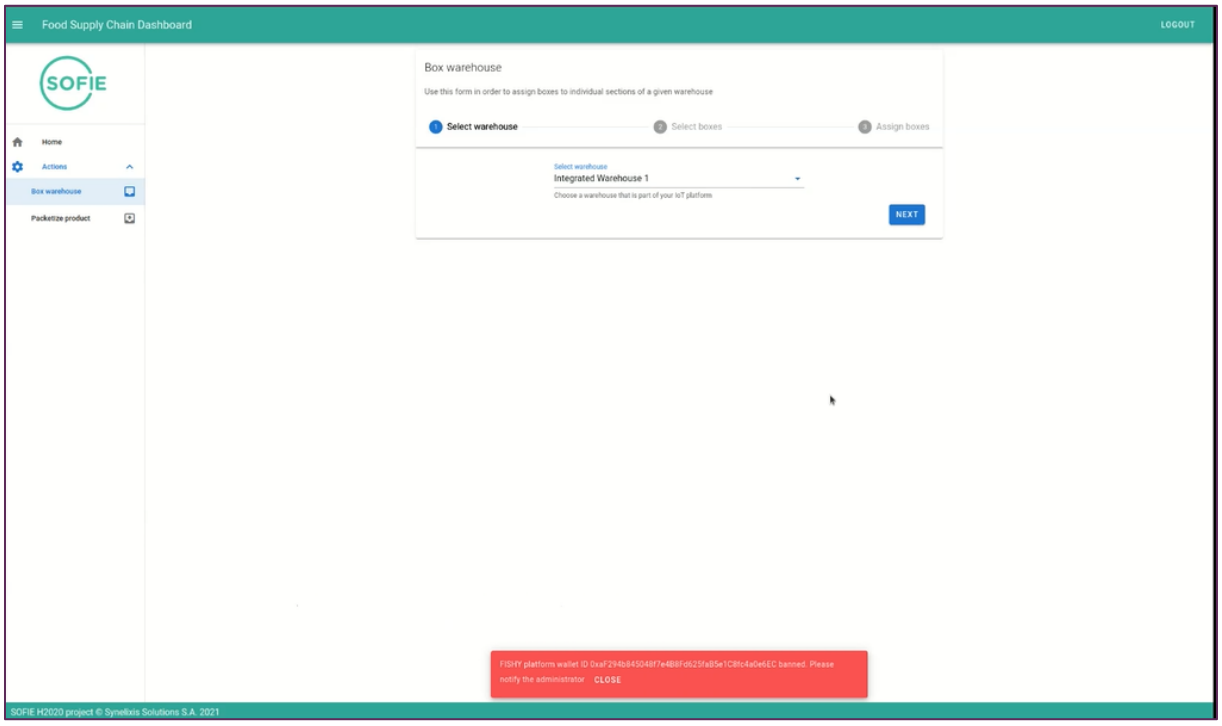


Figure 22: Print screen from the F2F platform where the inability of the malicious user (Chris) to enter information is shown

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.

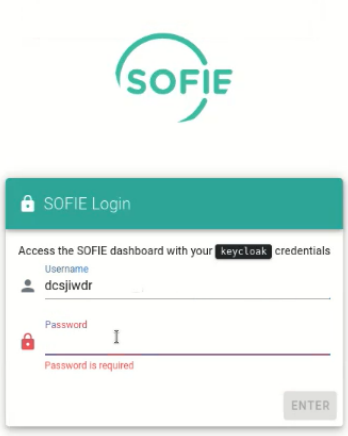


Figure 23: Malicious consumer attempts to register fake information compromising a user account (brute force attack)

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.

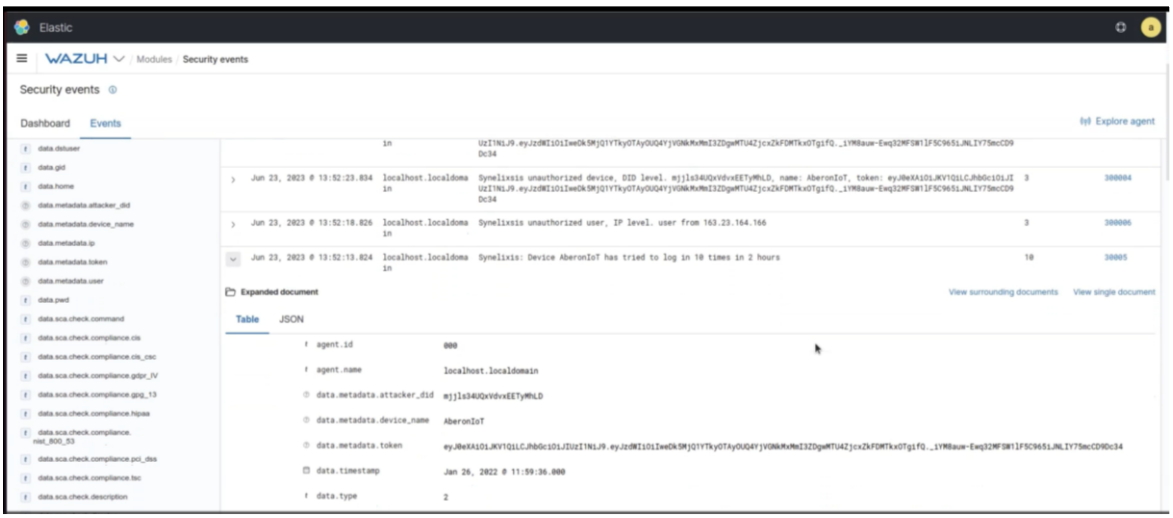


Figure 24: Screenshot from the dashboard of Wazuh that detects the brute force attack issued by David (masquerading a consumer)

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.

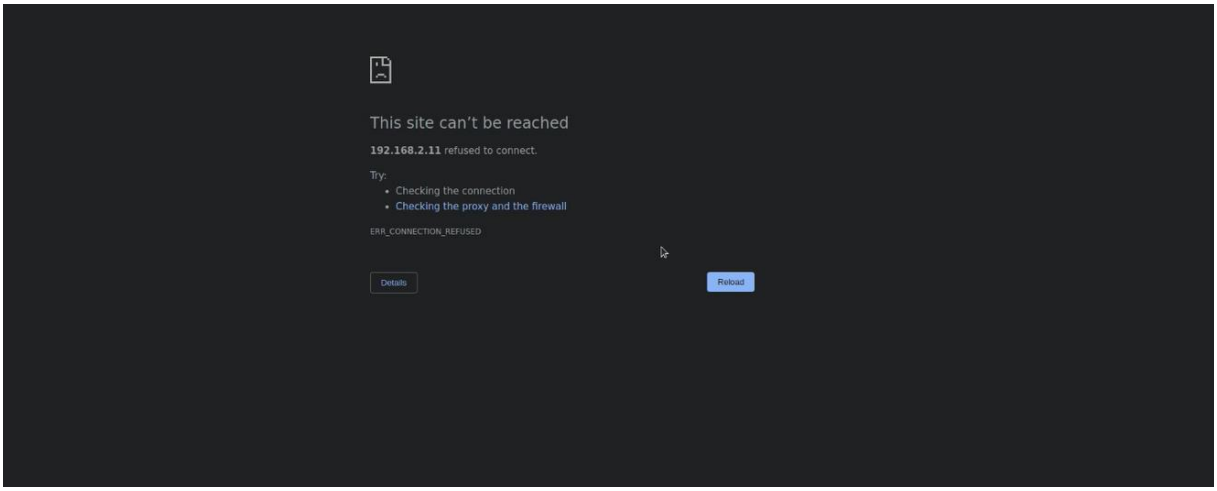


Figure 26: Screenshot from the F2F platform where the inability of the malicious user (David) to enter the platform is shown

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.

```
→ curl http://192.168.248.11:9001/partyinfo | jq '.'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   635  100   635    0     0  42333      0 --:--:-- --:--:-- --:--:-- 42333
{
  "url": "http://quorum-node2.fishy-sc:9001/",
  "peers": [
    {
      "url": "http://quorum-node1.fishy-sc:9001/"
    },
    {
      "url": "http://quorum-node2.fishy-sc:9001/"
    },
    {
      "url": "http://quorum-node3.fishy-sc:9001/"
    },
    {
      "url": "http://quorum-node4.fishy-sc:9001/"
    }
  ],
  "keys": [
    {
      "key": "E5SY6IBNuyesnXpjXhnrlfFq/H4NH+xzOTRkCz4Q2gM=",
      "url": "http://quorum-node4.fishy-sc:9001/"
    },
    {
      "key": "MHFxTeY8fS1aU+DdhpQvseYBSN20YREYH2levMyqhw8=",
      "url": "http://quorum-node3.fishy-sc:9001/"
    },
    {
      "key": "XvEGjW5CvngN8vVNpqWm3fD0g02cj/6AblOry6RSMTg=",
      "url": "http://quorum-node1.fishy-sc:9001/"
    },
    {
      "key": "fZsrQpqSy9xScXIgEUGXy2vokXJsxdAP18RgjxB9QCo=",
      "url": "http://quorum-node2.fishy-sc:9001/"
    }
  ]
}
```

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.

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.

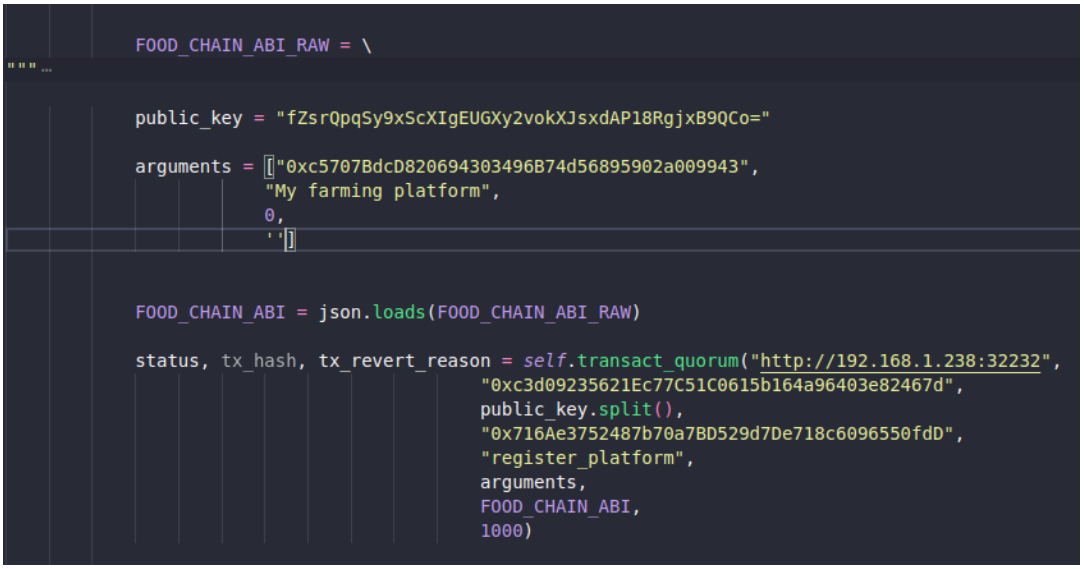


Figure 30: Screenshot from the attempt of the malicious user (Eric) to insert a fake farming platform in the F2F platform

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 NewConnectionE
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.

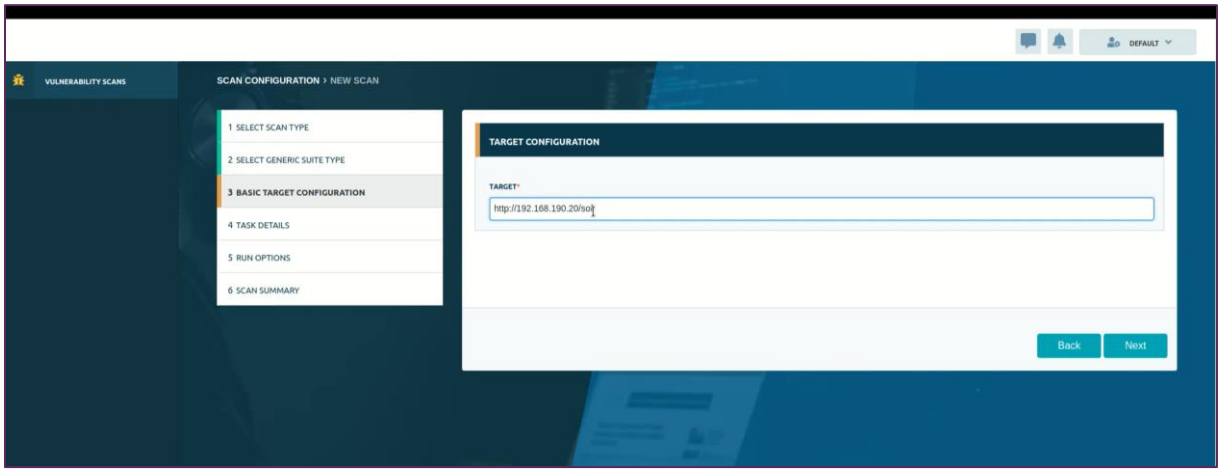


Figure 32: Configuration of VAT to scan the F2F platform

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.

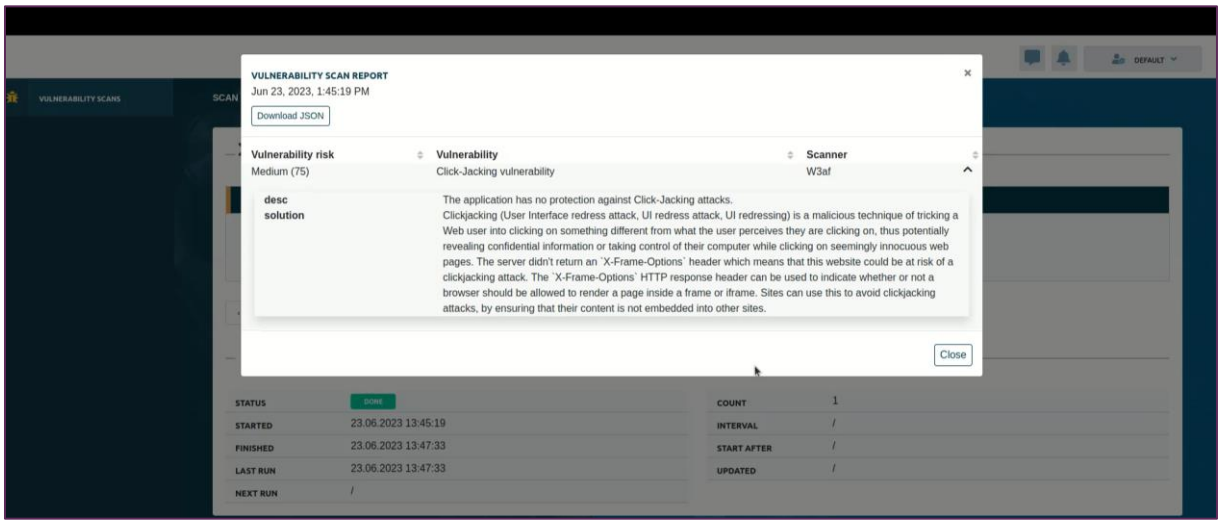


Figure 33: Results of the VAT scan of the F2F platform

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

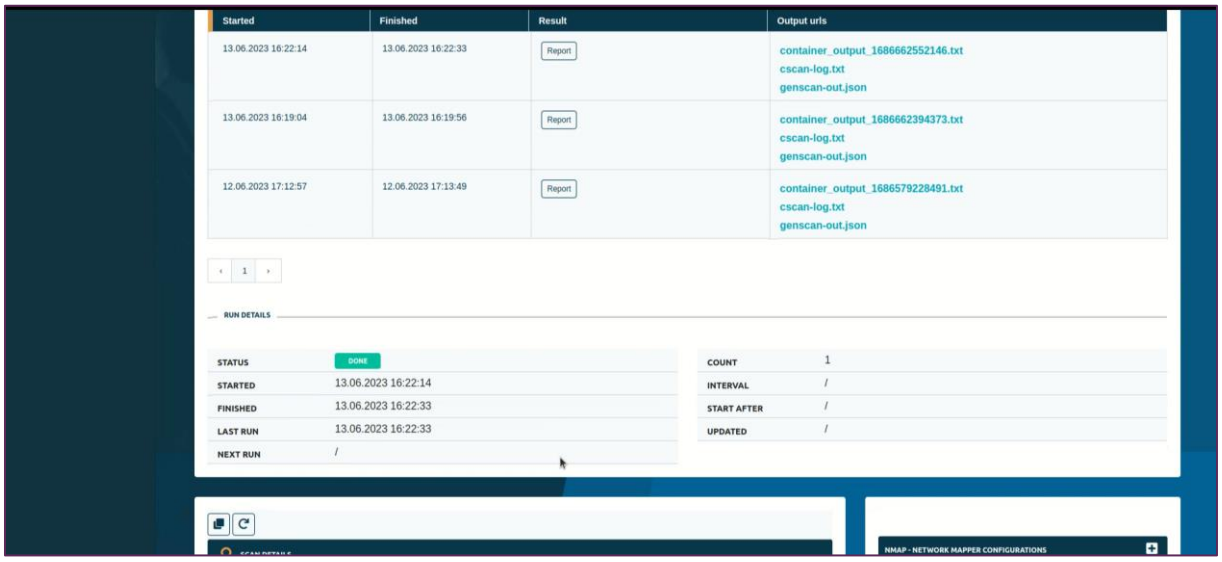


Figure 34: VAT monitors the availability of nodes

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.

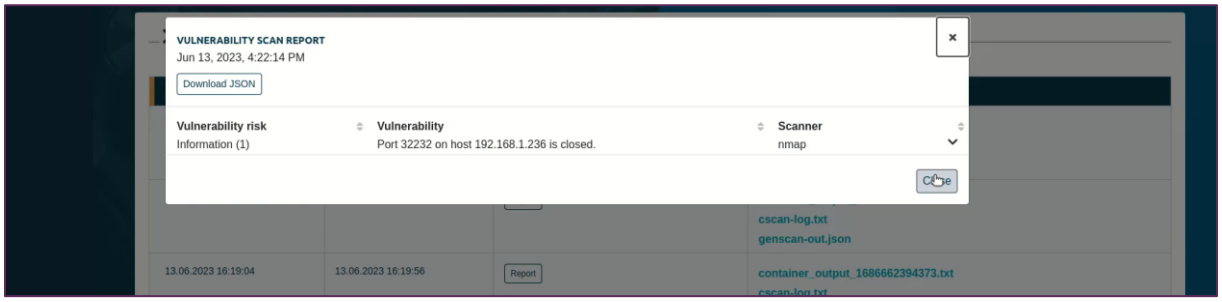


Figure 35: VAT has detected that the port is closed

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.

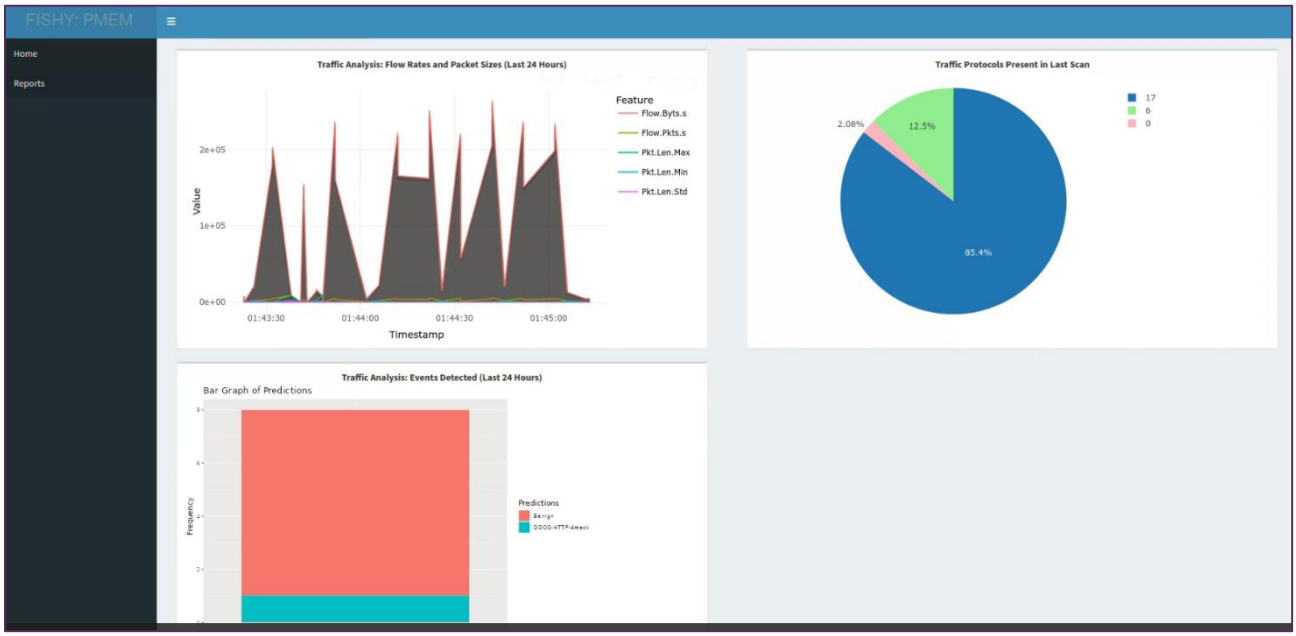
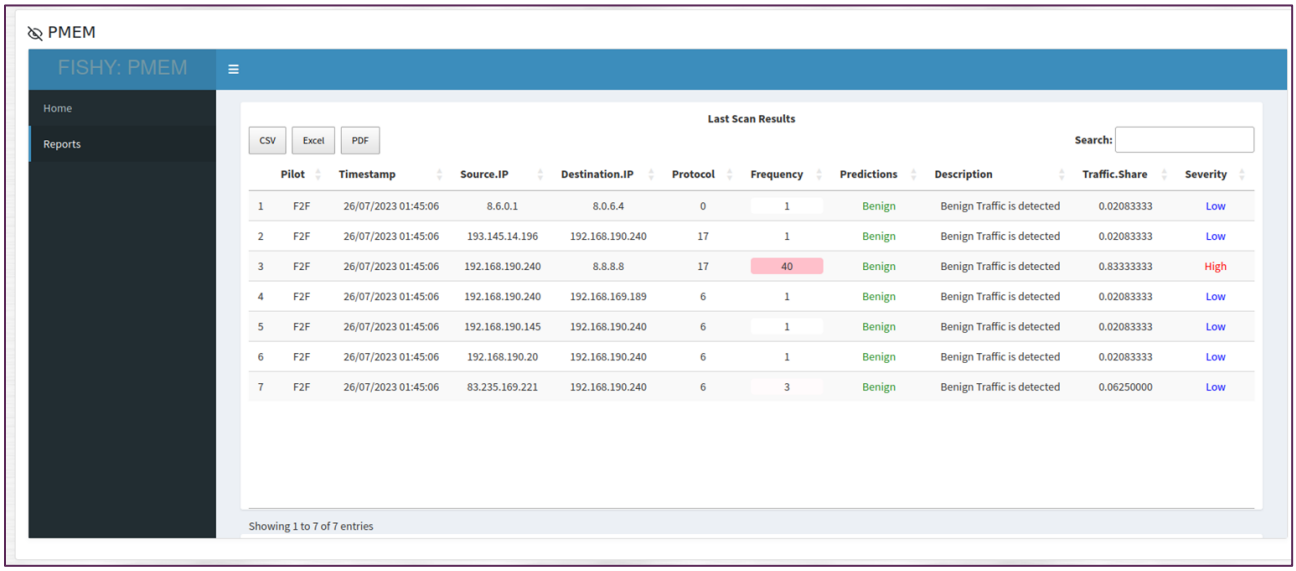


Figure 36: PMEM dashboard showing the traffic of the system under examination

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



Pilot	Timestamp	Source.IP	Destination.IP	Protocol	Frequency	Predictions	Description	Traffic.Share	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.

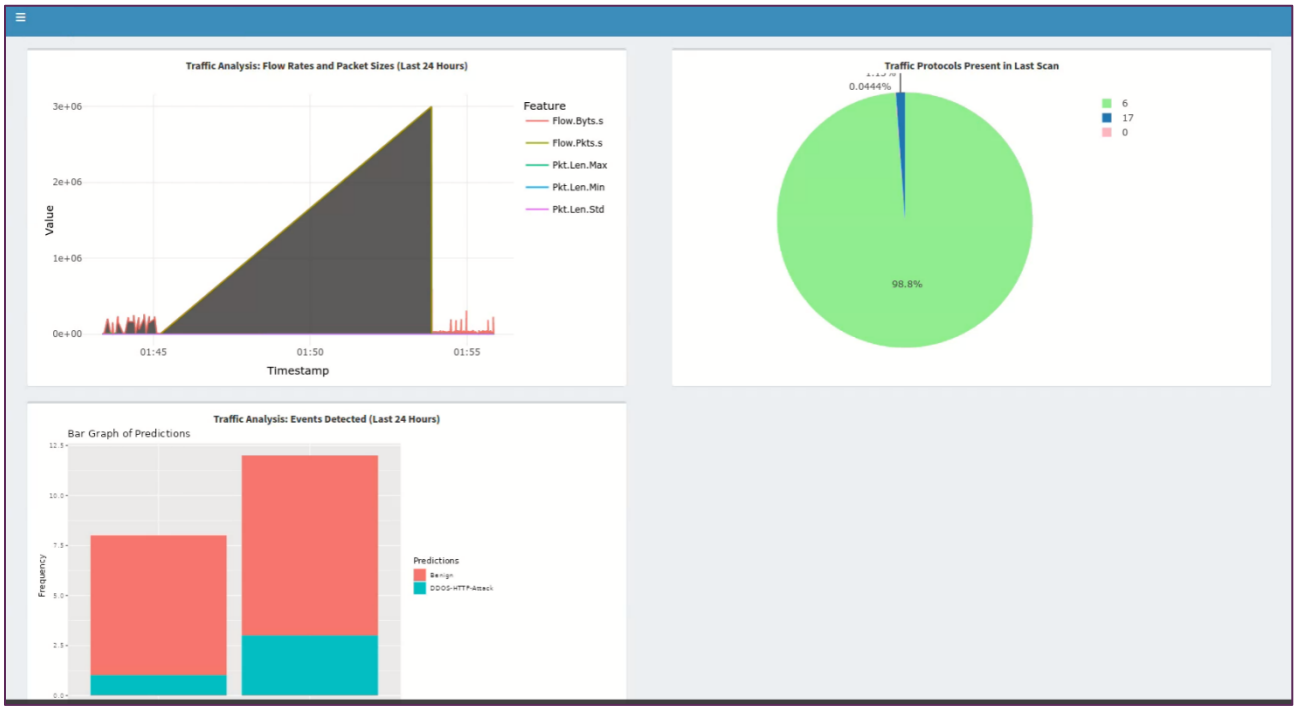
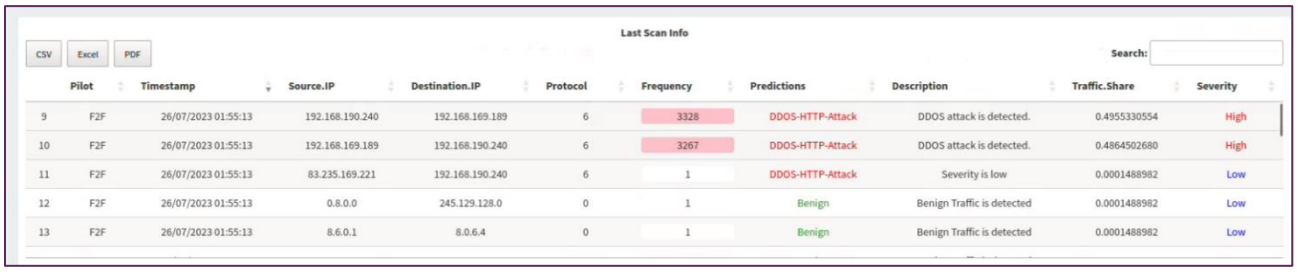


Figure 38: PMEM dashboard showing the statistics which show the results of the Machine Learning model (which classifies the traffic in benign and suspicious)

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



	Pilot	Timestamp	Source.IP	Destination.IP	Protocol	Frequency	Predictions	Description	Traffic.Share	Severity
9	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
10	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	High
11	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	Low
12	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
13	F2F	26/07/2023 01:55:13	8.6.0.1	8.0.6.4	0	1	Benign	Benign Traffic is detected	0.0001488982	Low

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.

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).

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

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	IoT Gateway	YES	
FISHY appliance	LOMOS, PMEM	YES	

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.

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

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 2nd 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.

	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.

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:

Table 6: Satisfaction of KPIs defined in the DoA

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.

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	Type	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

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.

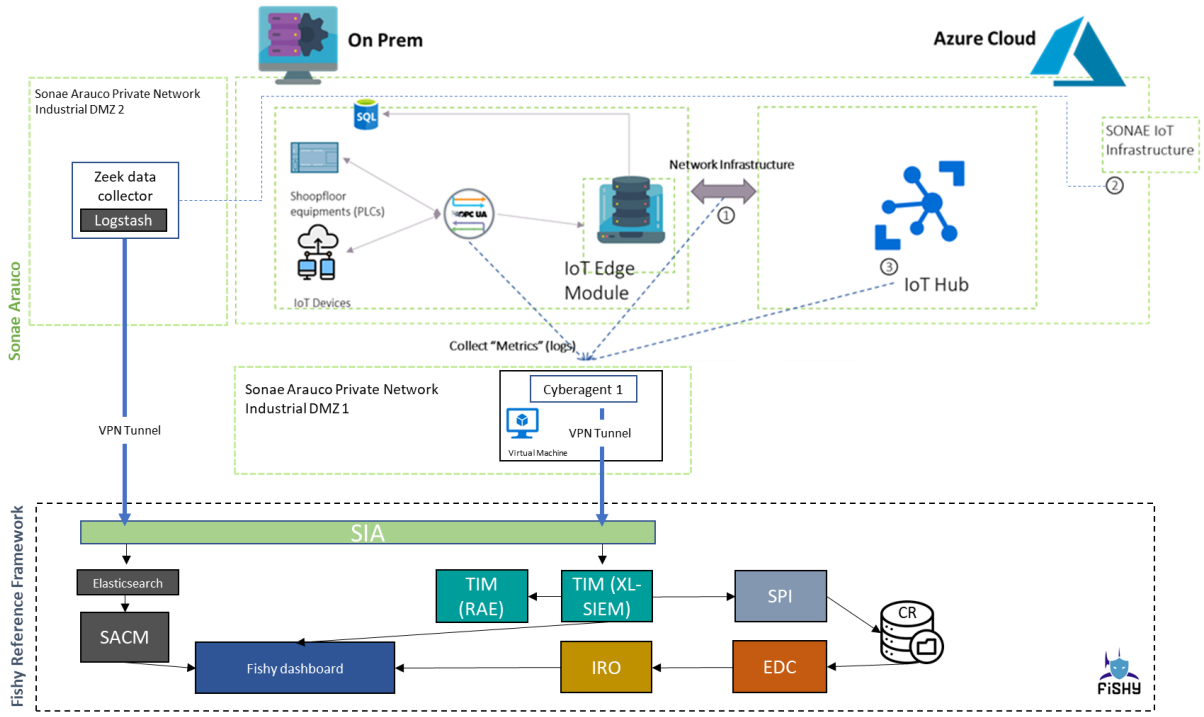


Figure 40: The connected factory architecture and its interconnection with the FISHY Platform in the FRF

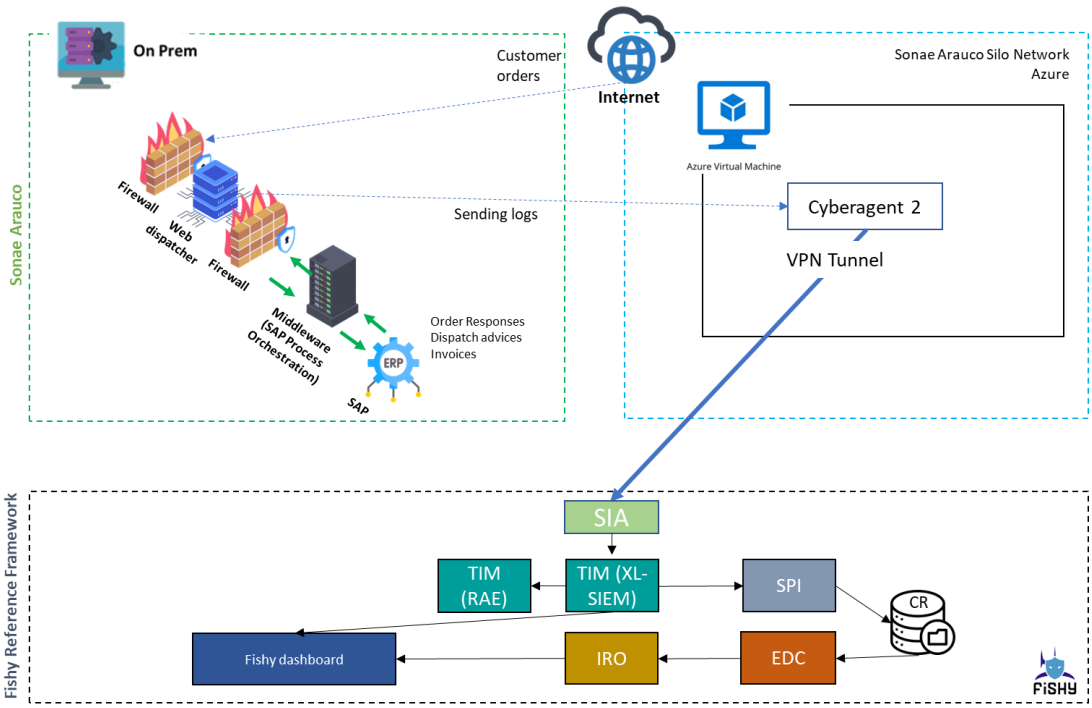


Figure 41: SAP EDI communications architecture and its interconnection with the FISHY Platform in the FRF

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)

    - 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*).

Table 8: ENISA framework applied to the WBP identified attacks

	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

Type 1: Unauthorized device	**Physical Attack or Modification** (physical intrusion of an unauthorized IoT device) **Exploit Security Vulnerabilities** (The unauthorized IoT device might have inherent security vulnerabilities or act as a bridge to compromise other devices or systems within the IoT infrastructure)	**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**

			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

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.

Table 9: Asset/Impact Synthesis

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 Dispatcher	Internet	High	Types 2, 4 and 5 attacks of the previous list

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.

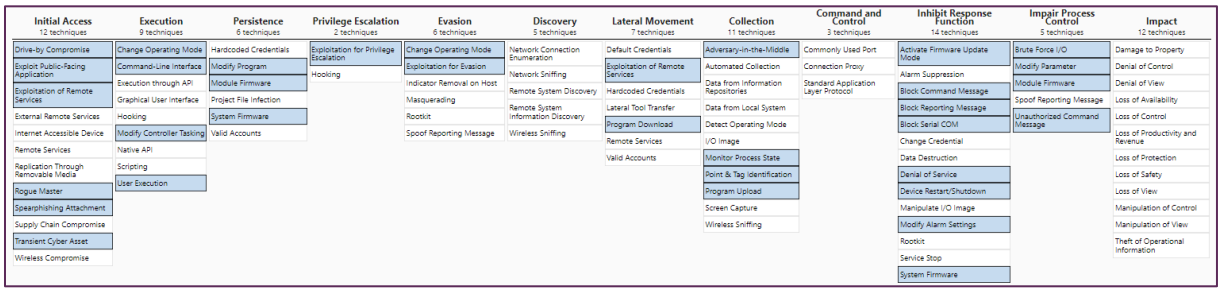


Figure 42: attacks that can be detected with logs as data source

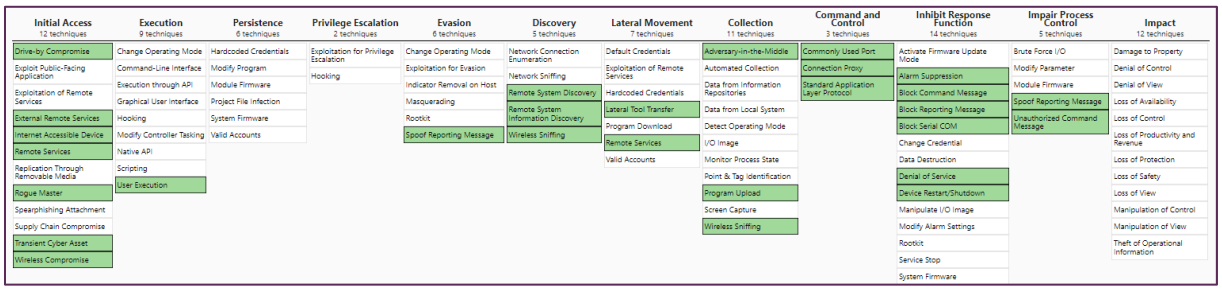


Figure 43: Attacks that can be detected with network traffic as data source

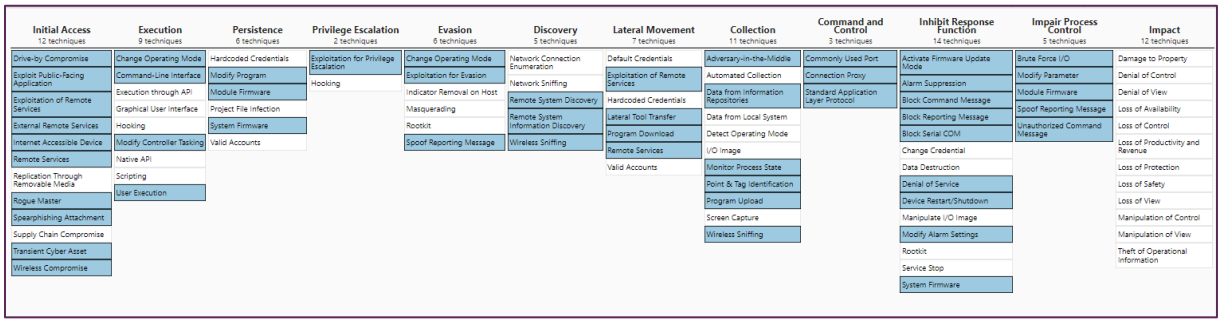


Figure 44: Attacks that can be detected with both logs and network traffic as data sources (53 out of 80, i.e. 66%)

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).

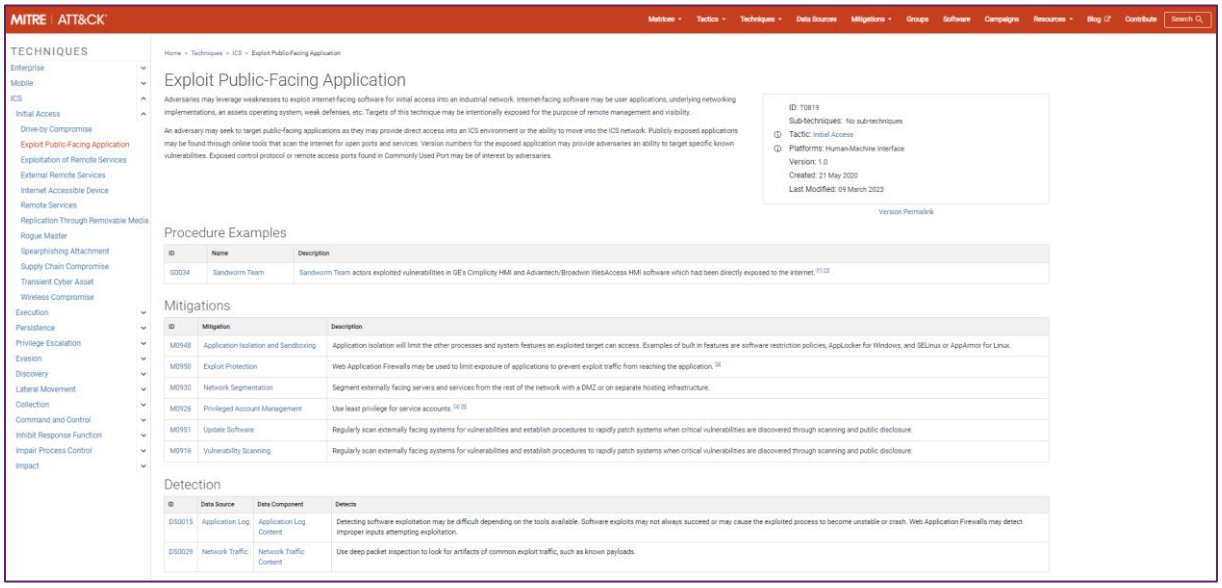


Figure 45: MITRE ATT&CK Exploit Public-Facing Application technique details on procedure examples, mitigation actions and detection sources

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.

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:

Table 10: Success probability assessment for potential attacks

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

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).

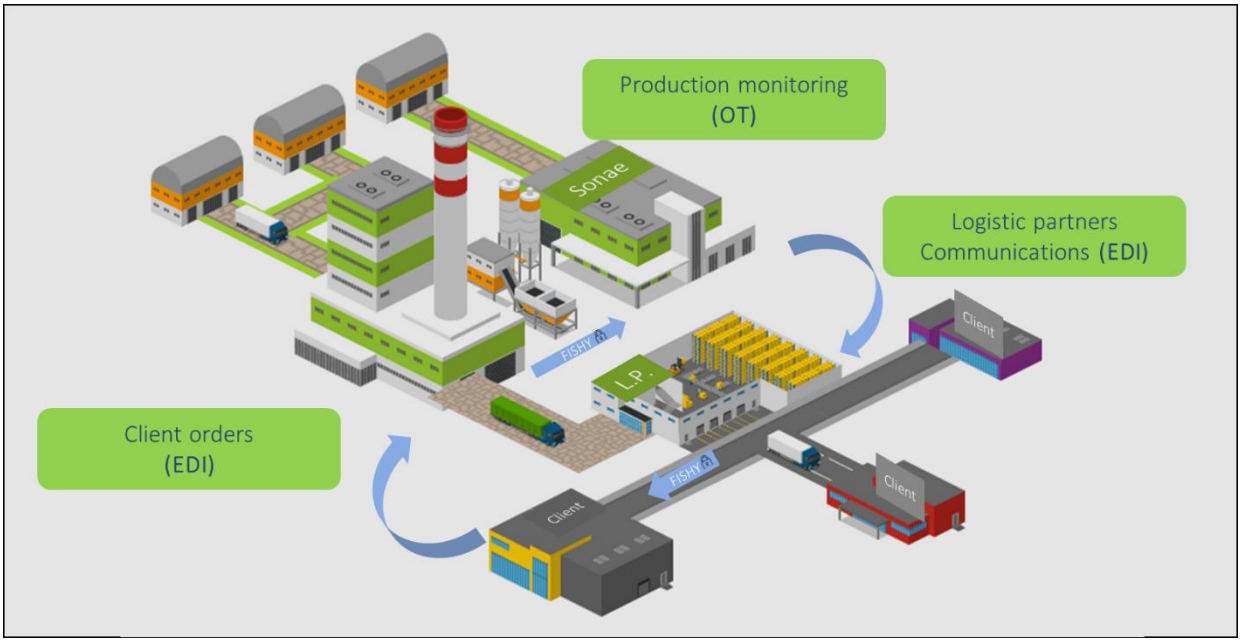


Figure 46: High level view of the three main nodes and streams of work affected by the WBP UC in FISHY

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:

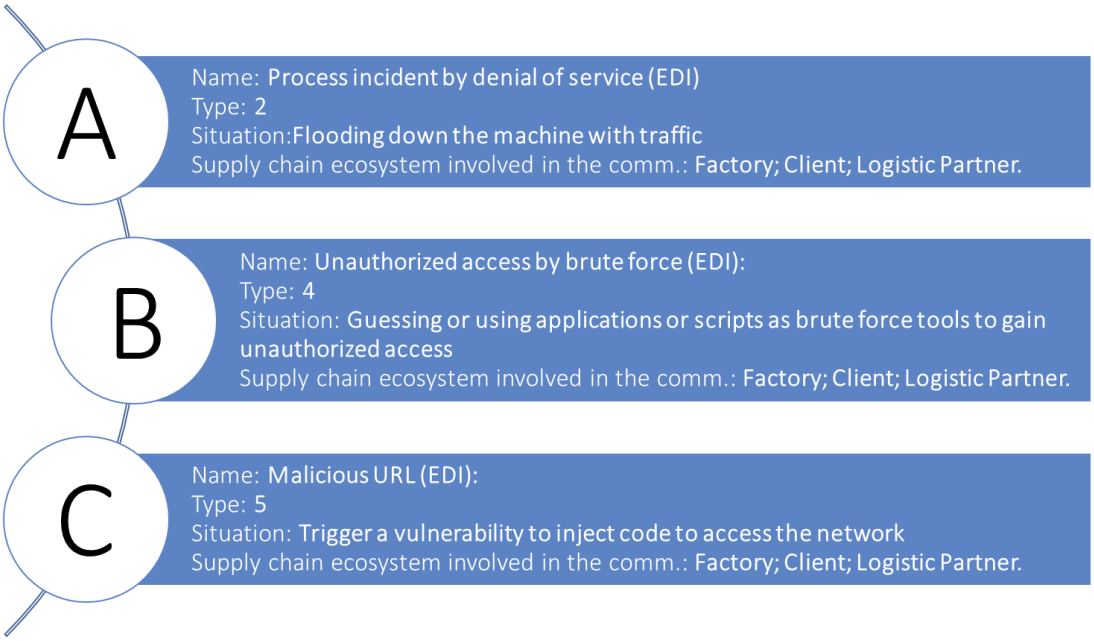


Figure 47: Priority threats identified and tested on FISHY for the EDI communications

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

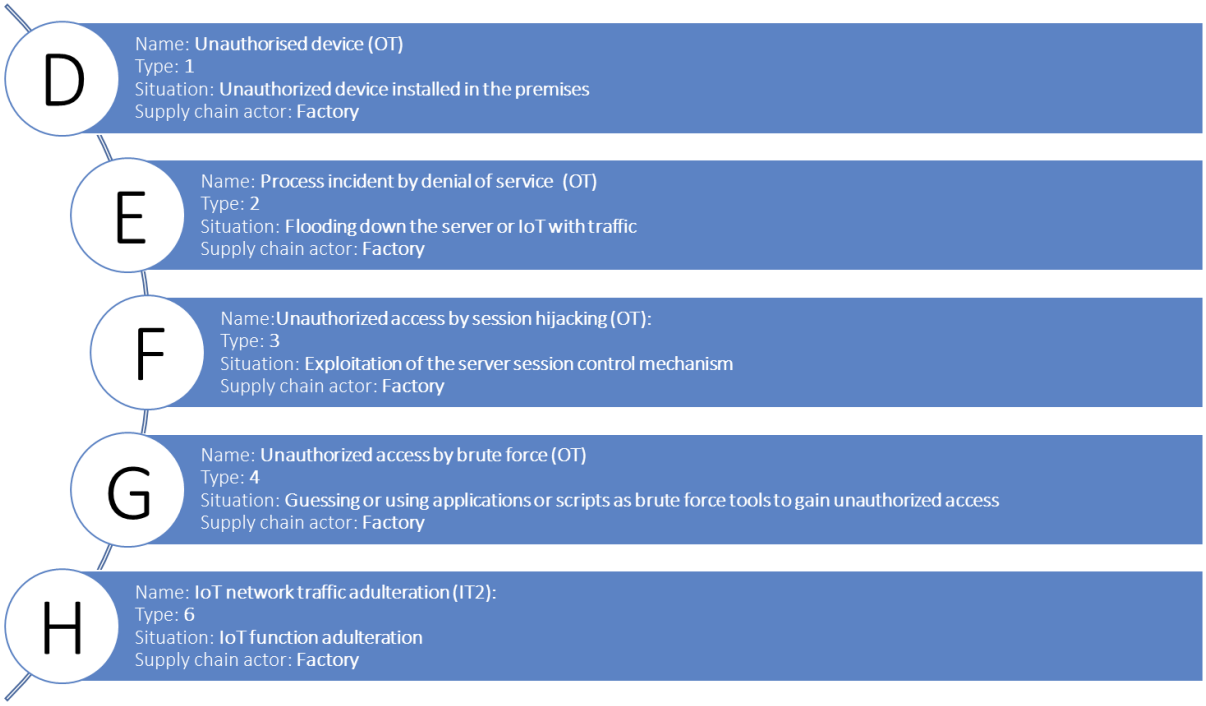


Figure 48: Priority threats identified and tested on FISHY for the production monitoring

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.

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.

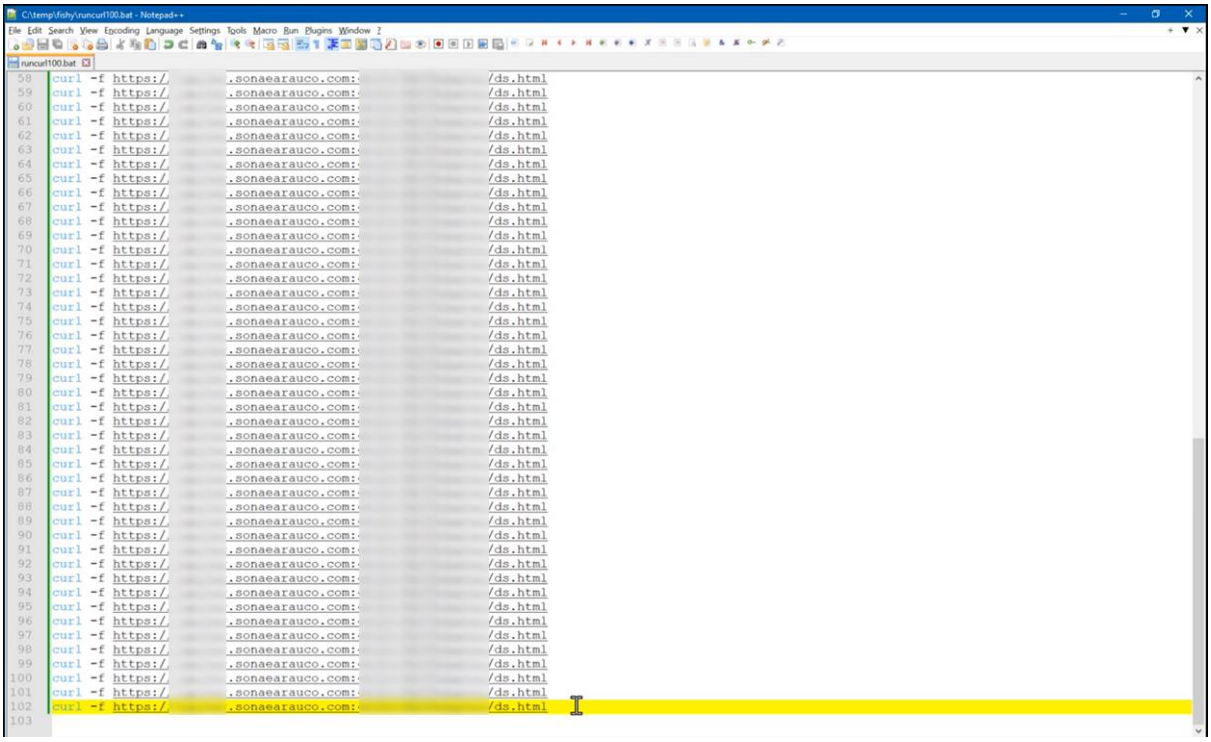


Figure 49: Evidence of the 102 calls made using the batch script created for the simulation

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.

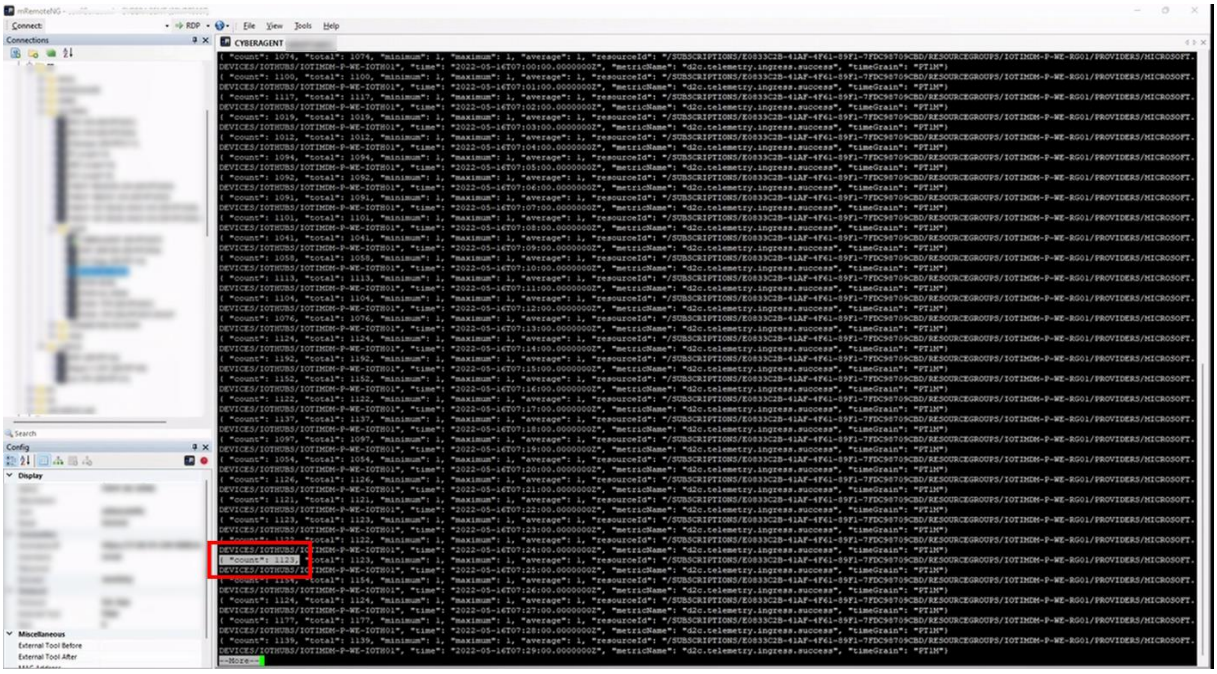


Figure 50: Evidence of the IoT Hub telemetry being above 1000

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.

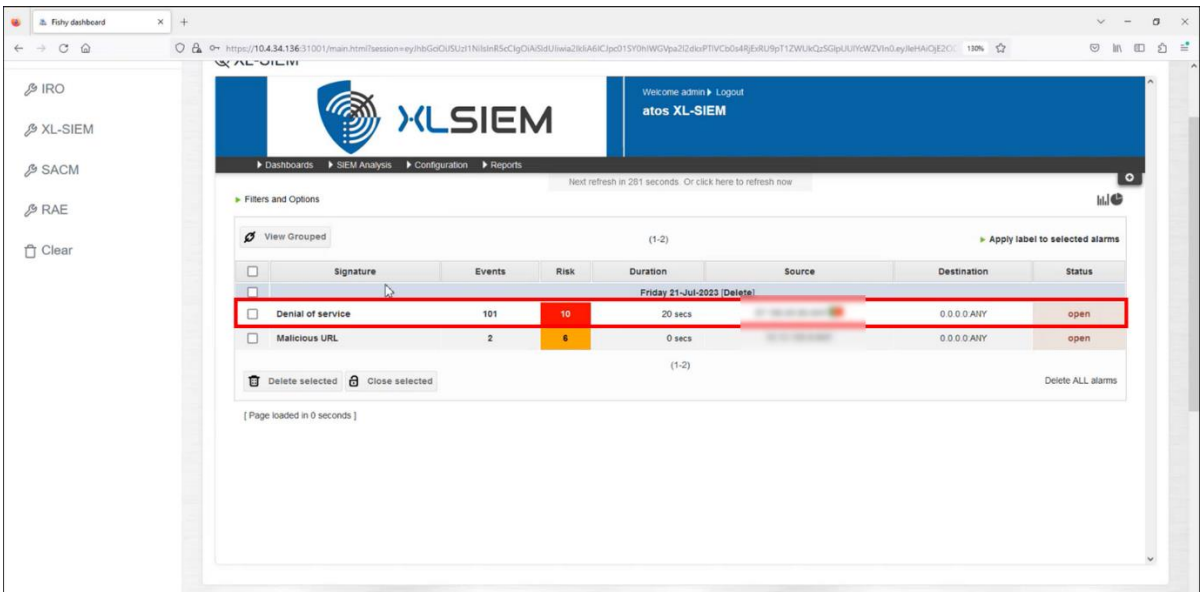


Figure 51: XL-SIEM alarm on the DoS

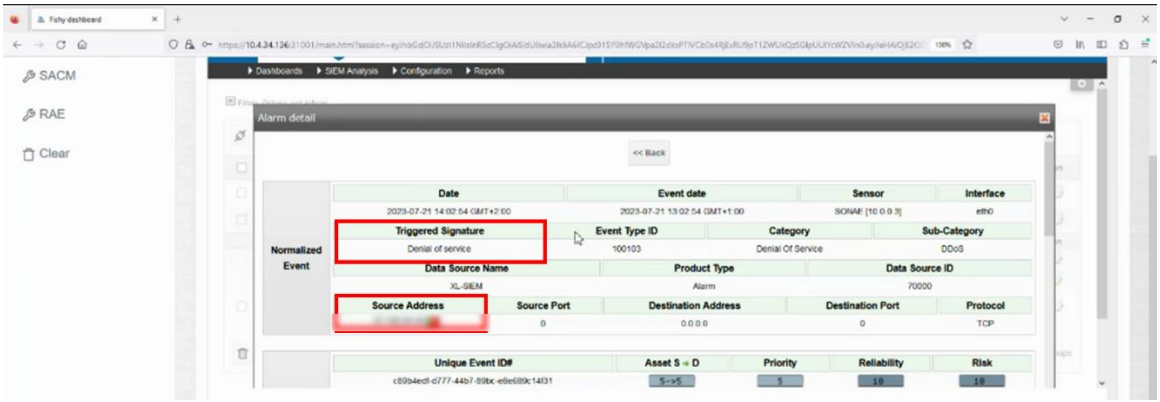


Figure 52: XL-SIEM displaying details on the events that originated the DoS

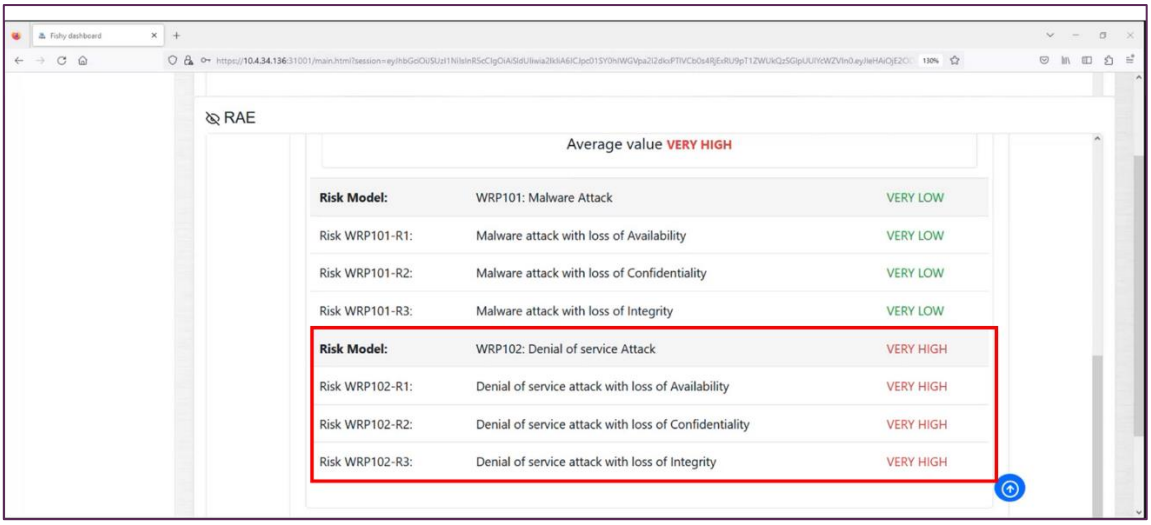


Figure 53: RAE displaying a risk level increase due to the risk of denial-of-service.

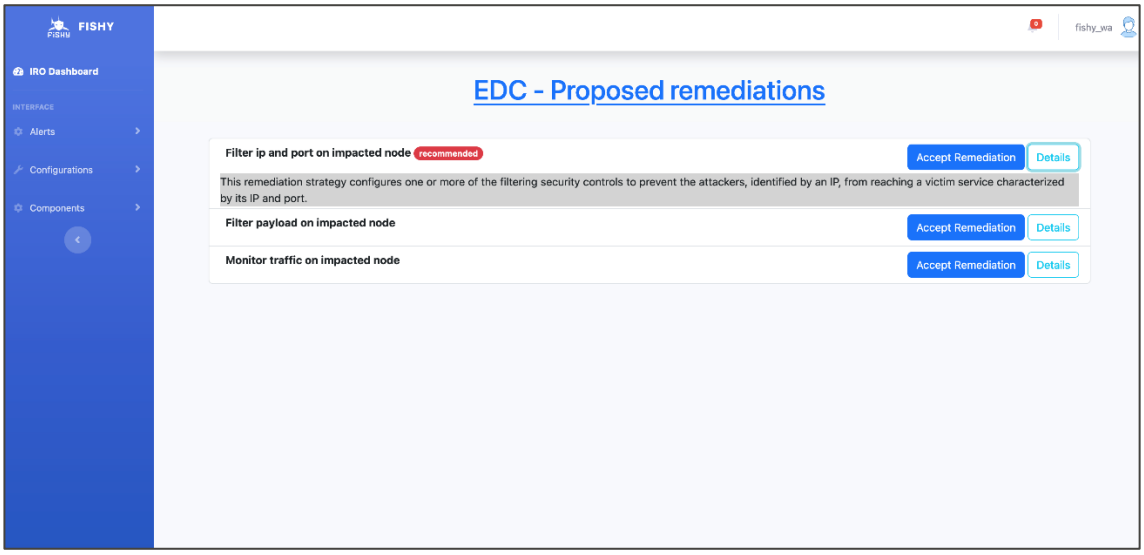


Figure 54: EDC recommendation on the IRO dashboard to “filter ip and port on impacted node”

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.

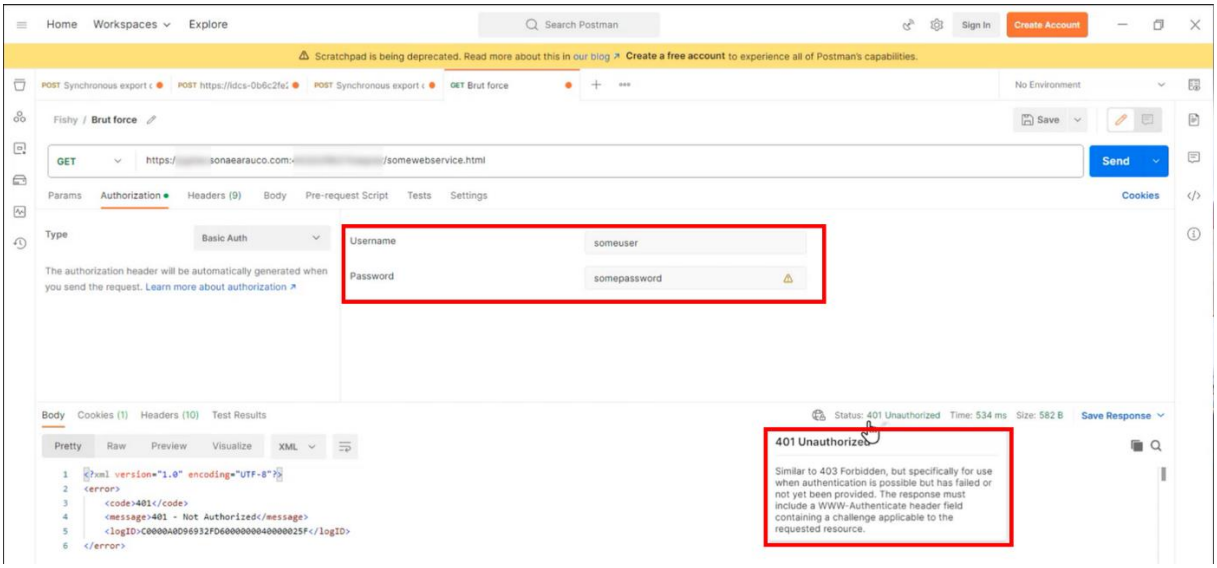


Figure 55: Brute force login attempt simulation via Postman using a wrong password multiple times

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) .

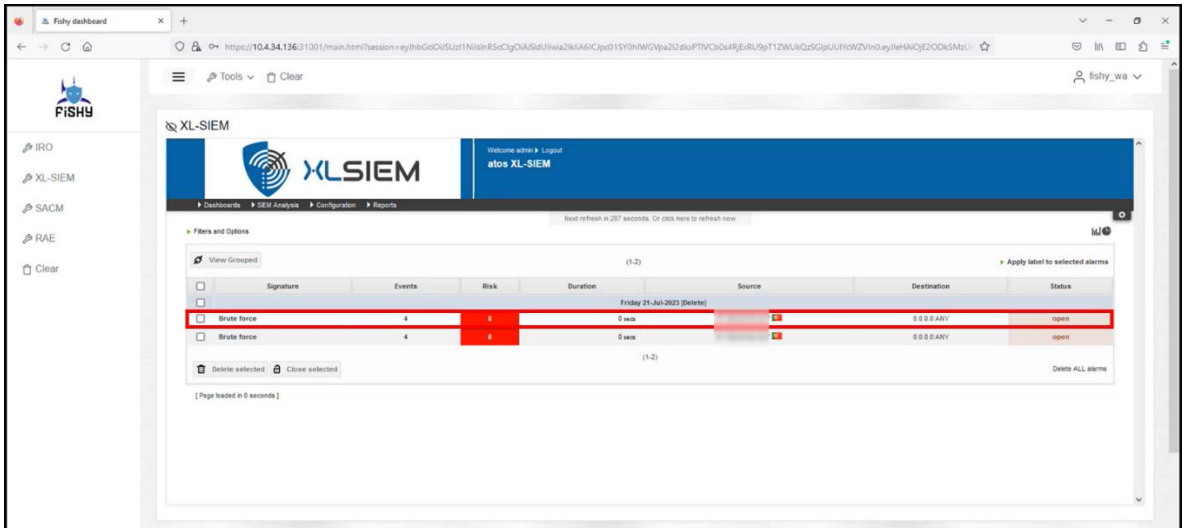


Figure 56: XL-SIEM alarm on the brute force attack attempt

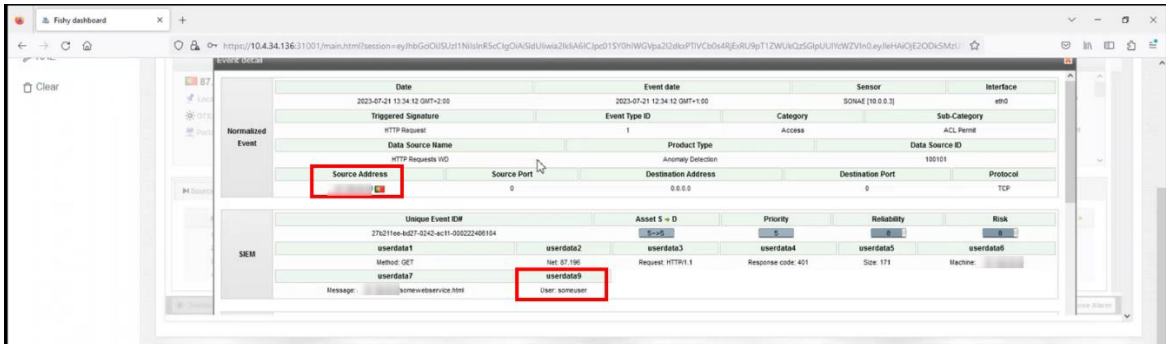


Figure 57: XL-SIEM displaying details on the events that originated the Brute Force detection

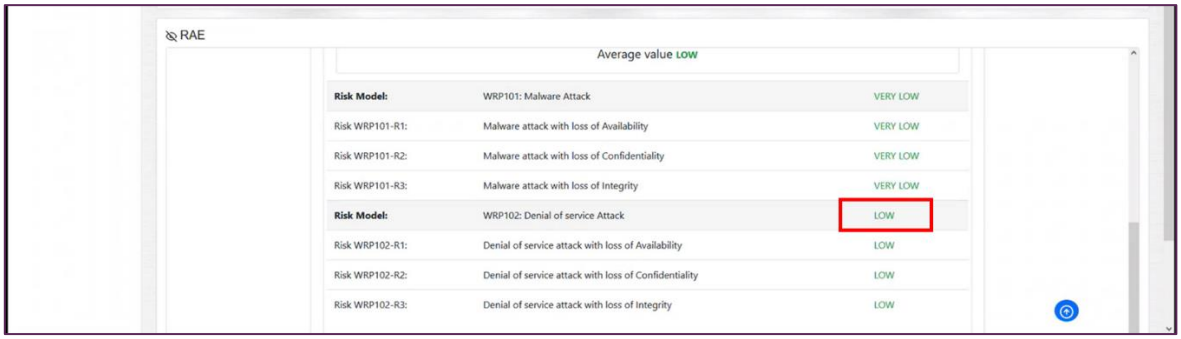


Figure 58: RAE displaying a risk level increase on the denial-of-service risk model

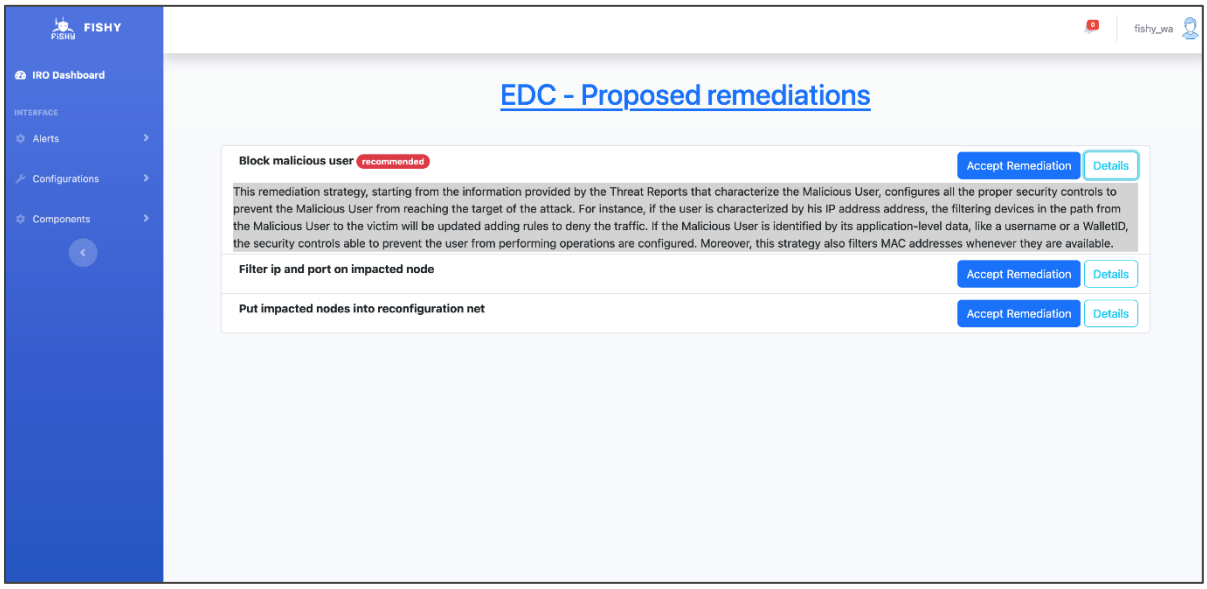


Figure 59: EDC recommendation on the IRO dashboard to block malicious user IP

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.

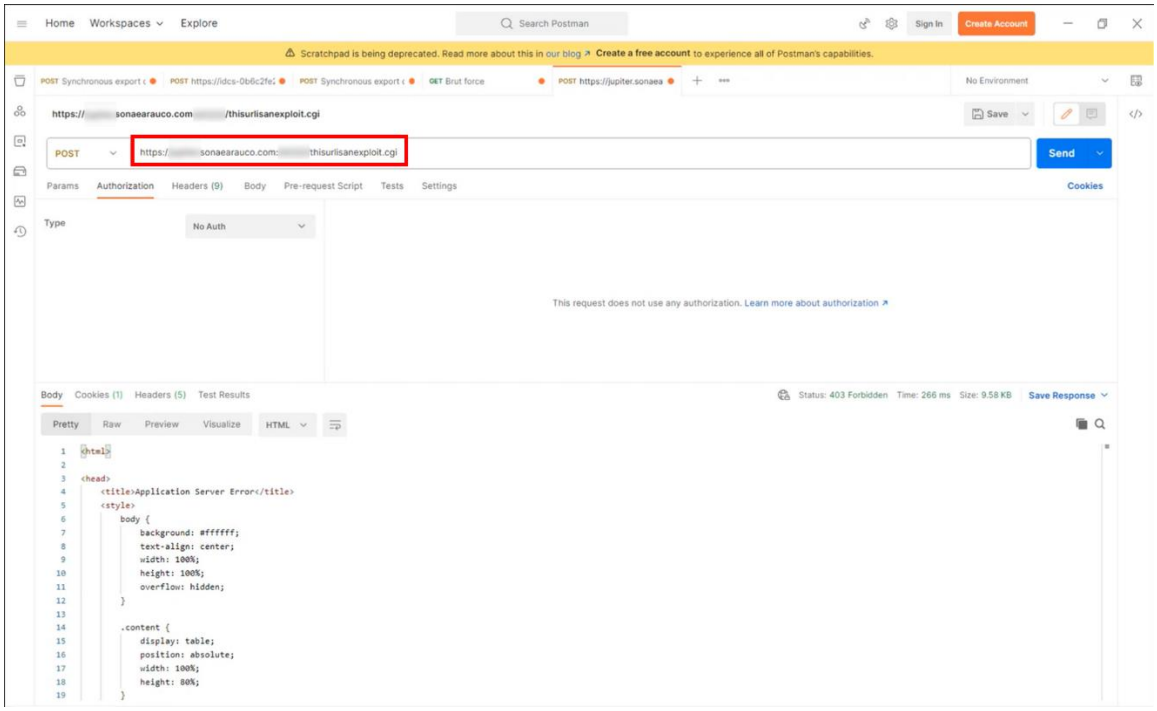


Figure 60: Malicious URL request simulation via Postman by calling an unauthorized URL

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).

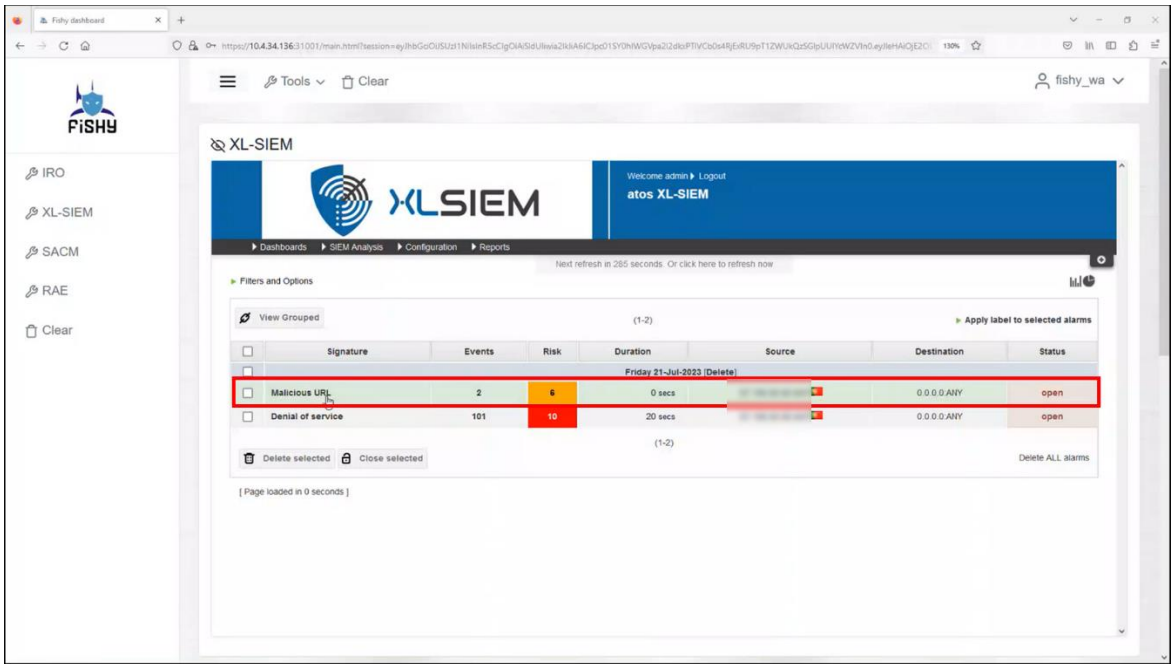


Figure 61: XL-SIEM alarm on the invalid URL request

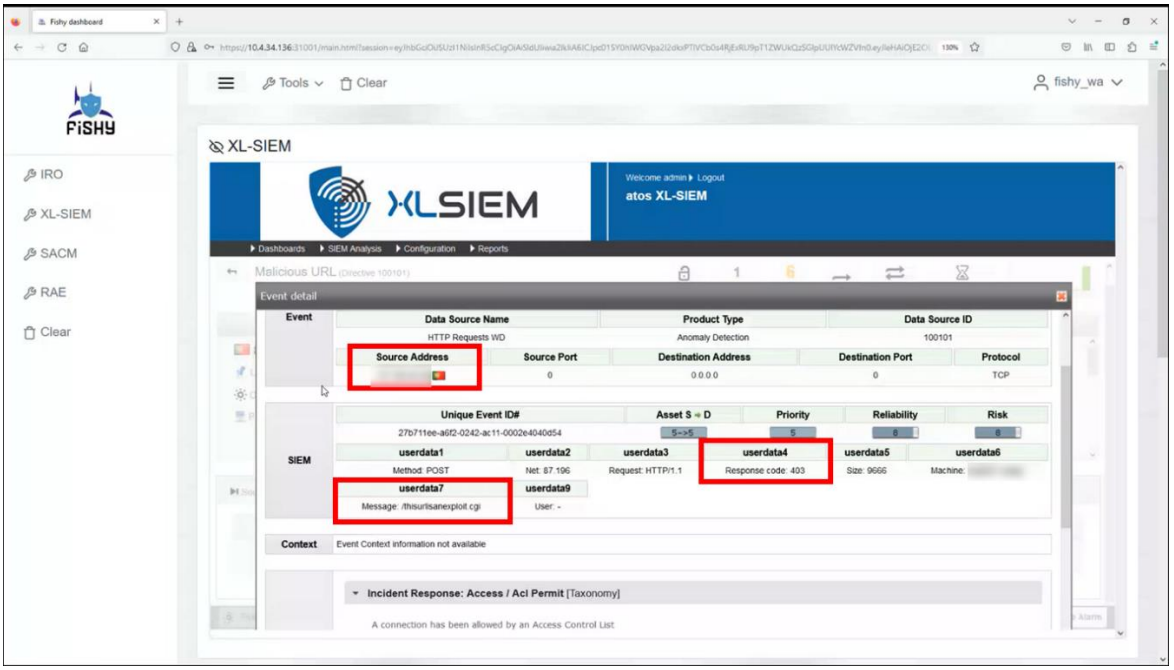


Figure 62: XL-SIEM displaying details on the events that originated the malicious URL detection.

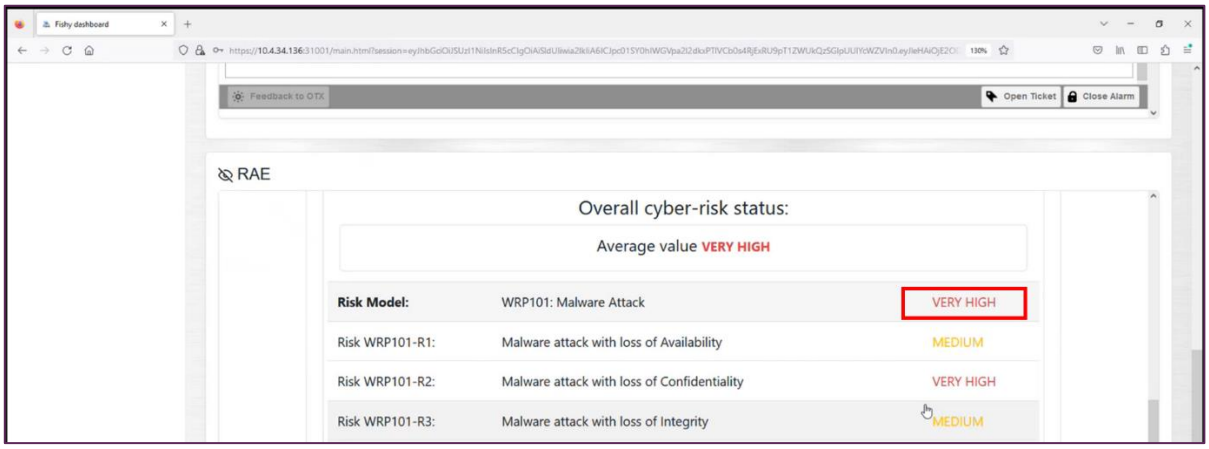


Figure 63: RAE risk increases due to the invalid URL request

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

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.

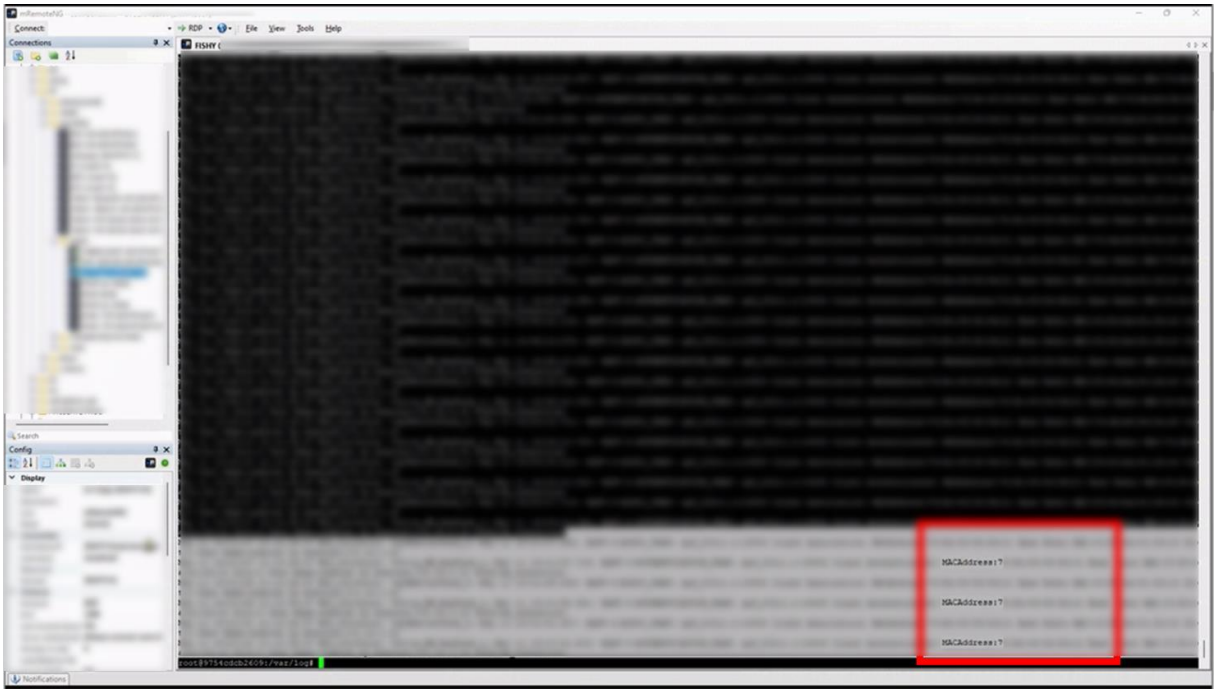


Figure 65: Cyberagent identifying the connection of an unknown new device with the Mac Address 74:fe:48:56:9d:21

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).

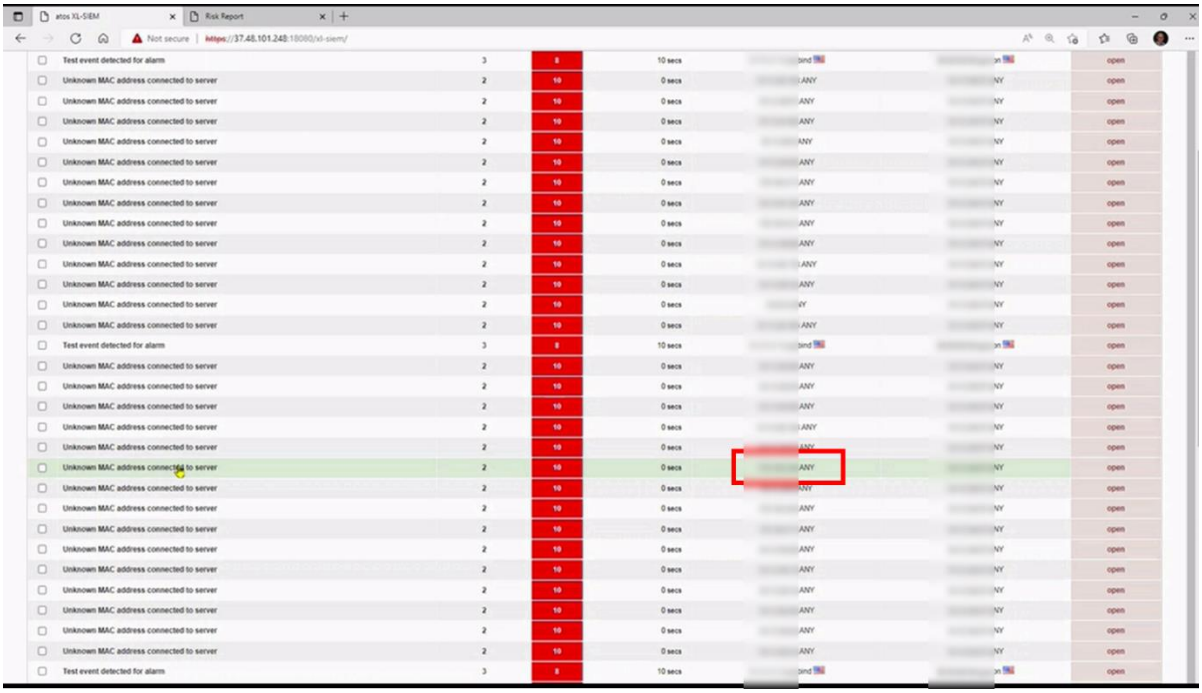


Figure 66: XL-SIEM alarm on the unknown device from the WIFI Controller IP, the source of the signal

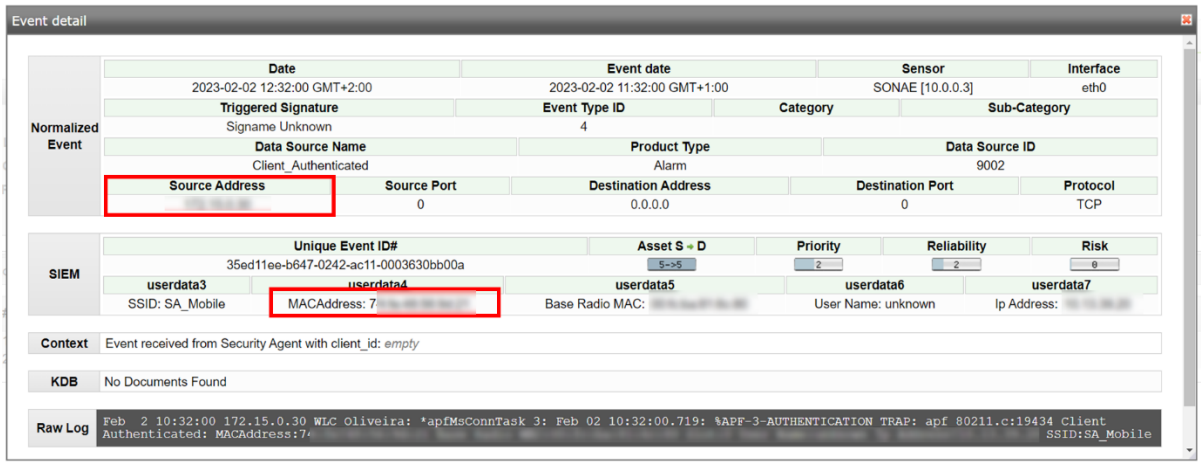


Figure 67: XL-SIEM displaying details on the device detected including the MAC Address

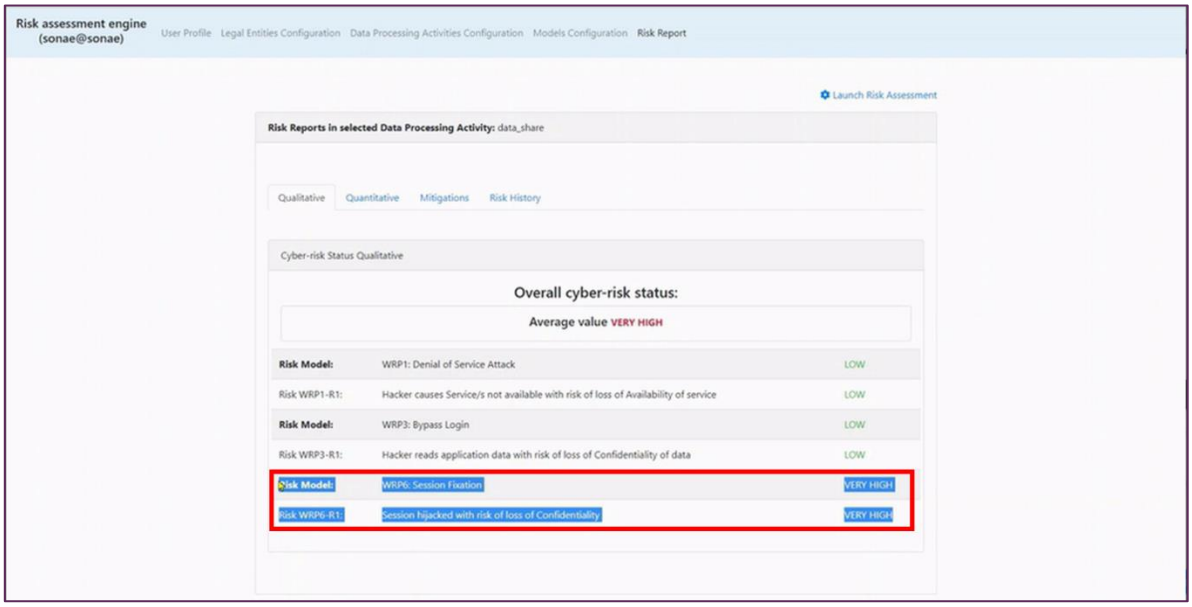


Figure 68: RAE risk increase due to the unauthorized connection

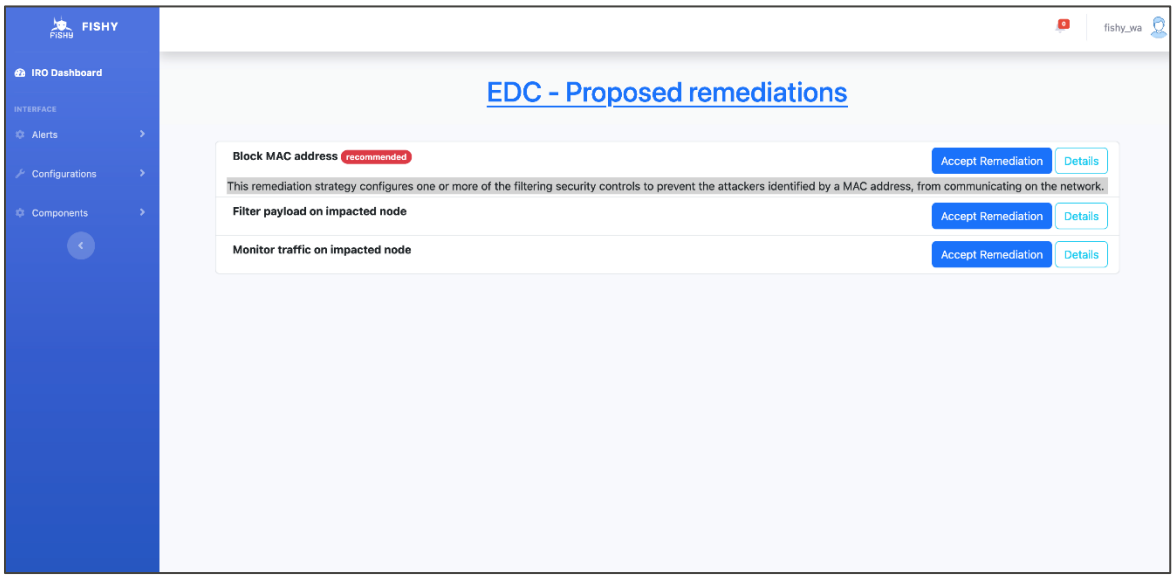


Figure 69: EDC recommendation on the IRO dashboard to react to the unknown device/asset by suggesting to block the MAC Address

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

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.

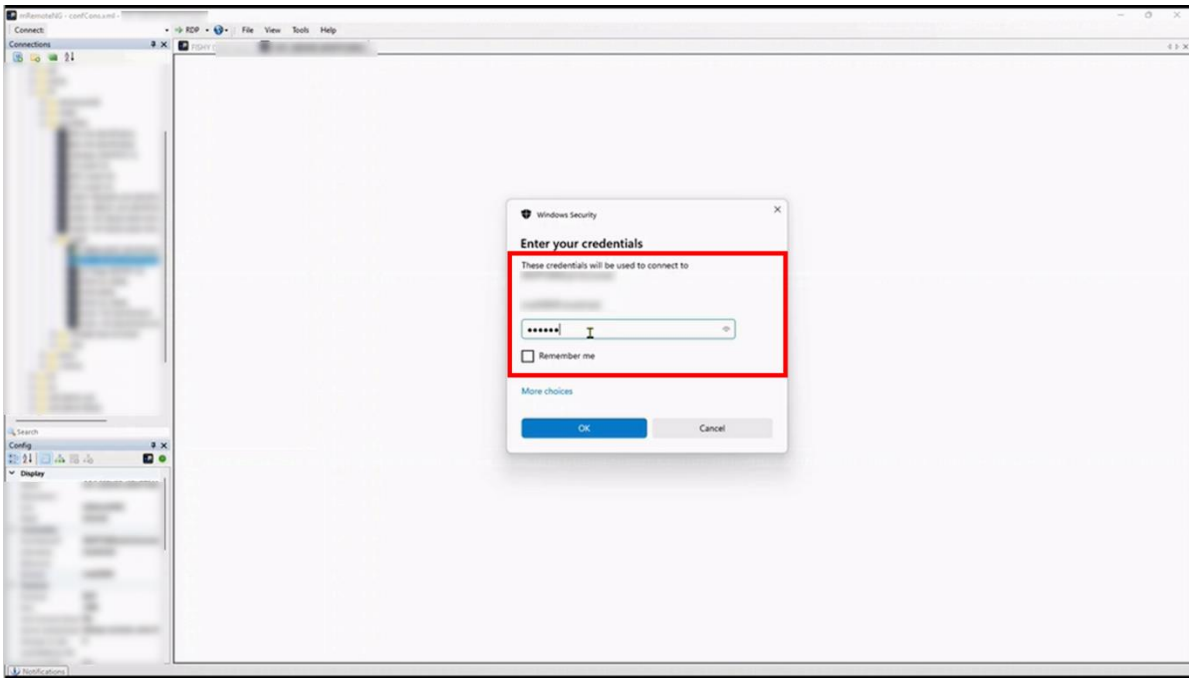


Figure 70: Logging in to the SRVPT5004 server with a valid user ID

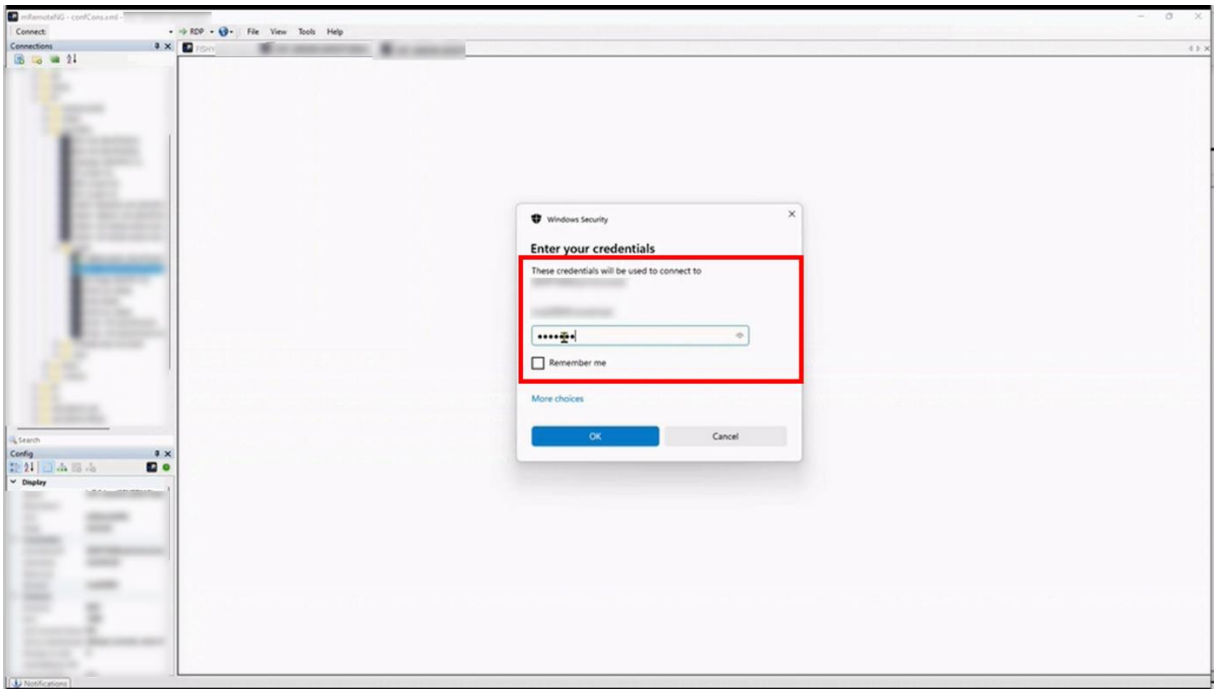


Figure 71: Logging in to the SRVPT5110 server with the same user ID from Figure 64 simultaneously

FISHY reacts to the attack

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).

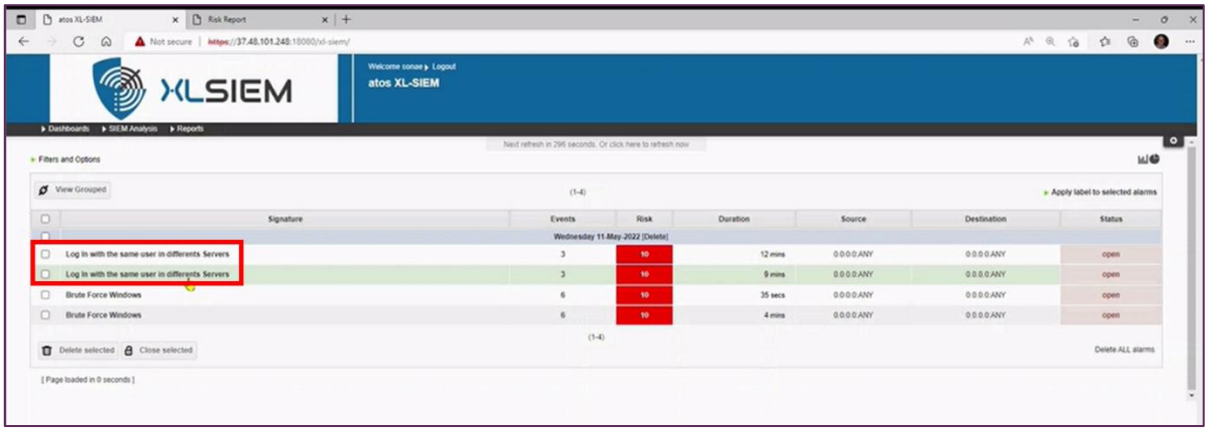


Figure 72: XL-SIEM alarm on attempt to login in different servers with the same user ID

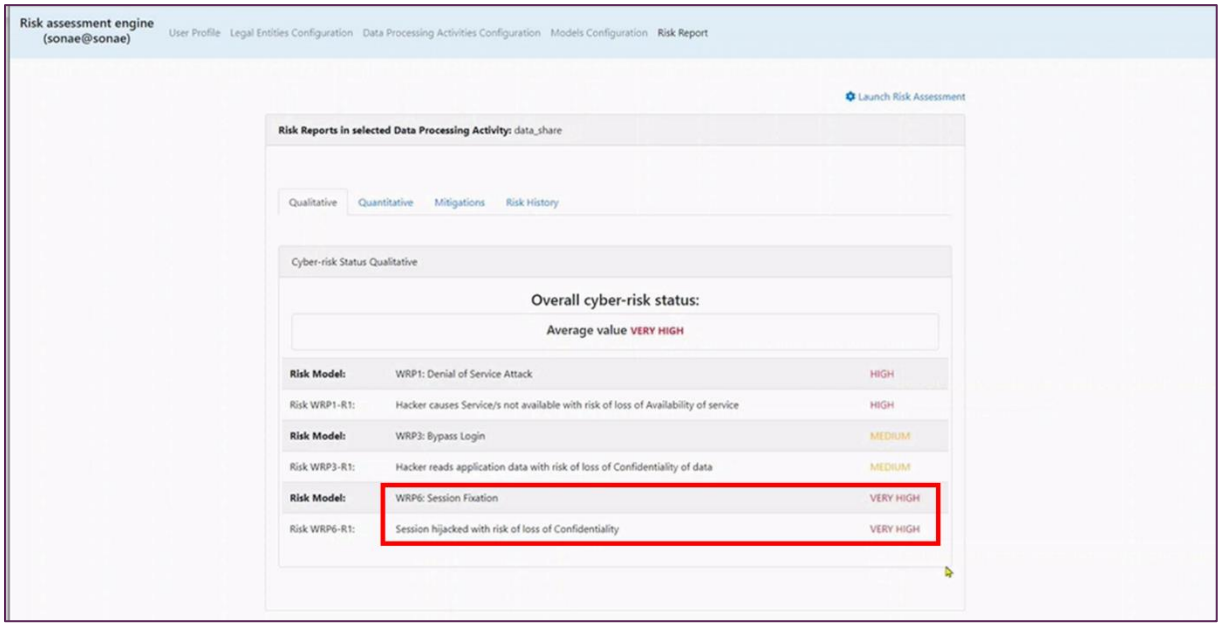


Figure 73: RAE displaying a risk increase due to the possible session hijacking

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].

```
PING 192.168.2.33 (192.168.2.33): 56 data bytes
64 bytes from 192.168.2.33: seq=0 ttl=64 time=0.932 ms
64 bytes from 192.168.2.33: seq=1 ttl=64 time=0.450 ms
64 bytes from 192.168.2.33: seq=2 ttl=64 time=0.159 ms
64 bytes from 192.168.2.33: seq=3 ttl=64 time=0.157 ms
64 bytes from 192.168.2.33: seq=4 ttl=64 time=0.160 ms
64 bytes from 192.168.2.33: seq=5 ttl=64 time=0.166 ms
64 bytes from 192.168.2.33: seq=6 ttl=64 time=0.171 ms
64 bytes from 192.168.2.33: seq=7 ttl=64 time=0.164 ms
64 bytes from 192.168.2.33: seq=8 ttl=64 time=0.188 ms
64 bytes from 192.168.2.33: seq=9 ttl=64 time=0.152 ms
64 bytes from 192.168.2.33: seq=10 ttl=64 time=0.164 ms
64 bytes from 192.168.2.33: seq=11 ttl=64 time=0.232 ms
^C
--- 192.168.2.33 ping statistics ---
12 packets transmitted, 12 packets received, 0% packet loss
```

Figure 75: Simulating an ICMP flood

FISHY reacts to the attack

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.

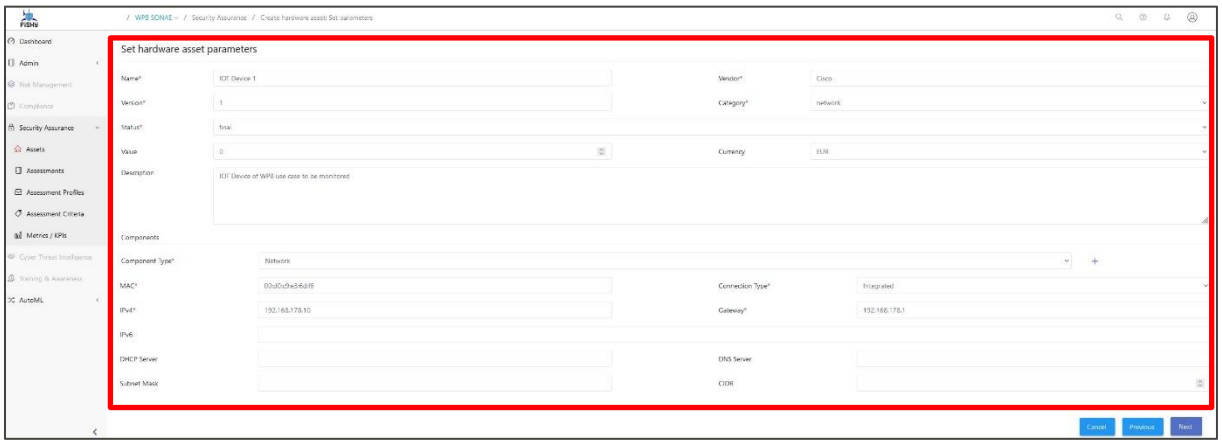


Figure 76: SACM configuration of a new asset/device to be monitored.

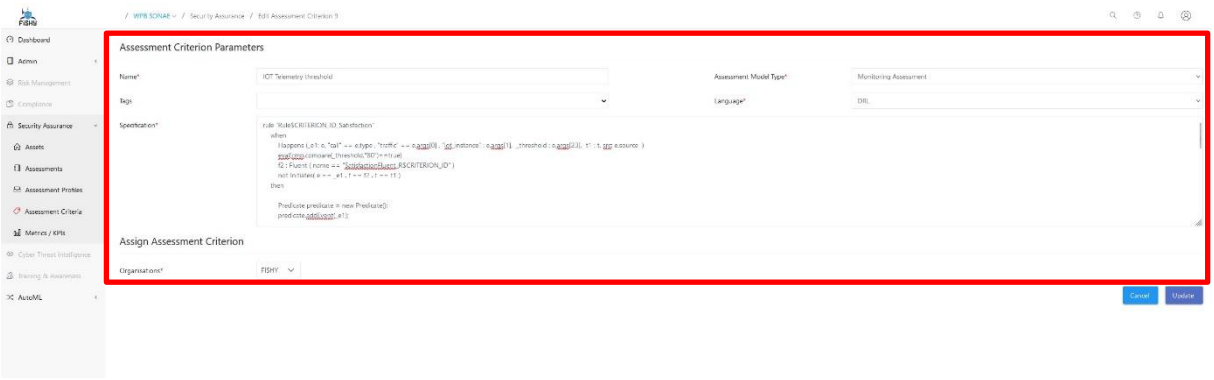


Figure 77: SACM definition of rule specifications including every threshold value

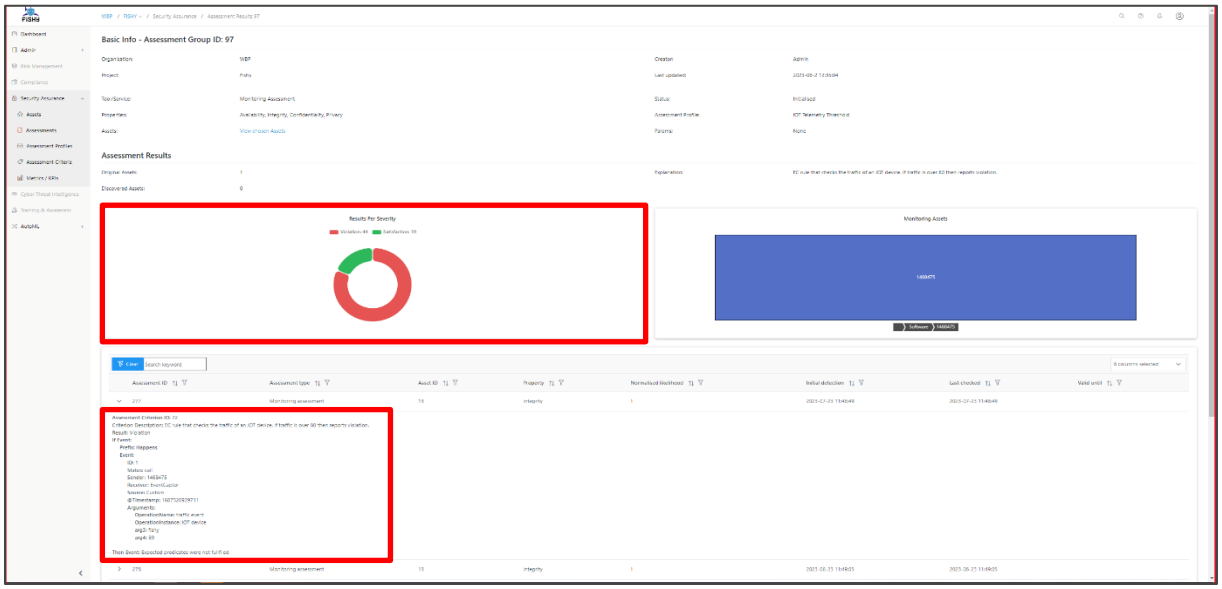


Figure 78: SACM monitoring results regarding the satisfaction of applied rules

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 XL-SIEM in terms of loss of availability, integrity or confidentiality

	VAT	NO	
	WAZUH	NO	
	Trust Monitor	NO	
	Zeek	YES	Iot 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.

Table 12: Rules defined for the detection of the attacks

Type	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; • FISHY notifies/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 IP 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 cyber-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 URL path 1/HttpAdapter/ 2/XISOAPAdapter/

	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 Ips 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.

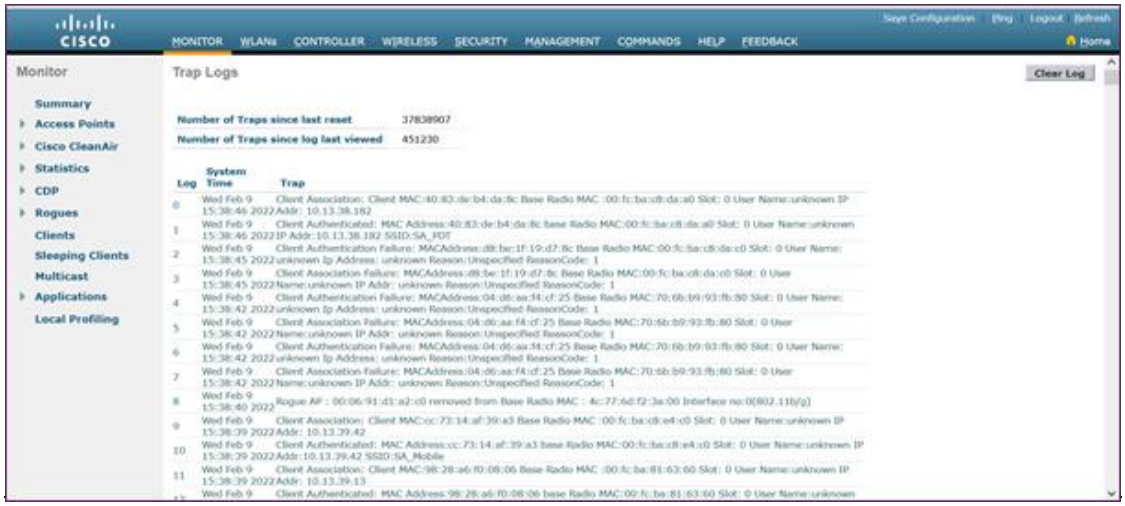


Figure 79: Screenshot of syslog of WLAN Controller sending logs to TIM (XL-SIEM module) – use case scenario 1

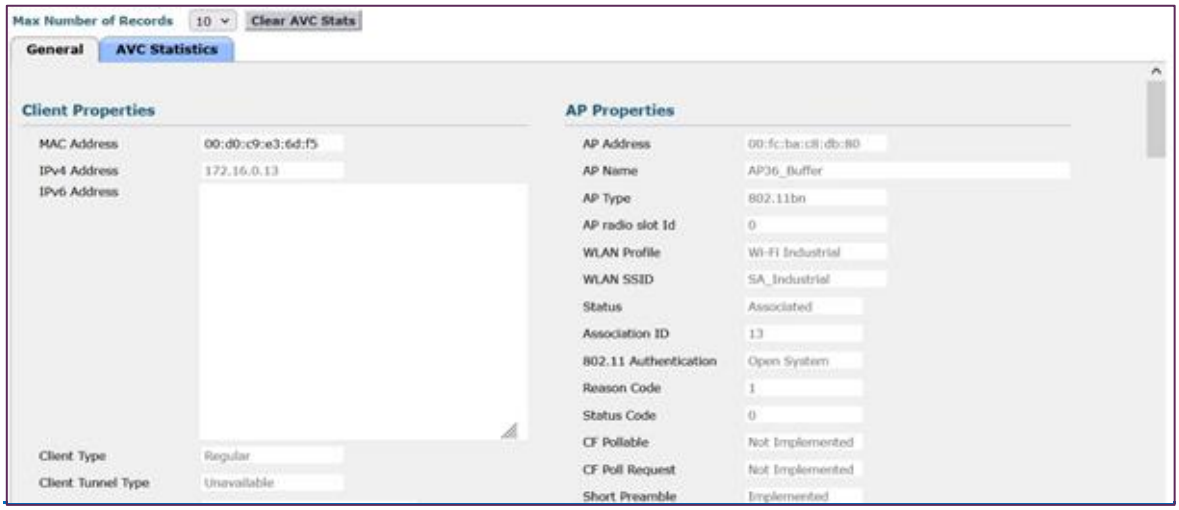


Figure 80: Registered IoT device information set from WLAN Controller to TIM (XL-SIEM module) – use case scenario 1

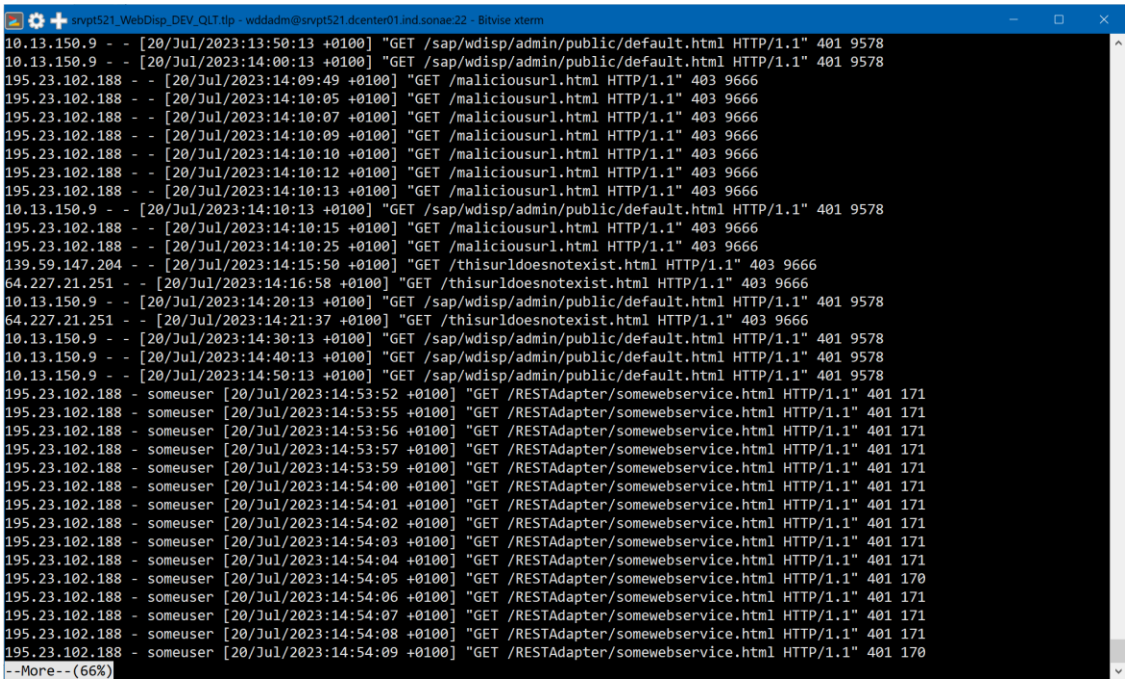


Figure 81: Screenshot of the SAP Web Dispatcher server logs sent to TIM (XL-SIEM module) – use case scenario 2

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

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:

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

Metric ID	Metric description	Type	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

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.

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.

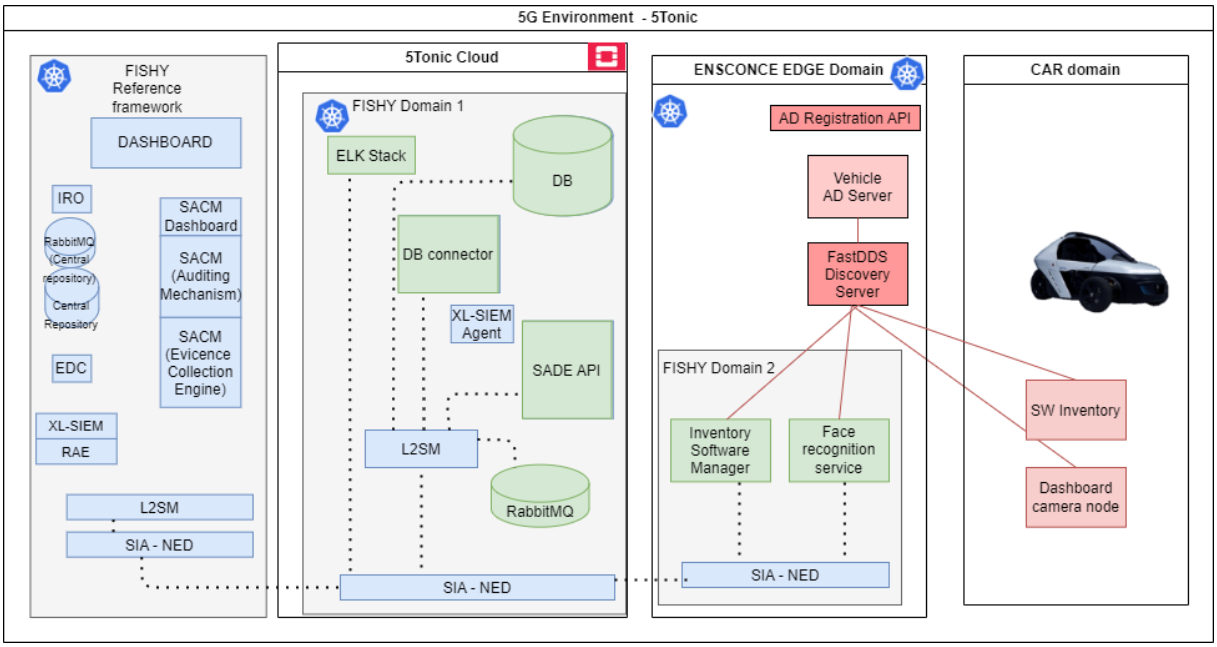


Figure 82: SADE use case deployment.

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}

- 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 **attack modelling according to the ENISA model** 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.

Table 14: ENISA modelling of SADE use case attacks.

	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	**Brute Force – Ghost Car for traffic tampering** (not authorized car started) **Supplier:** LOCAL EDGE OPERATOR	EDGE. The **traffic data, and data shared** between connected cars	**Trusted relationship** (between the drivers and the Edge Traffic manager) **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)	**Social engineering attacks** (not authorized user with stolen credentials trying to activate facial recognition to power on the car using PIN) **Supplier:** DEALER	User credentials, User data	Trusted relationship (between the car, the Edge and the SADE On premise cloud) **Customer:** CAR OWNER	Vehicle

SADE – UC3 SW Patch certification **UC4 SW Patch level correction** **Type 1**	**Malware/code injection** (not validated software) **Suppliers:** MANUFACTURER DEALERS (as main Manufacturers of the vehicle)	Hardware **component's pre-existing software provided by the manufacturer**	**Trusted relationship** (between the drivers and manufacturer) **CUSTOMER:** Car Owners	Vehicles, traffic 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** (car duplicated to receive 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.

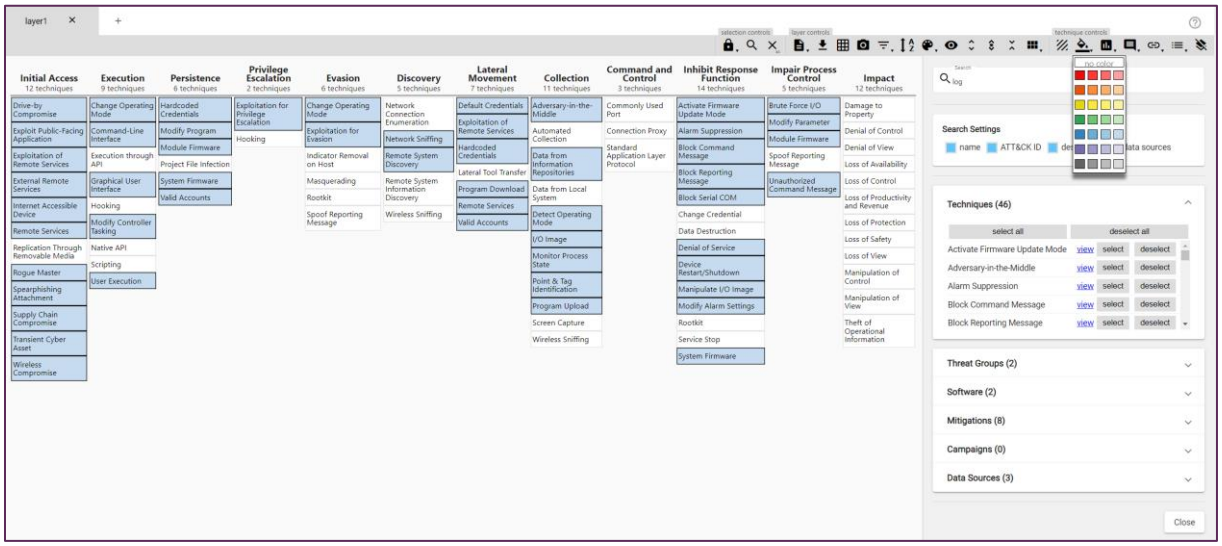


Figure 83: The attacks that can be detected based on logs shown/highlighted in Blue (53 out of 80, i.e. 66%)

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.

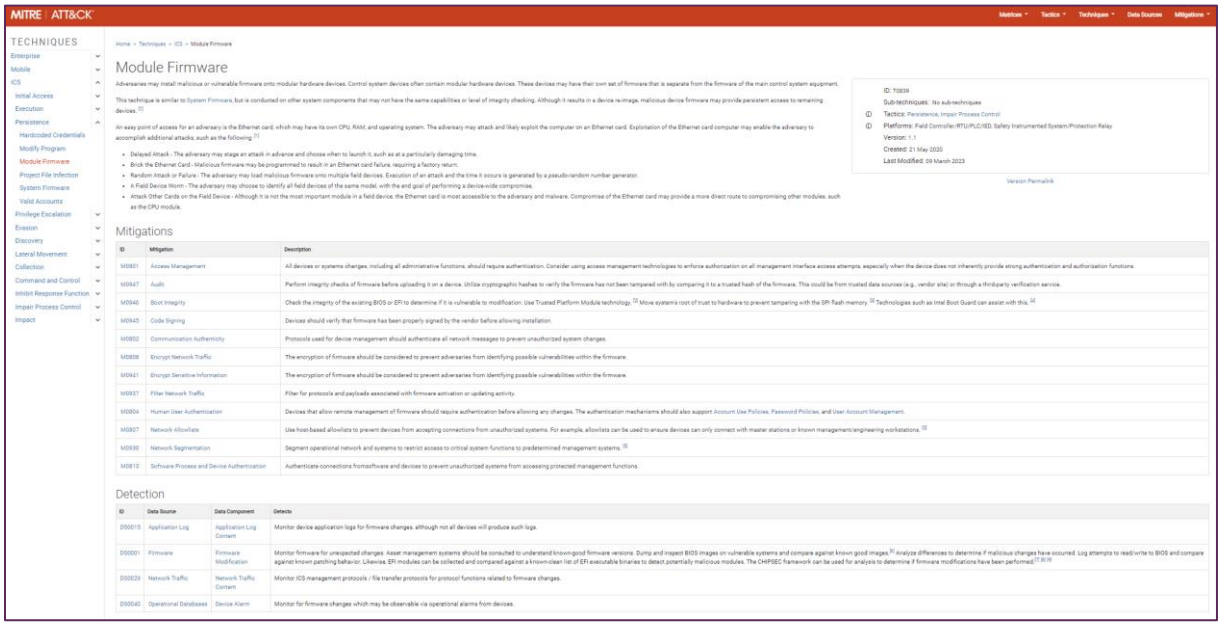
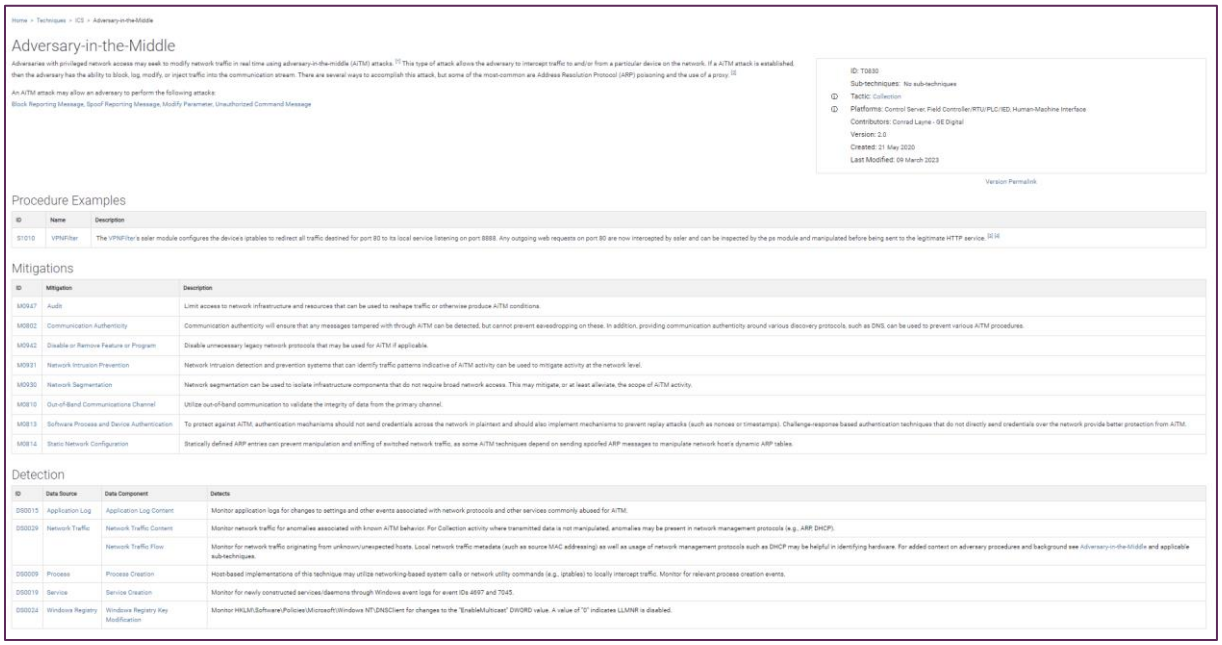


Figure 84: Module firmware threat.



Adversary-in-the-Middle

Adversaries with privileged network access may seek to modify network traffic in real time using adversary-in-the-middle (AITM) attacks.[1] This type of attack allows the adversary to intercept traffic to and/or from a particular device on the network. If a AITM attack is established, then the adversary has the ability to block, log, modify, or inject traffic into the communication stream. There are several ways to accomplish this attack, but some of the most common are Address Resolution Protocol (ARP) poisoning and the use of a proxy.[2]

An AITM attack may allow an adversary to perform the following attacks:
Block Reporting Message, Spoof Reporting Message, Modify Parameter, Unauthorized Command Message

ID: T0830
Sub-techniques: No sub-techniques
Tactic: Collection
Platforms: Control Server, Field Controller/RTU/PLC/IED, Human-Machine Interface
Contributors: Conrad Layne - 9E Digital
Version: 2.0
Created: 21 May 2020
Last Modified: 09 March 2023

Version Permalink

Procedure Examples

ID	Name	Description
S1010	VPNFilter	The VPNFilter's ssler module configures the device's iptables to redirect all traffic destined for port 80 to its local service listening on port 8888. Any outgoing web requests on port 80 are now intercepted by ssler and can be inspected by the ps module and manipulated before being sent to the legitimate HTTP service.[3][4]

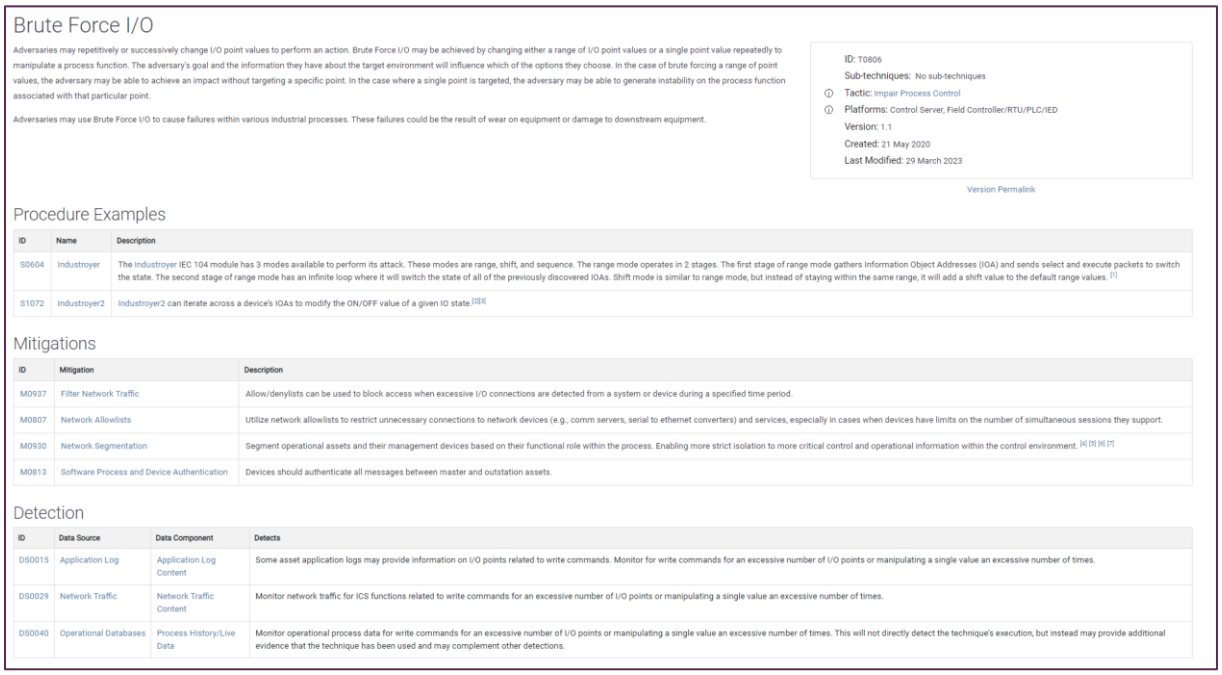
Mitigations

ID	Mitigation	Description
M0947	Audit	Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AITM conditions.
M0802	Communication Authenticity	Communication authenticity will ensure that any messages tampered with through AITM can be detected, but cannot prevent eavesdropping on these. In addition, providing communication authenticity around various discovery protocols, such as DNS, can be used to prevent various AITM procedures.
M0942	Disable or Remove Feature or Program	Disable unnecessary legacy network protocols that may be used for AITM if applicable.
M0931	Network Intrusion Prevention	Network intrusion detection and prevention systems that can identify traffic patterns indicative of AITM activity can be used to mitigate activity at the network level.
M0930	Network Segmentation	Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AITM activity.
M0810	Out-of-Band Communications Channel	Utilize out-of-band communication to validate the integrity of data from the primary channel.
M0813	Software Process and Device Authentication	To protect against AITM, authentication mechanisms should not send credentials across the network in plaintext and should also implement mechanisms to prevent replay attacks (such as nonces or timestamps). Challenge-response based authentication techniques that do not directly send credentials over the network provide better protection from AITM.
M0814	Static Network Configuration	Statically defined ARP entries can prevent manipulation and sniffing of switched network traffic, as some AITM techniques depend on sending spoofed ARP messages to manipulate network host's dynamic ARP tables.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor application logs for changes to settings and other events associated with network protocols and other services commonly abused for AITM.
DS0029	Network Traffic	Network Traffic Content	Monitor network traffic for anomalies associated with known AITM behavior. For Collection activity where transmitted data is not manipulated, anomalies may be present in network management protocols (e.g., ARP, DHCP).
		Network Traffic Flow	Monitor for network traffic originating from unknown/unexpected hosts. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware. For added context on adversary procedures and background see Adversary-in-the-Middle and applicable sub-techniques.
DS0009	Process	Process Creation	Host-based implementations of this technique may utilize networking-based system calls or network utility commands (e.g., iptables) to locally intercept traffic. Monitor for relevant process creation events.
DS0019	Service	Service Creation	Monitor for newly constructed services/daemons through Windows event logs for event IDs 4697 and 7045.
DS0024	Windows Registry	Windows Registry Key Modification	Monitor HKLM\Software\Policies\Microsoft\Windows NT\DNSClient for changes to the "EnableMulticast" DWORD value. A value of "0" indicates LLMNR is disabled.

Figure 85: Adversary in the middle threat.



Brute Force I/O

Adversaries may repetitively or successively change I/O point values to perform an action. Brute Force I/O may be achieved by changing either a range of I/O point values or a single point value repeatedly to manipulate a process function. The adversary's goal and the information they have about the target environment will influence which of the options they choose. In the case of brute forcing a range of point values, the adversary may be able to achieve an impact without targeting a specific point. In the case where a single point is targeted, the adversary may be able to generate instability on the process function associated with that particular point.

Adversaries may use Brute Force I/O to cause failures within various industrial processes. These failures could be the result of wear on equipment or damage to downstream equipment.

ID: T0806
Sub-techniques: No sub-techniques
Tactic: Impair Process Control
Platforms: Control Server, Field Controller/RTU/PLC/IED
Version: 1.1
Created: 21 May 2020
Last Modified: 29 March 2023

Version Permalink

Procedure Examples

ID	Name	Description
S0604	Industroyer	The Industroyer IEC 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 packets 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 staying within the same range, it will add a shift value to the default range values.[1]
S1072	Industroyer2	Industroyer2 can iterate across a device's IOAs to modify the ON/OFF value of a given IO state.[2][3]

Mitigations

ID	Mitigation	Description
M0937	Filter Network Traffic	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 Allowlists	Utilize 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 Segmentation	Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment.[4][5][6][7]
M0813	Software Process and Device Authentication	Devices should authenticate all messages between master and outstation assets.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Some asset application logs may provide information on I/O points related to write commands. Monitor for write commands for an excessive number of I/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 excessive number of times.
DS0040	Operational Databases	Process History/Live Data	Monitor operational process data for write commands for an excessive number of I/O points or manipulating a single value an excessive number of times. This will not directly detect the technique's execution, but instead may provide additional evidence that the technique has been used and may complement other detections.

Figure 86: Brute force threat

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:

Table 16: Success probability assessment for potential attacks

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

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.

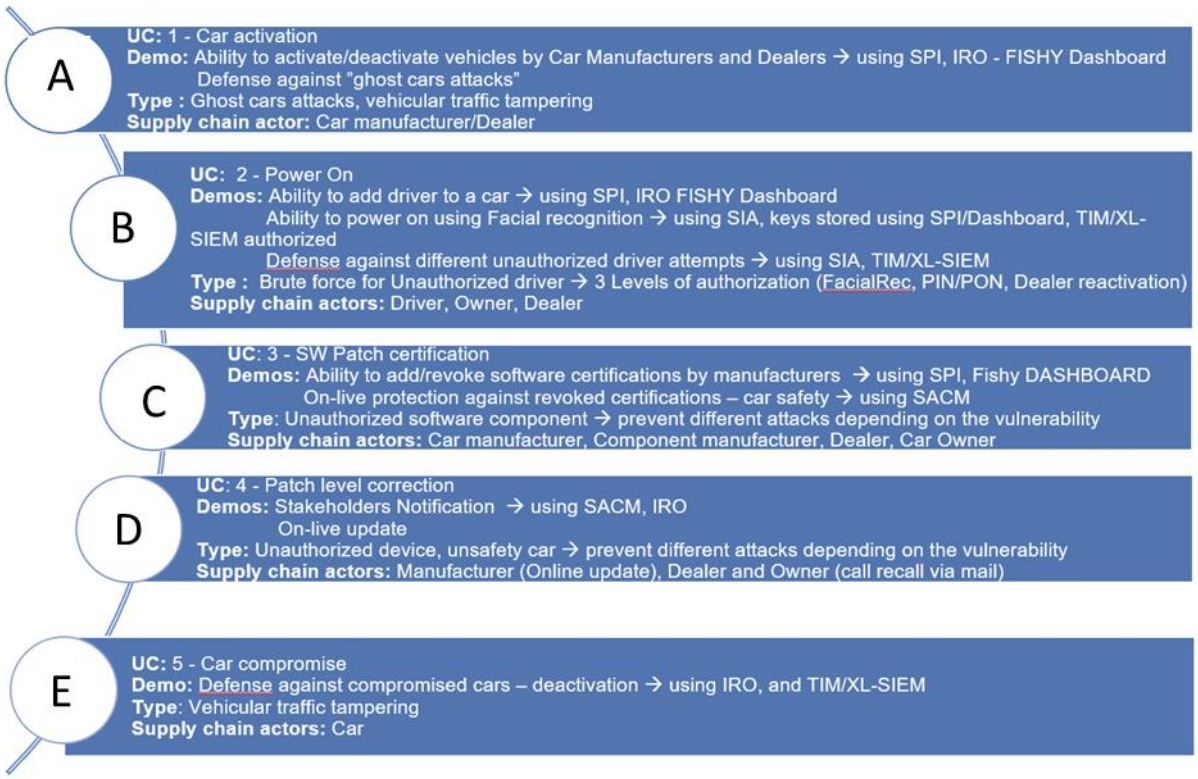


Figure 87: SADE use cases

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.

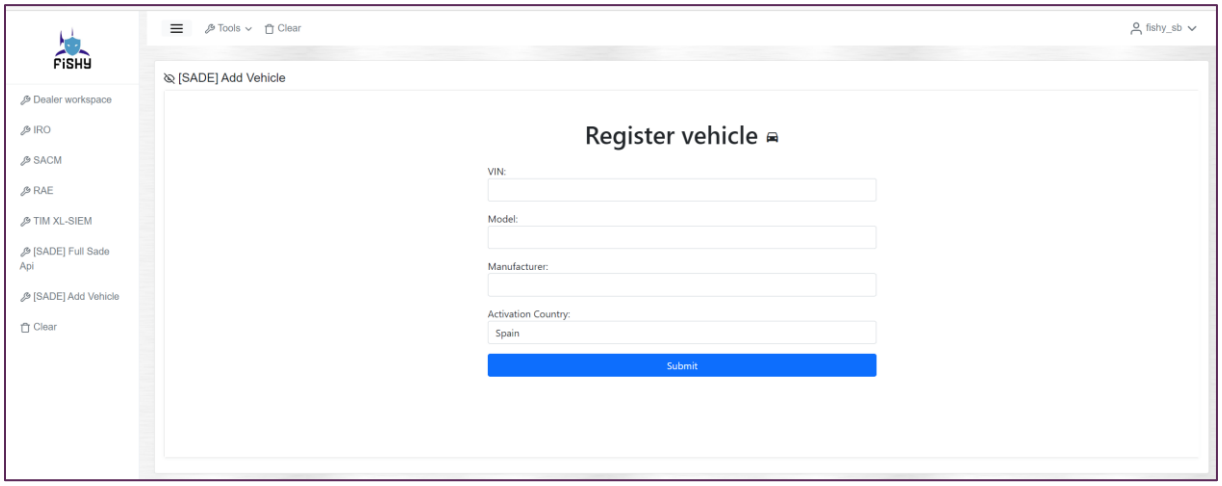


Figure 88: Dealer's fishy dashboard workspace. With the *add vehicle* form (fishy_sb user is a dealer)

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

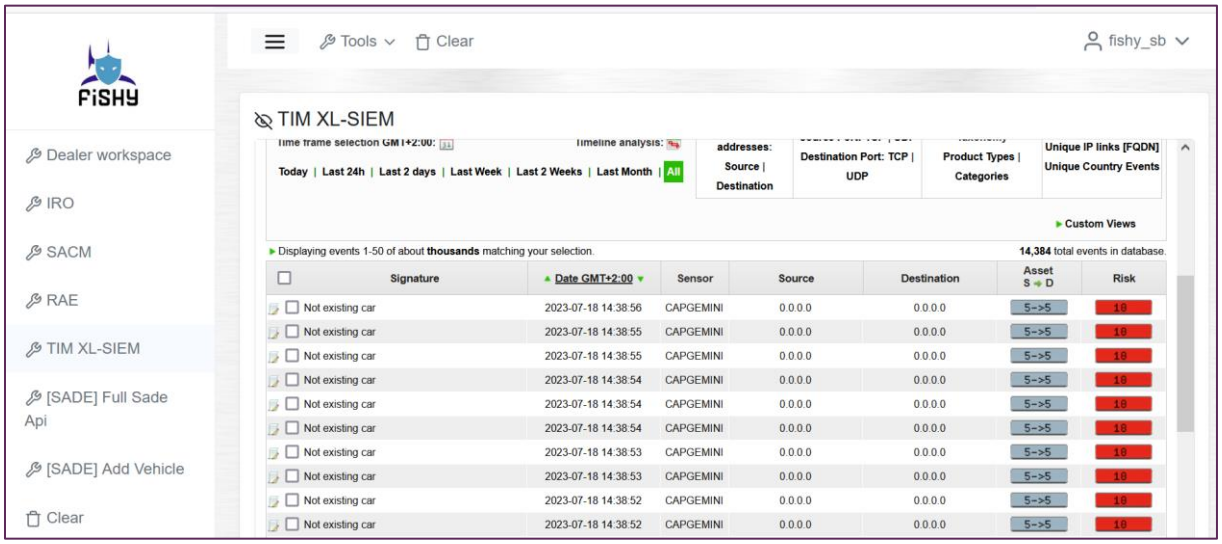


Figure 90: Not existing car events in XL-SIEM dashboard.

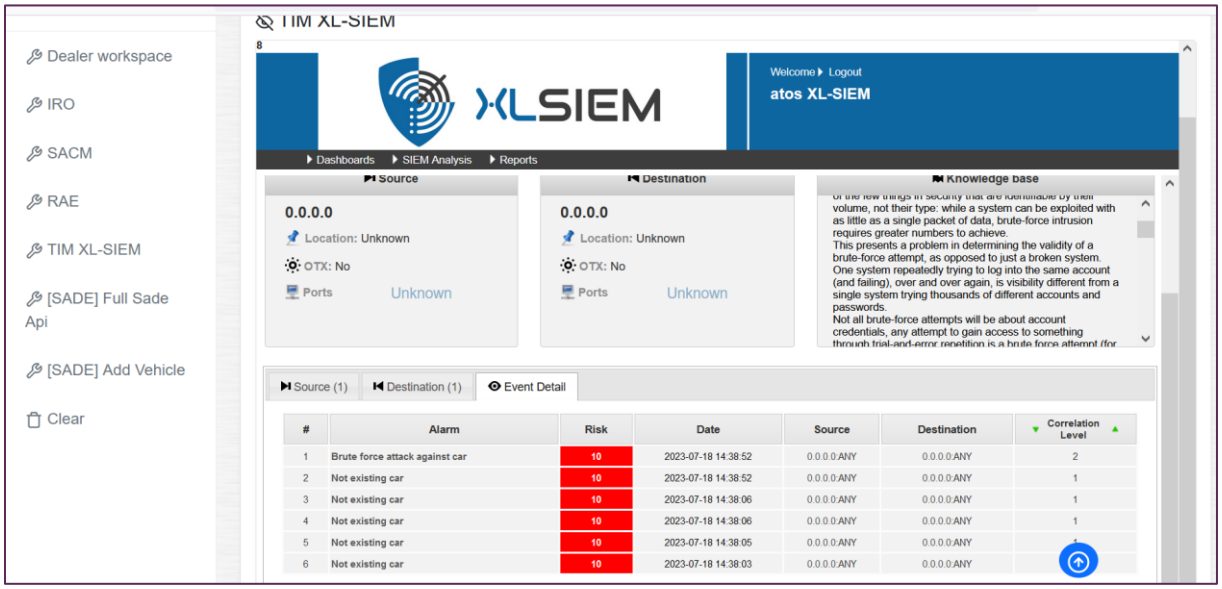


Figure 91: Brute force attack alarm.

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.

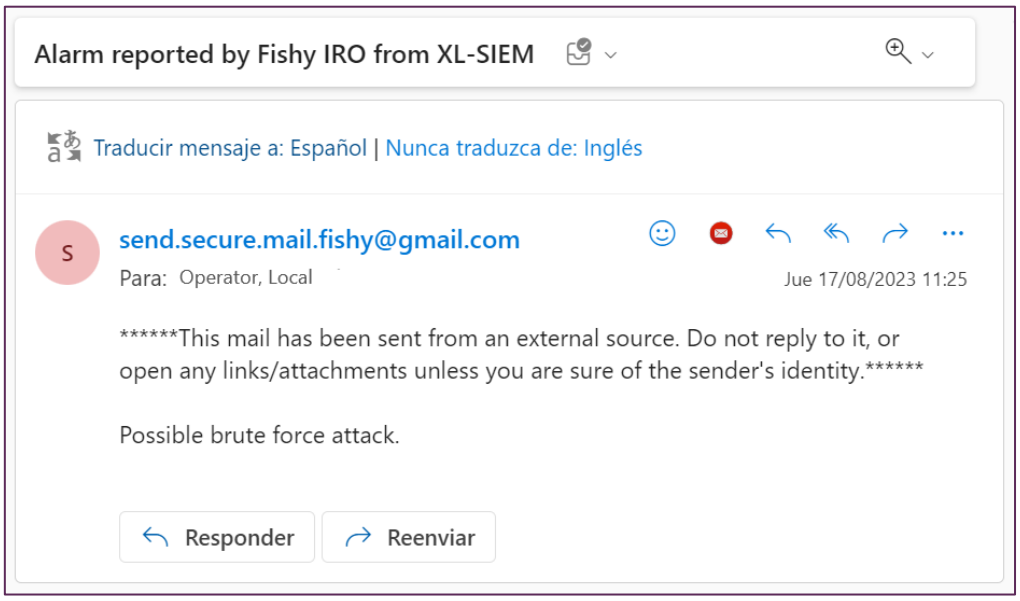


Figure 92. Mail received by Local Operator.

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.

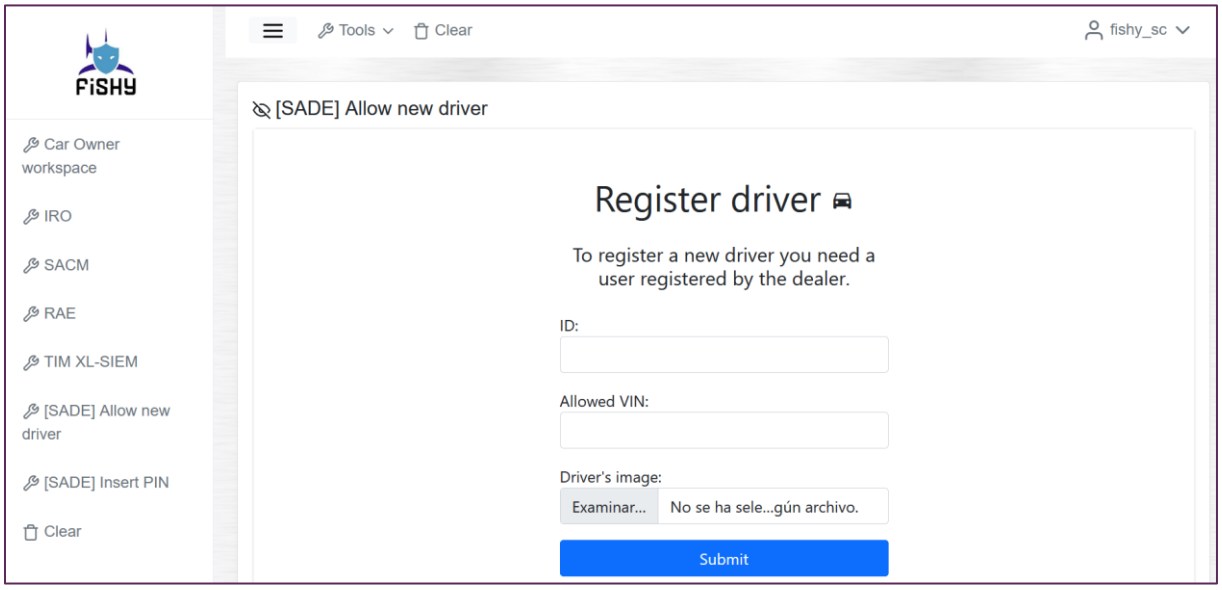


Figure 93: Allow new driver form. Only available for car owner (fishy_sc)

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.

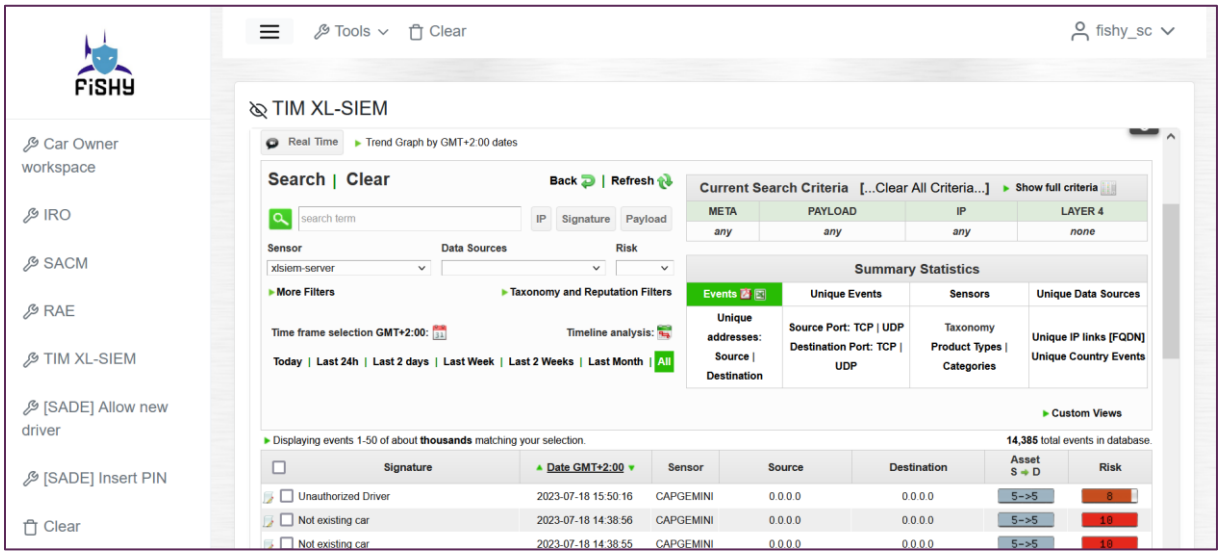


Figure 95: Unauthorized driver event.

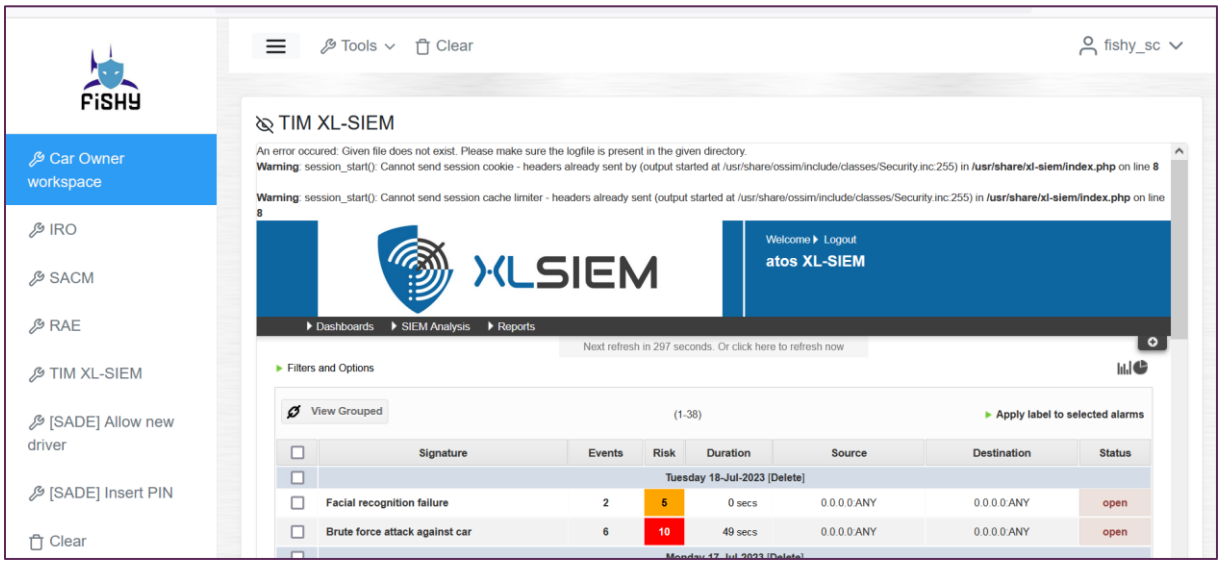


Figure 96: First unauthorized driver alarm.

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.

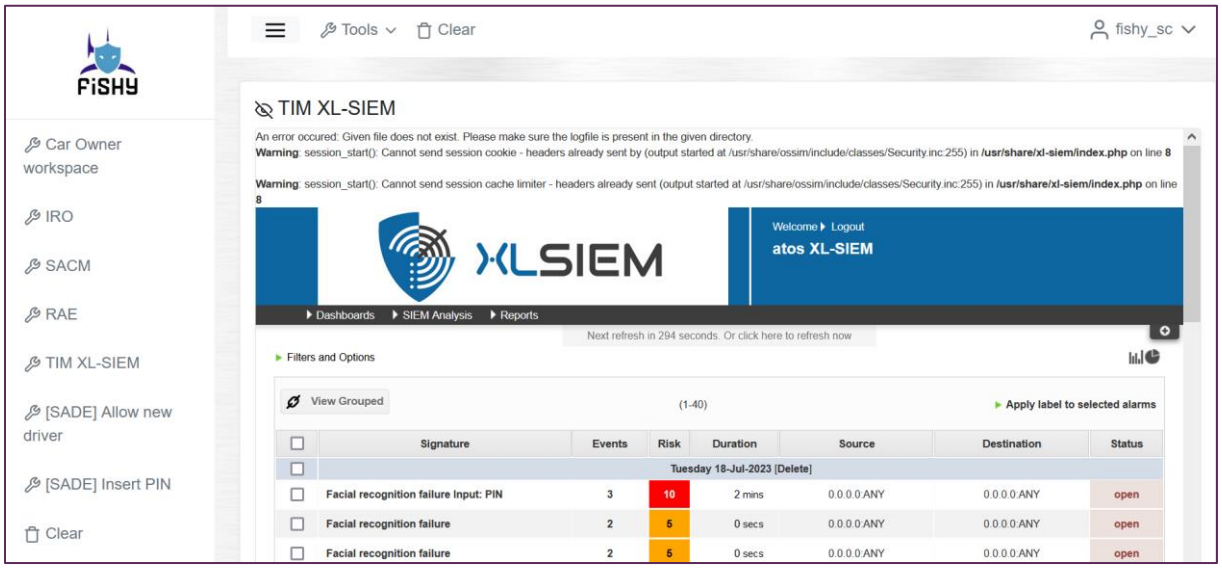


Figure 97: Second unauthorized driver alarm à Pin blocked alarm

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.

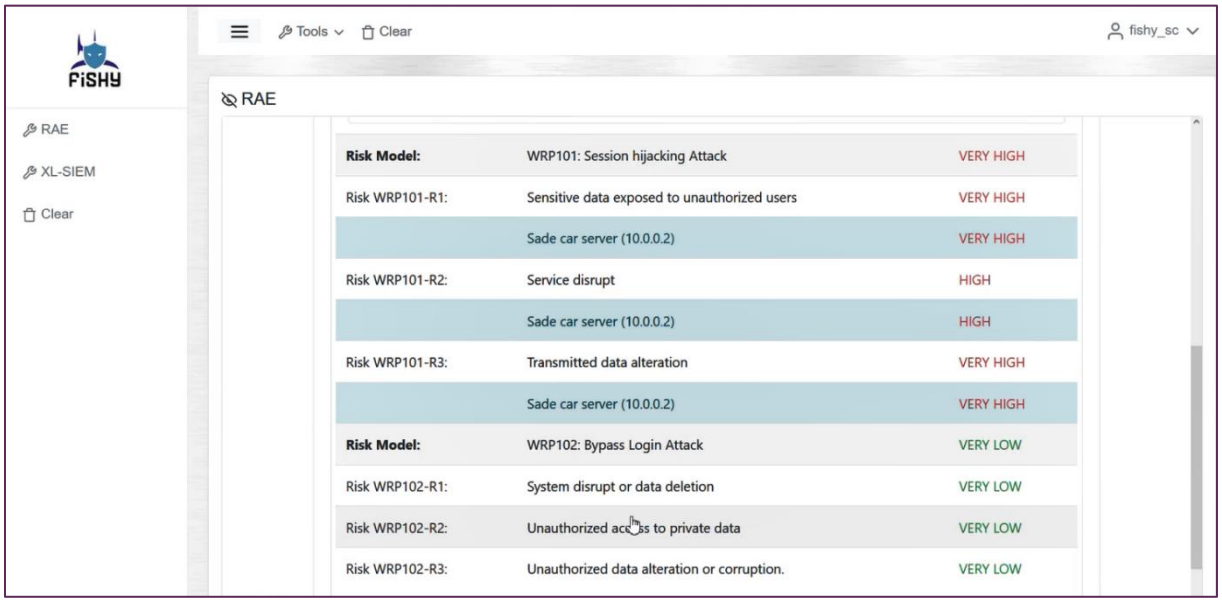


Figure 98: Qualitative risk analysis.

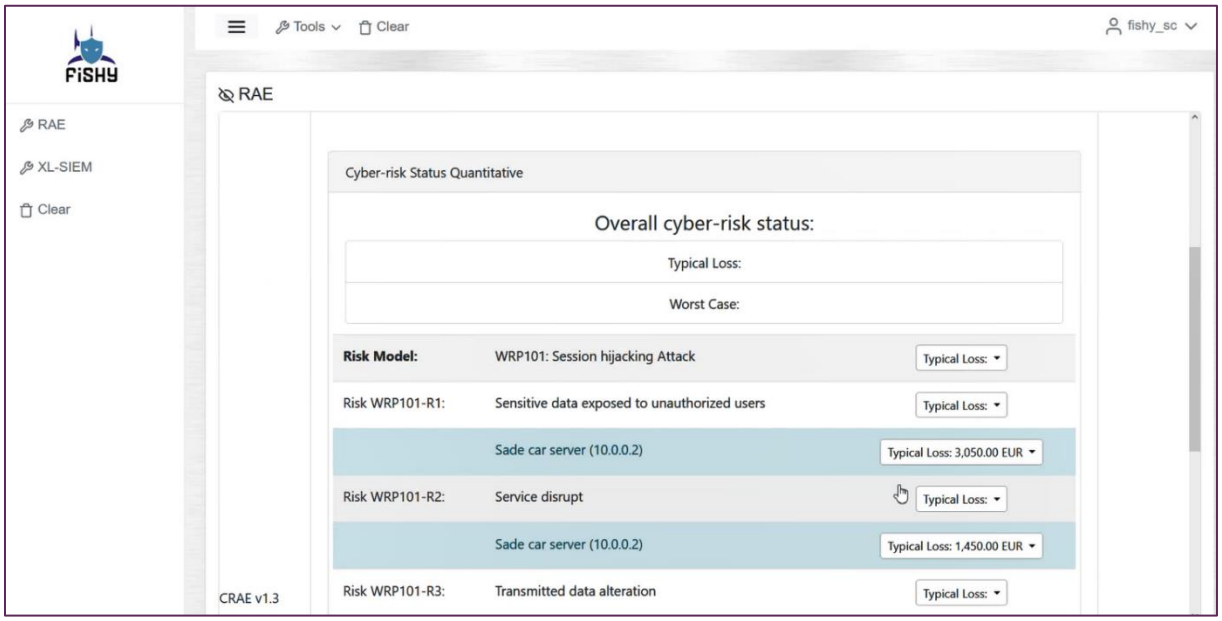


Figure 99: Quantitative risk analysis.

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.

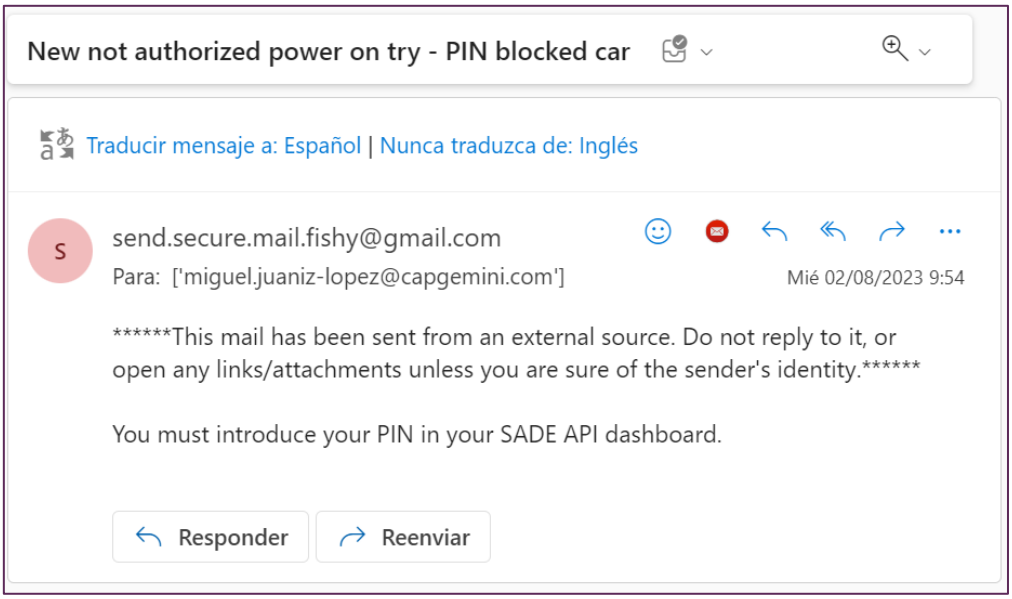


Figure 100: Mail telling the allowed drivers to input its PIN.

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.

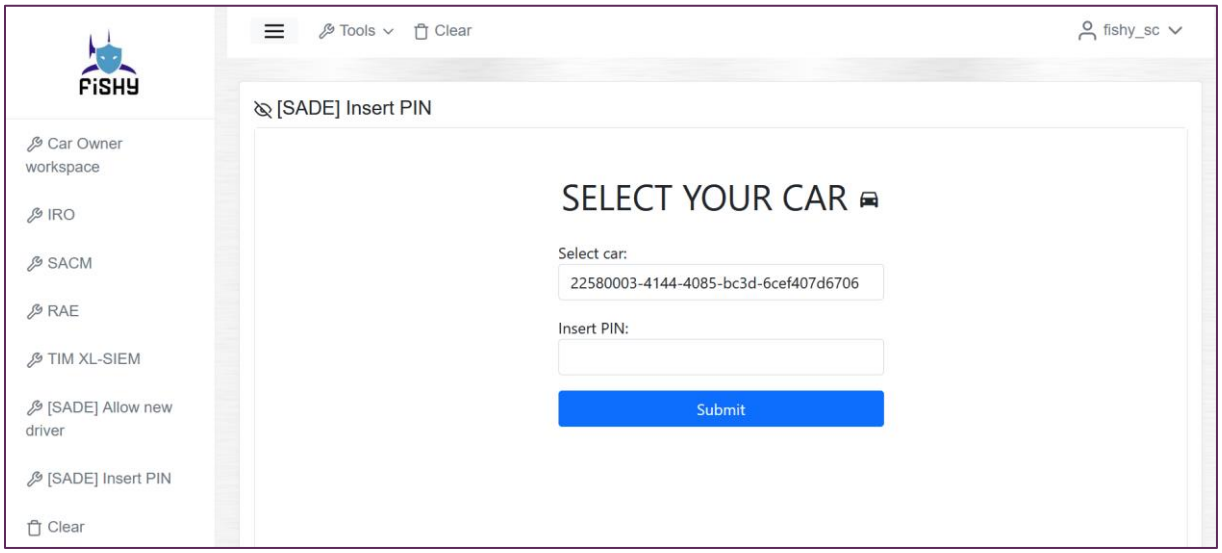


Figure 101: Insert PIN form in the car owner workspace in FISHY dashboard.

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

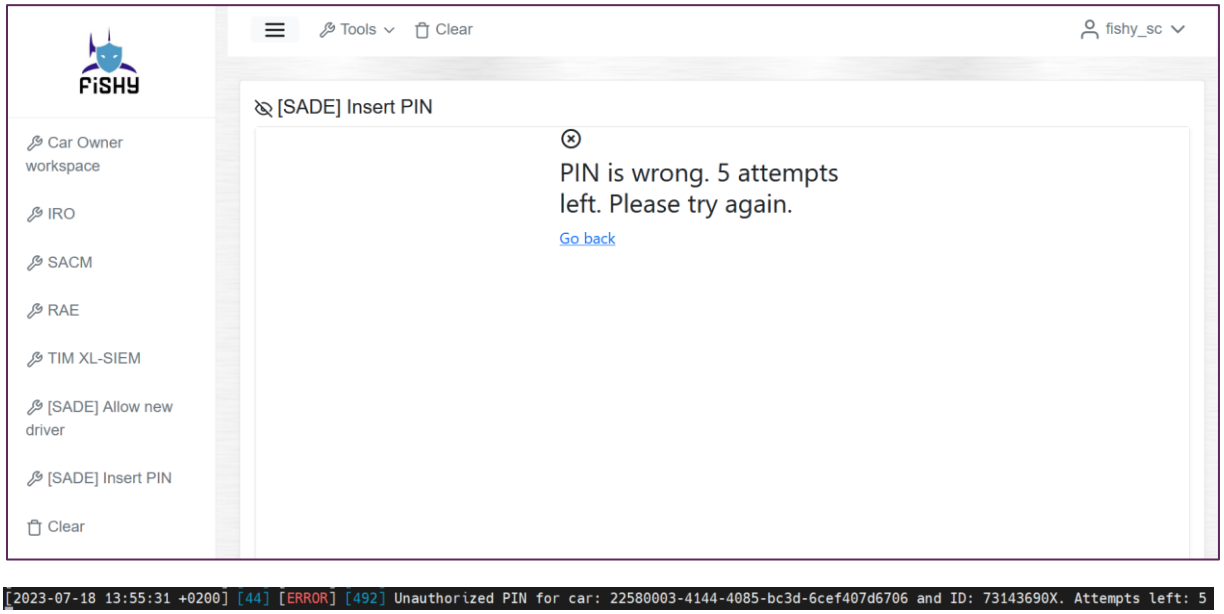


Figure 102: Unauthorized PIN error

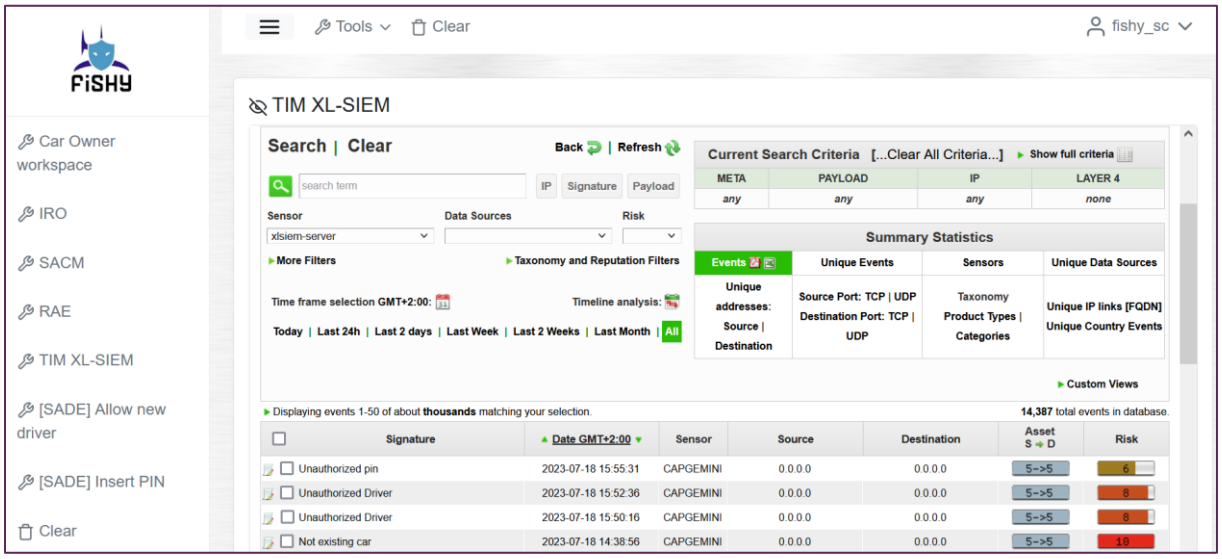


Figure 103: The evant of unauthorized PIN error as shown in the dashboard.

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.

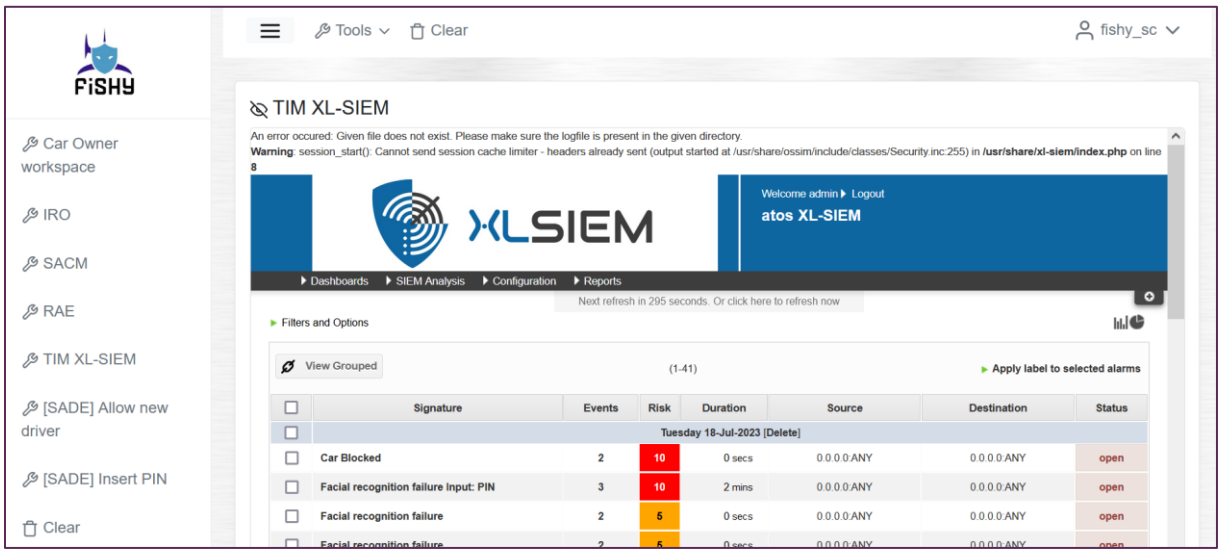


Figure 104: Car blocked alarm.

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.

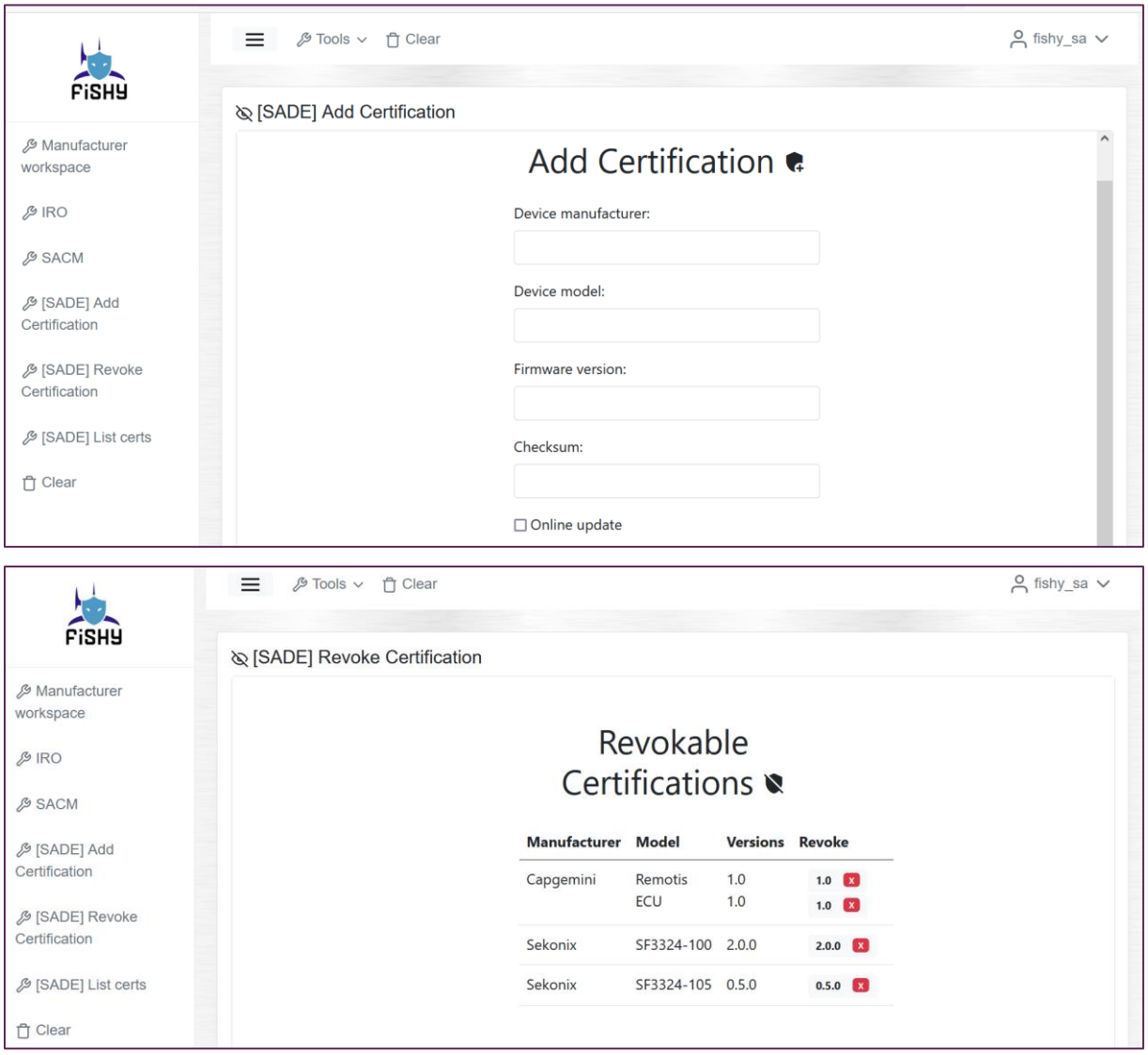


Figure 105: Certification management in the manufacturer workspace.

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

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.

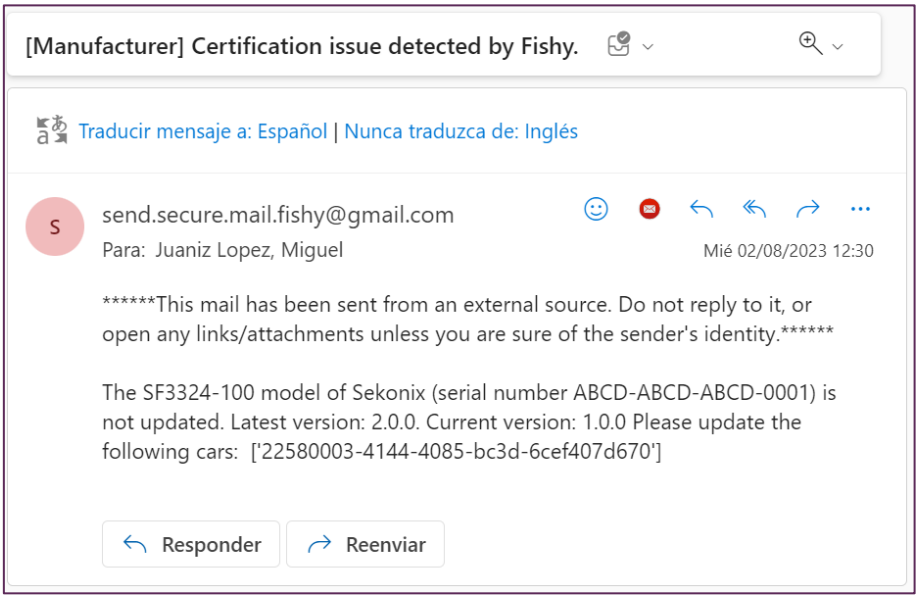


Figure 106: Mail asking manufacturer to update an IoT device online.

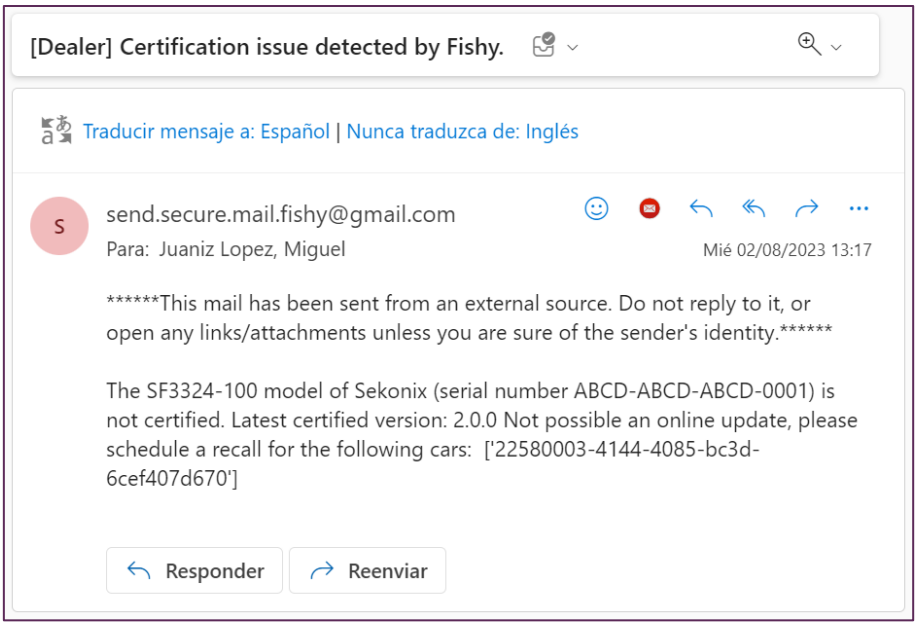


Figure 107: Mail asking dealer to schedule a recall to update components offline.

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.

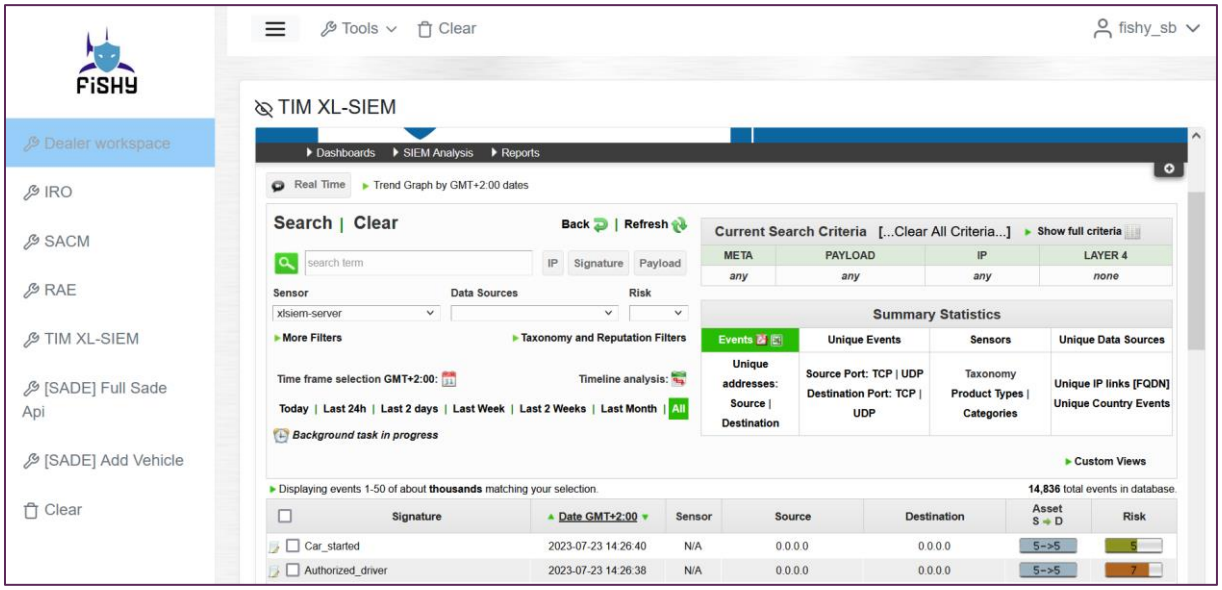


Figure 108: Normal workflow of a vehicle power on.

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.

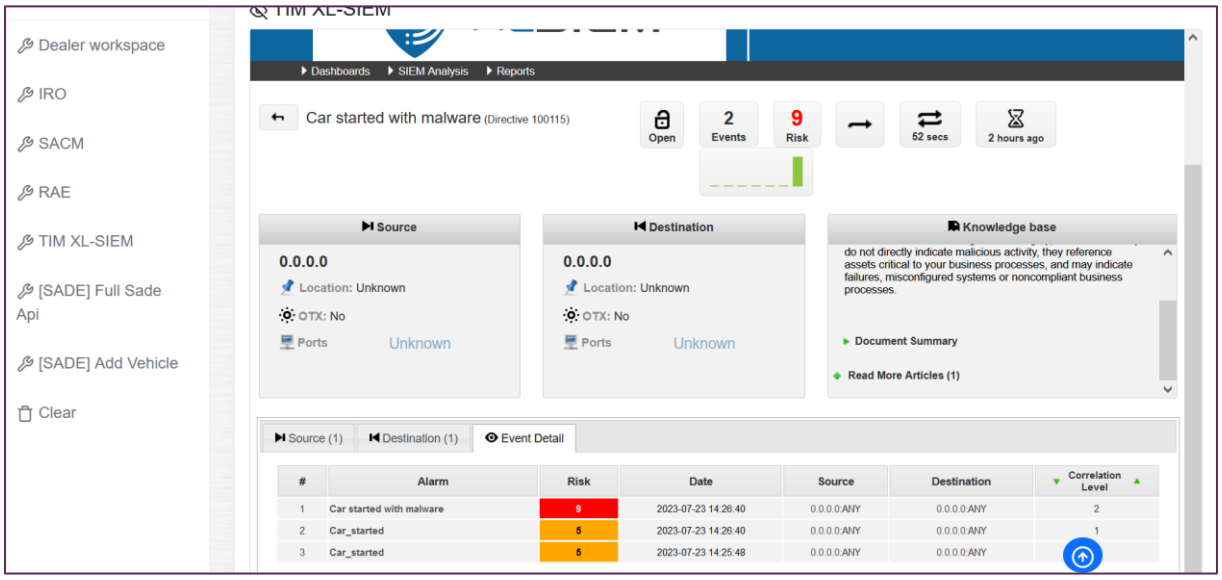


Figure 109: Possible malware alarm.

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

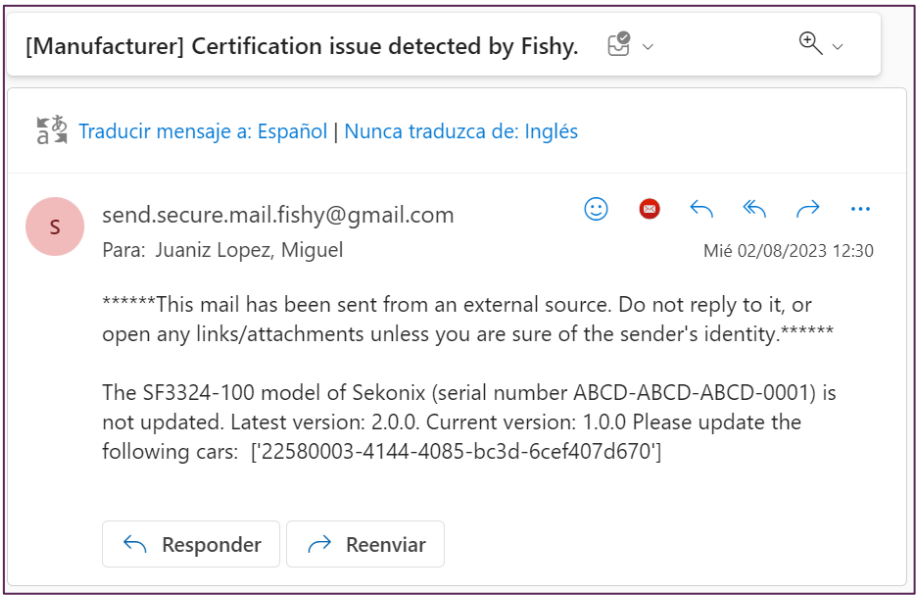


Figure 110: Mail asking manufacturer to update an IoT device online.

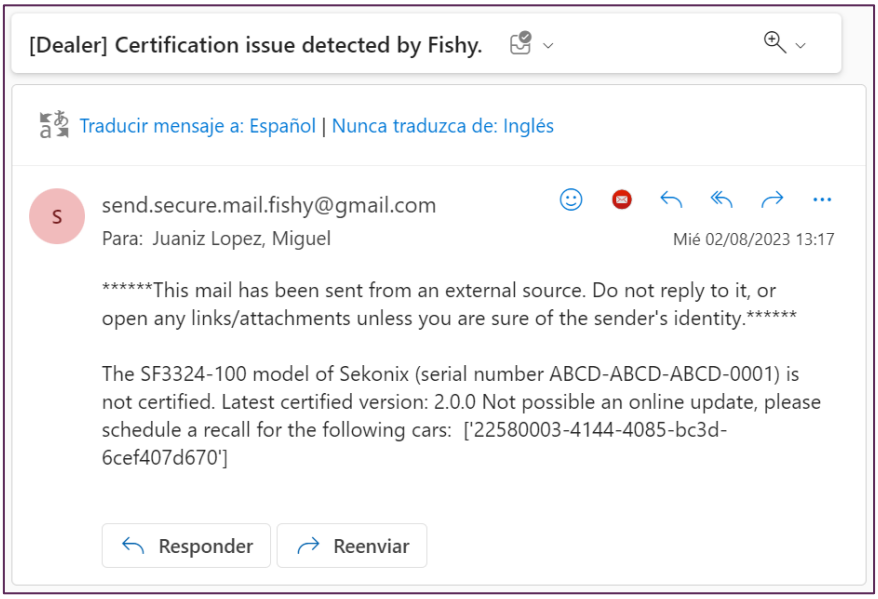


Figure 111: Mail asking dealer to schedule a recall to update components offline.

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.

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

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

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

	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	Iot 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	

```
{
”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 theFISHY 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

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.
  - **RULE:**
    - 5 x not existing car log → send mail to local operator.
    - [POST] https://192.168.0.103:5000/api/actions/report_local_operator {'subject':'', 'message': ''}
- **UC2.1.** Attempt to power on by unauthorized driver.
  - **RULE:**
    - 2 x unauthorized driver log → send mail to owner.
    - [POST] https://192.168.0.103:5000/api/actions/send_mail {'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] https://192.168.0.103:5000/api/actions/send_mail {'VIN': 'vin_number[uuid4]', 'subject':'', 'message': ''}
- **UC5.** Duplicated behicle for traffic tampering.
  - **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.

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:

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

Metric ID	Metric description	Type	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

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:

Key message 1. **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.

Key message 2. **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.

Key message 3. **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.

Key message 4. **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.

Key message 5. **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.

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

FISHY Component	Components	F2F	WBP Trust	SADE
SPI	Identity Manager	YES	YES	YES
	Data Management	YES	YES	YES
TIM	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

Key message 6. **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.

Key message 7. **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.

6 Conclusions

In this document we have described the FISHY IT-2 deployments in the infrastructures of the three-pilot 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.**

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] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[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/

8 Annex: User Manual

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

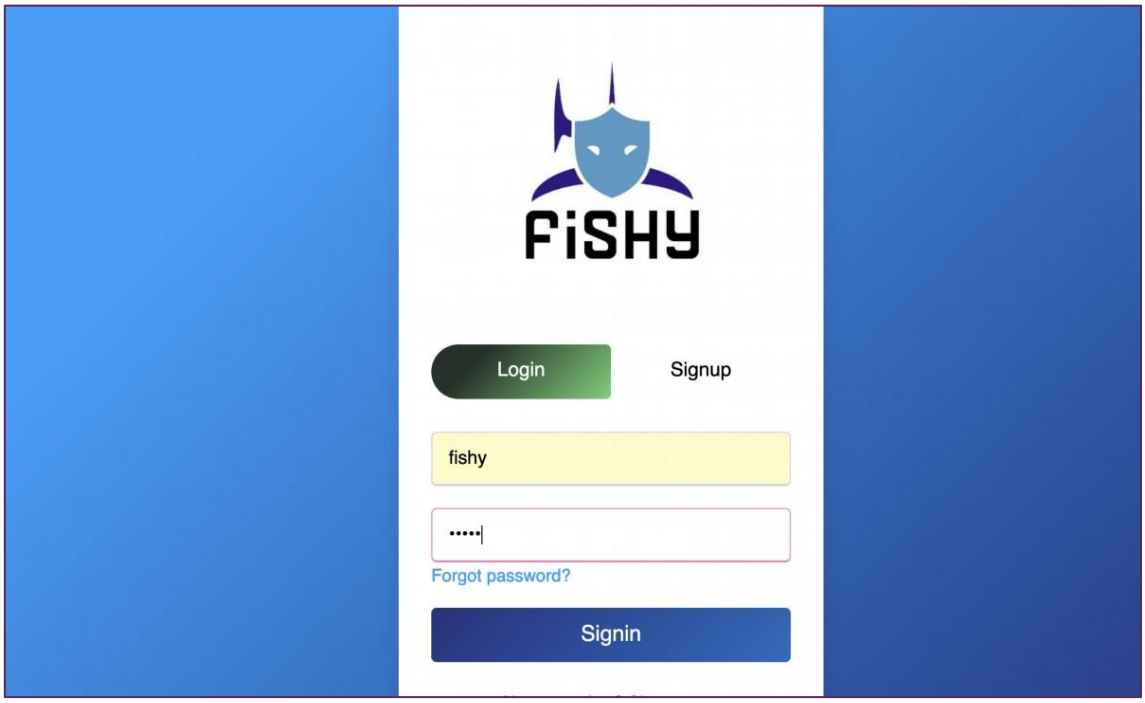


Figure 113: Accessing FISHY dashboard

When accessing, the main page is the IRO.

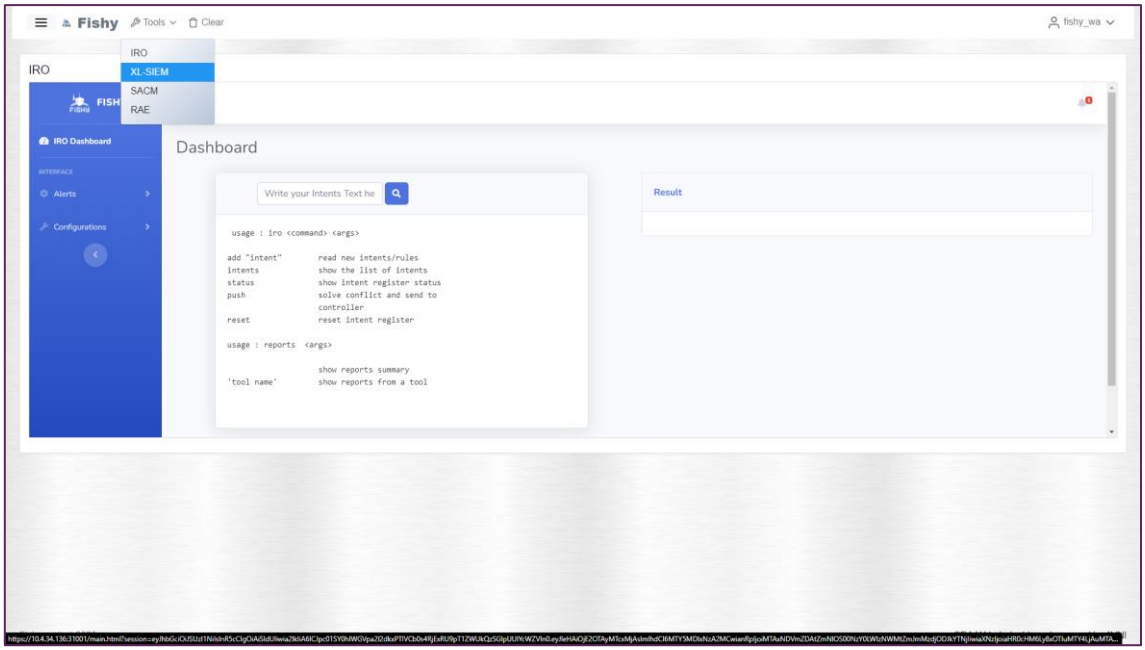


Figure 114: Main page in FISHY dashboard

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.

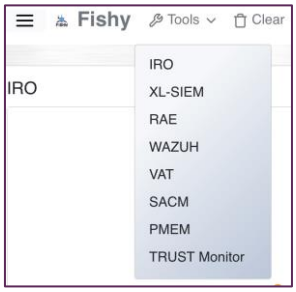


Figure 115: FISHY tools in FISHY dashboard

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.

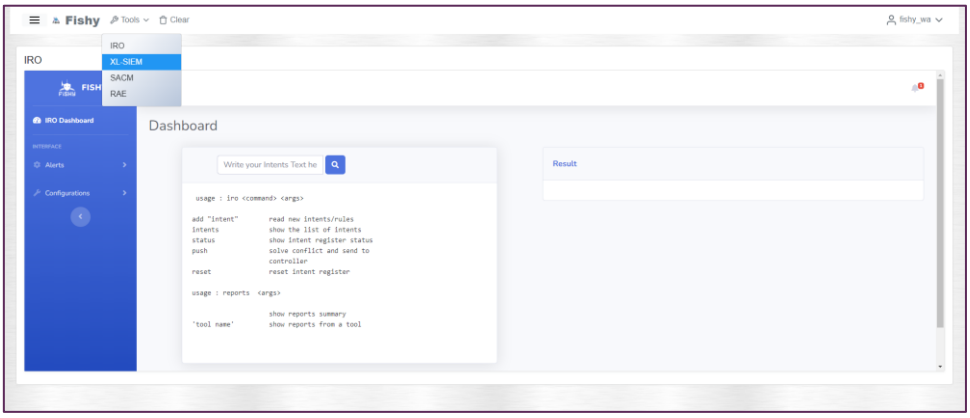


Figure 116: Through the FISHY dashboard, we are able to select the XL-SIEM.

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.

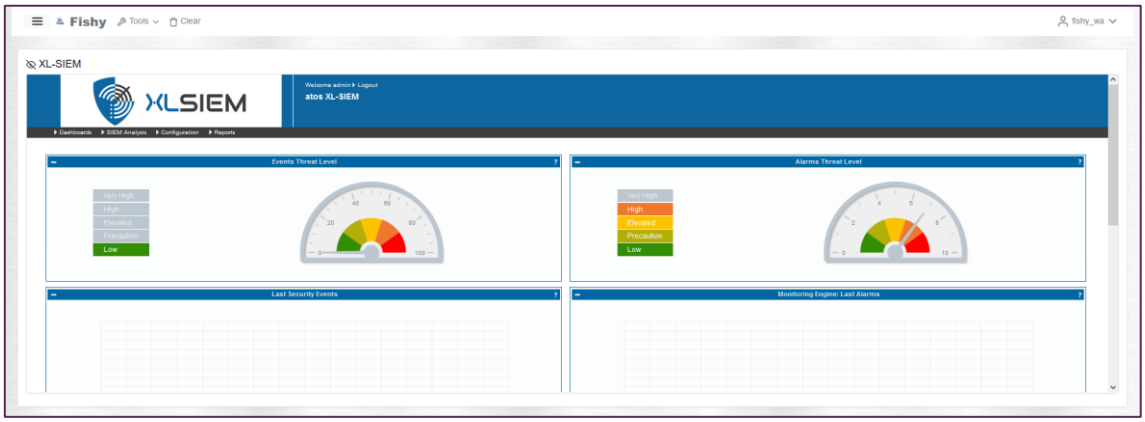


Figure 117: Main view [1] At first glance, we can observe a threat level based on the events and alarms generated in the recent hours and we also have a summary of the alarms and statistics generated in the last few hours.

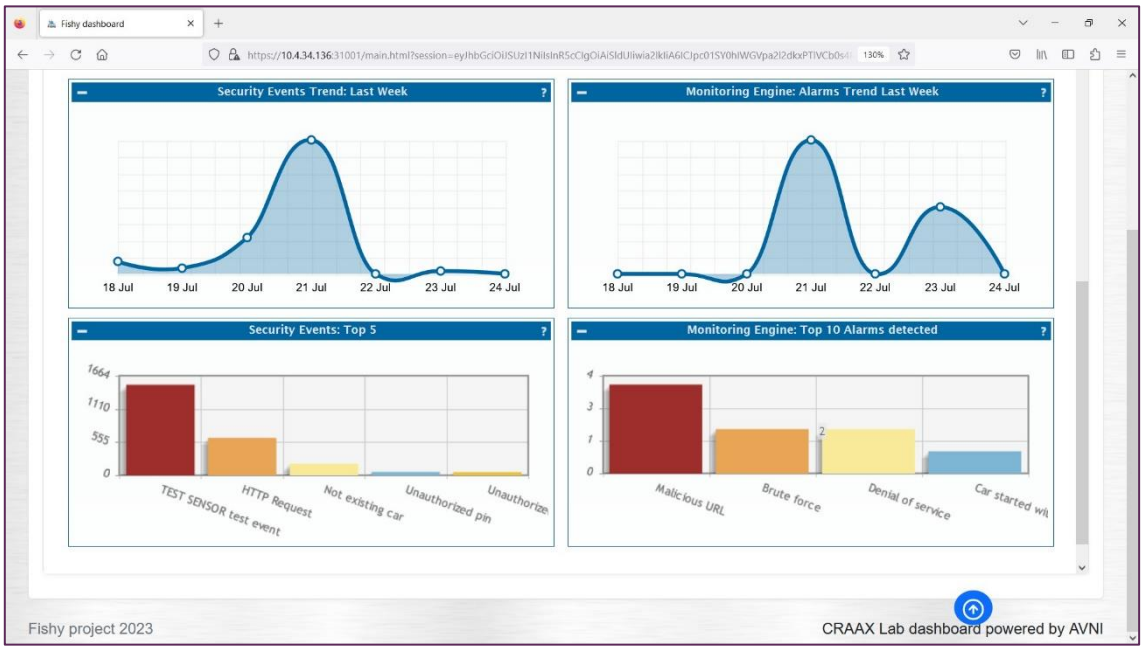


Figure 118: Statistics on the detected attacks are provided.

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.

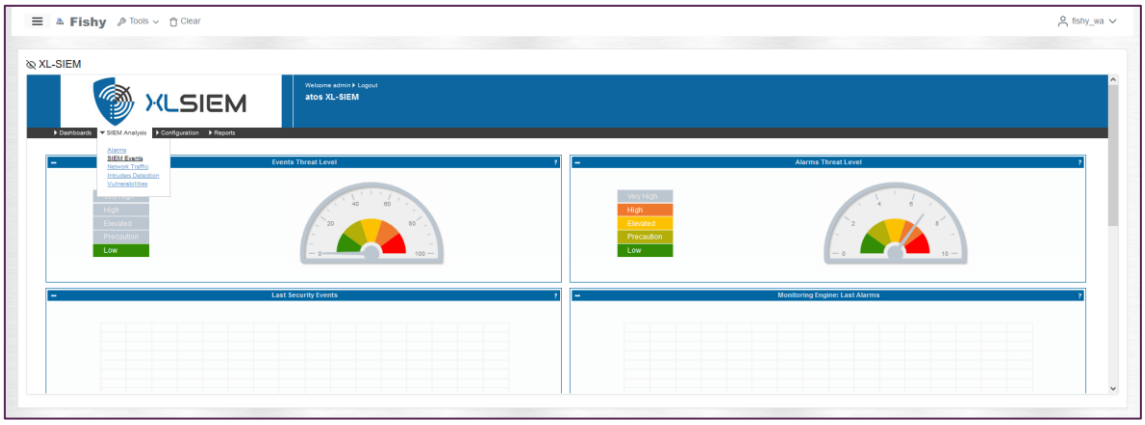


Figure 119: We use the navigation menu of the XL-SIEM to view the list of events.

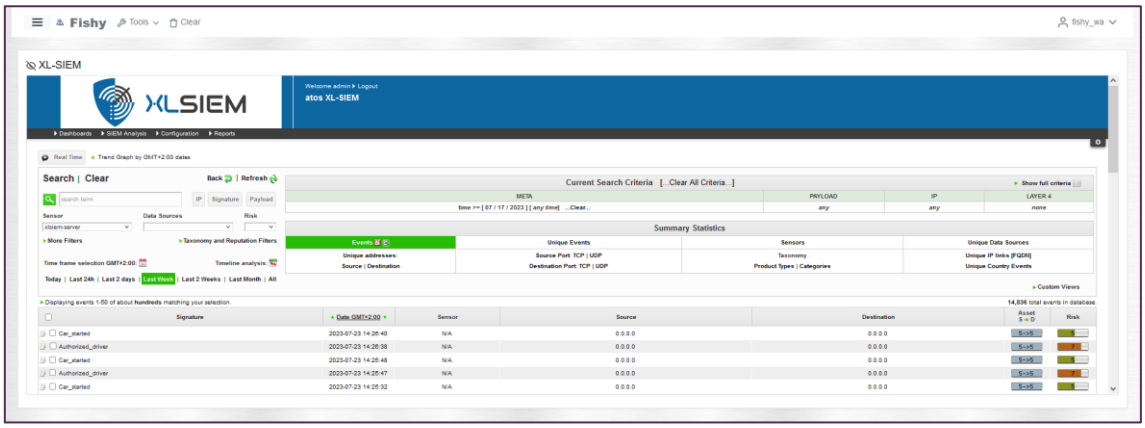


Figure 120: Events List

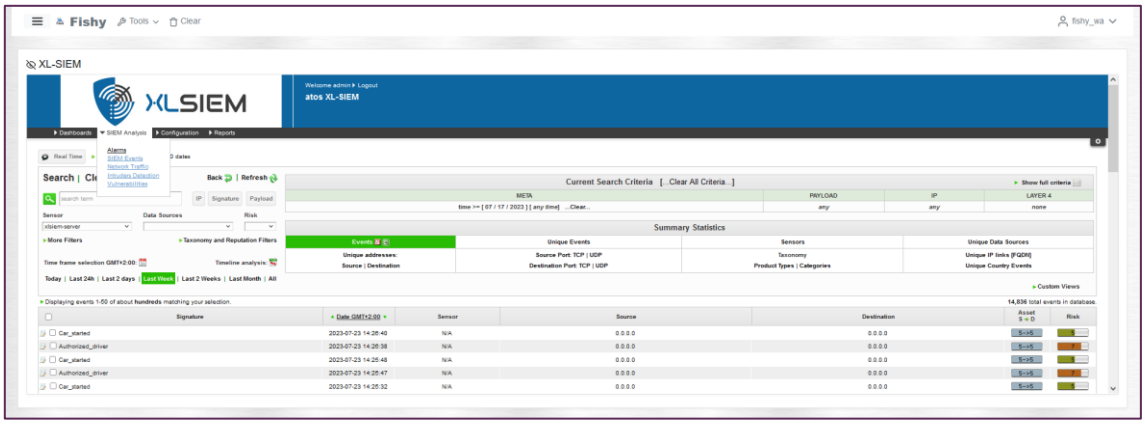


Figure 121:We use the navigation menu of the XL-SIEM to view the list of alarms.

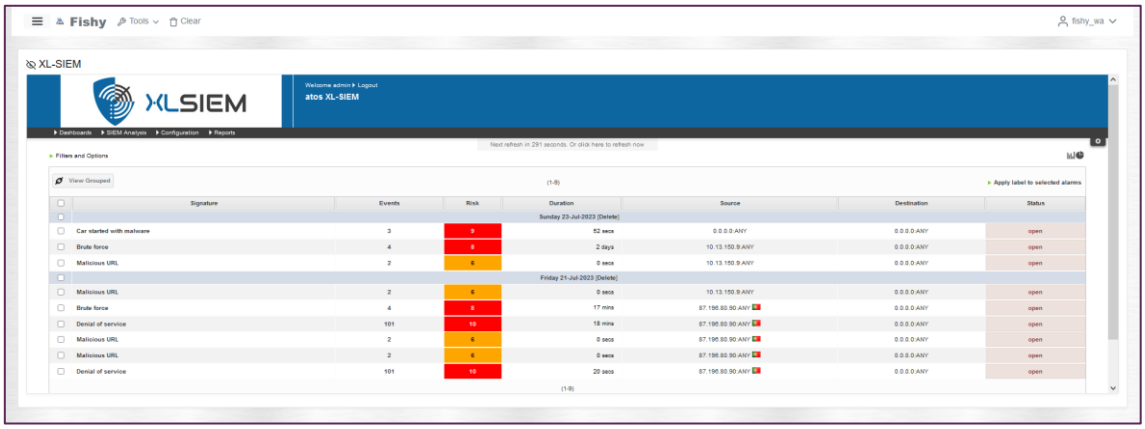


Figure 122:Alarms List

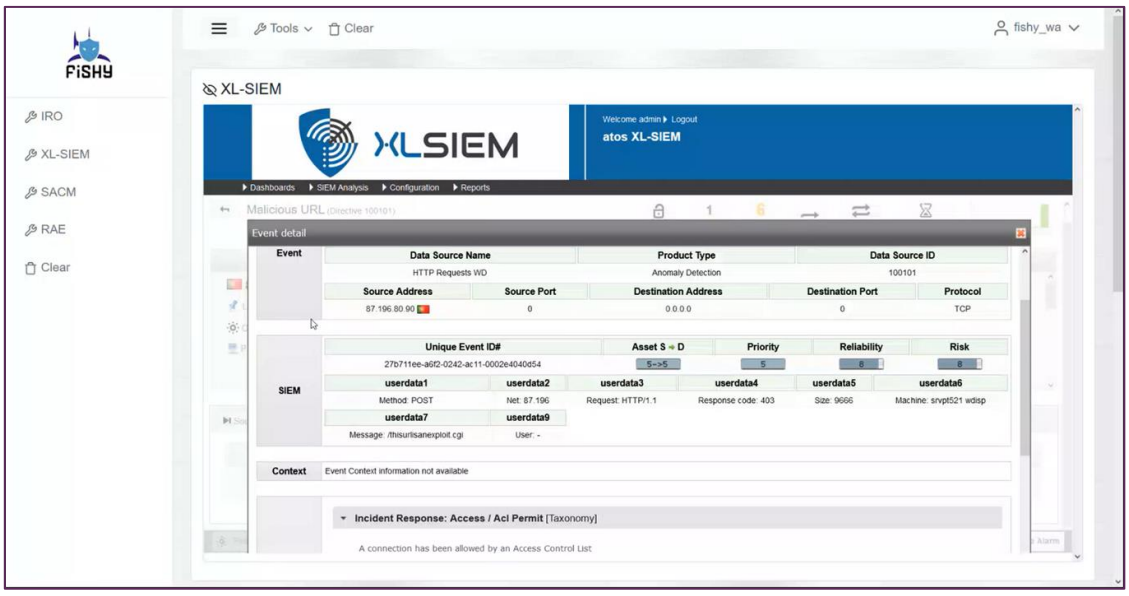


Figure 123:Alarms details

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.

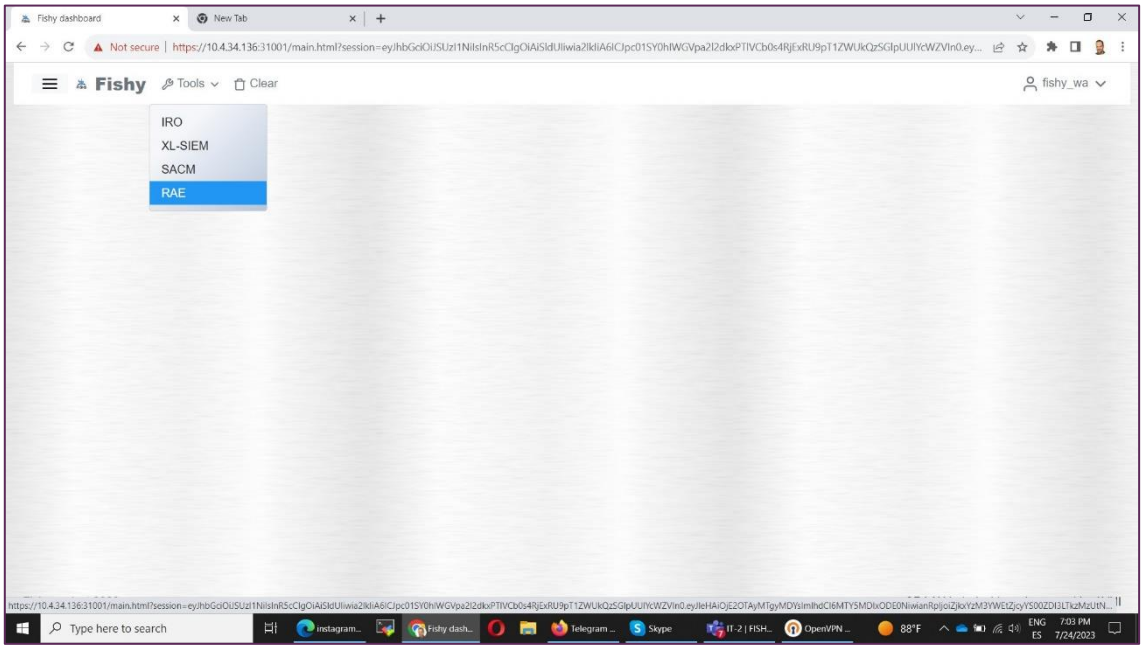


Figure 124: RAE selection from the landing page

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*.

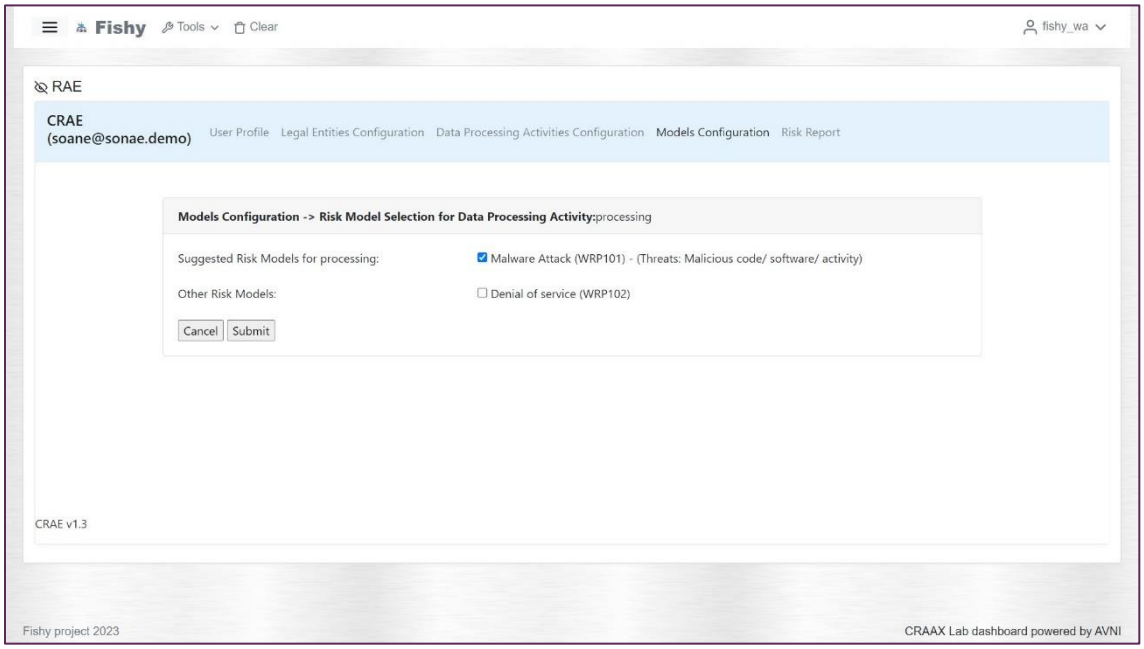


Figure 125. The user can choose a risk model

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

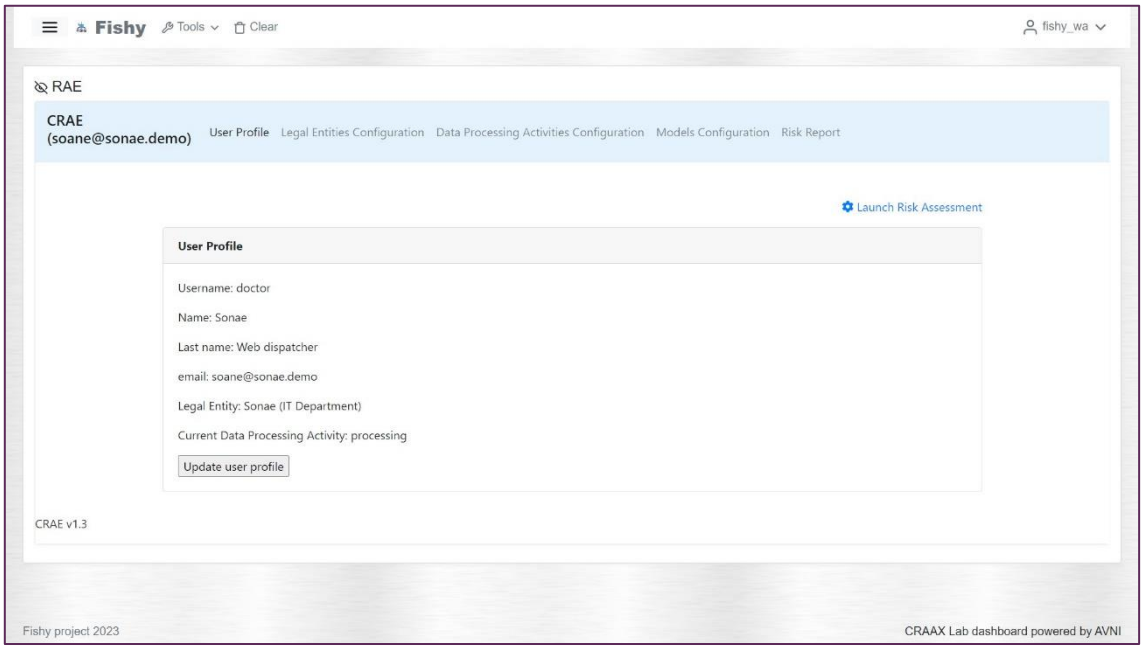


Figure 126:Main RAE view with basic info.

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.

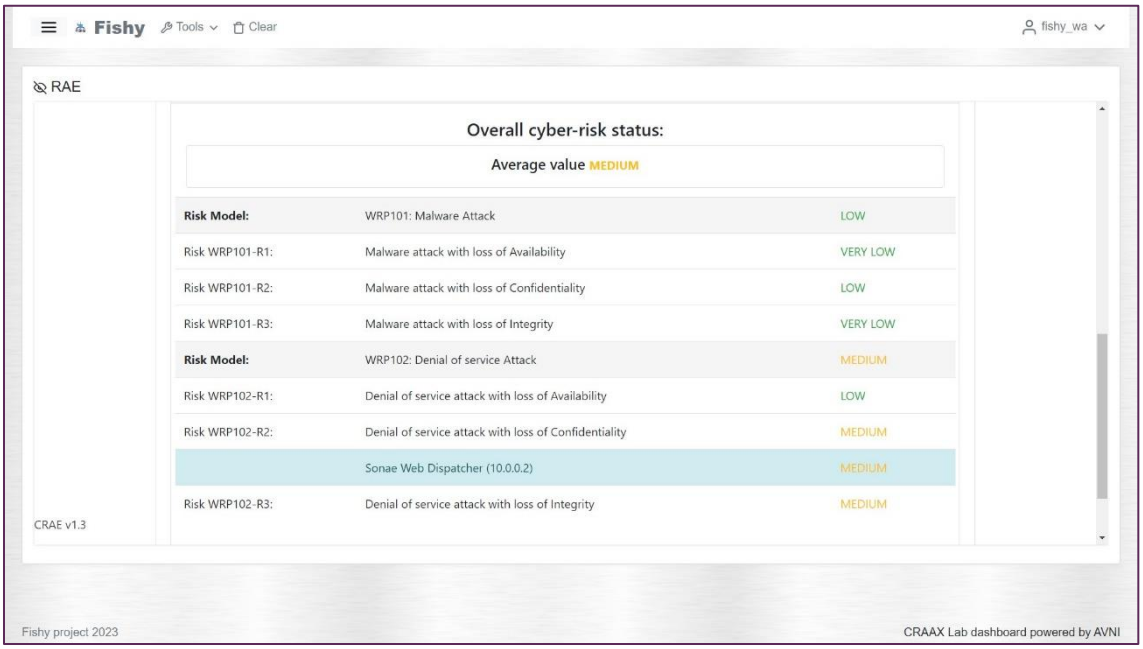


Figure 127. RAE qualitative risk assessment

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

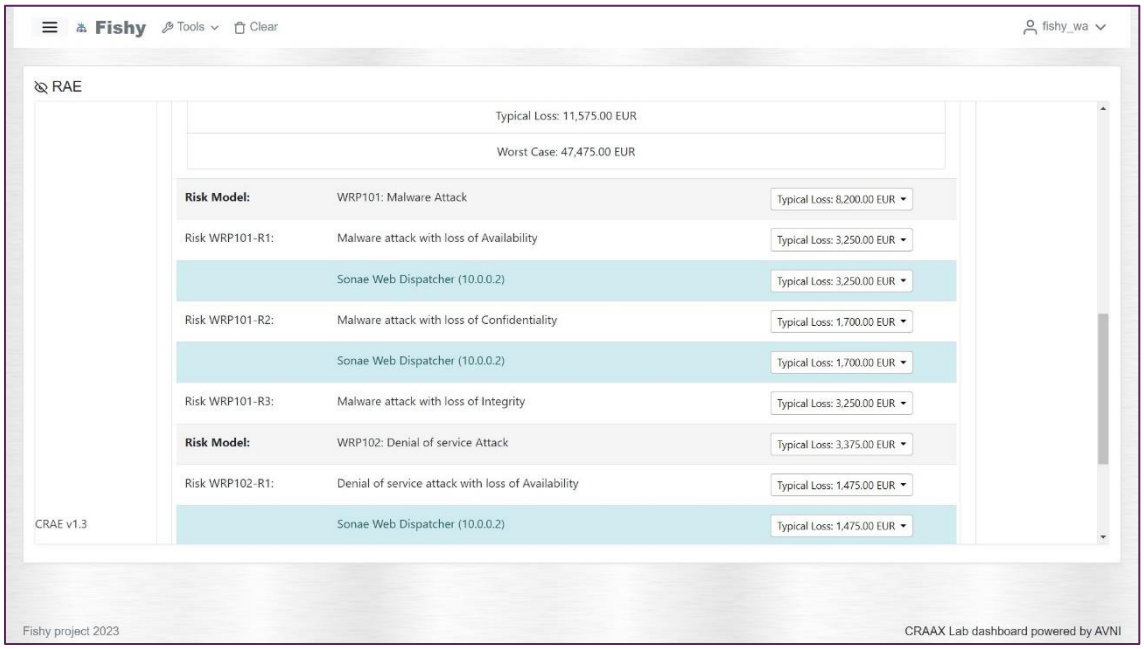


Figure 128. RAE quantitative risk assessment

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.

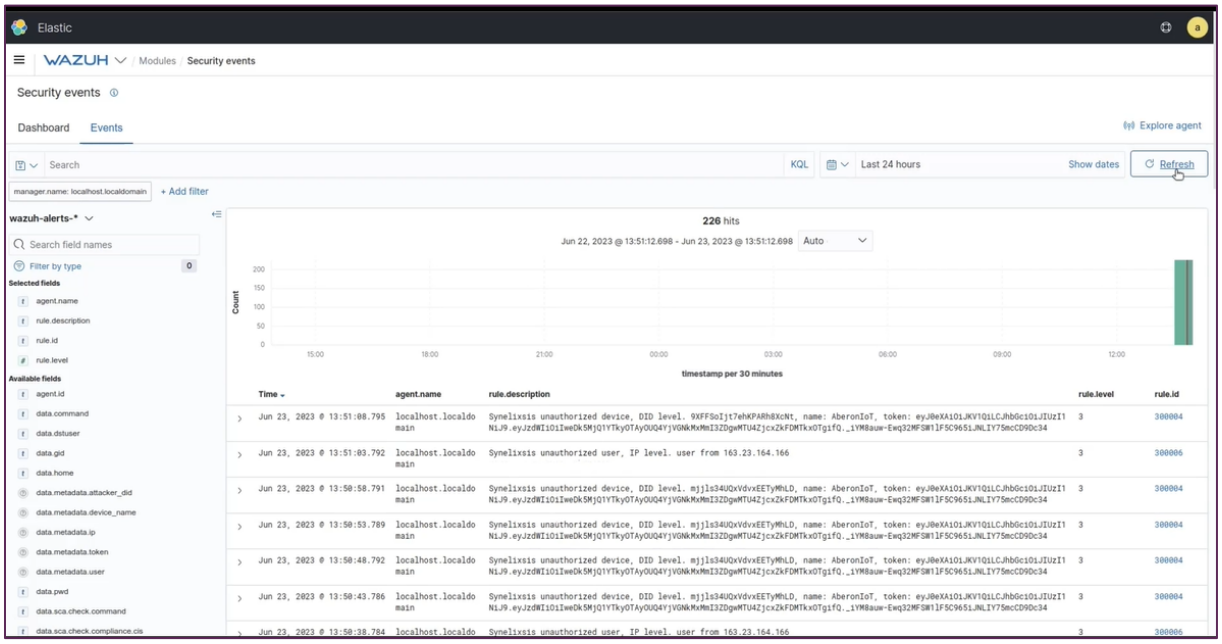


Figure 129: Printscreen from the dashboard of Wazuh

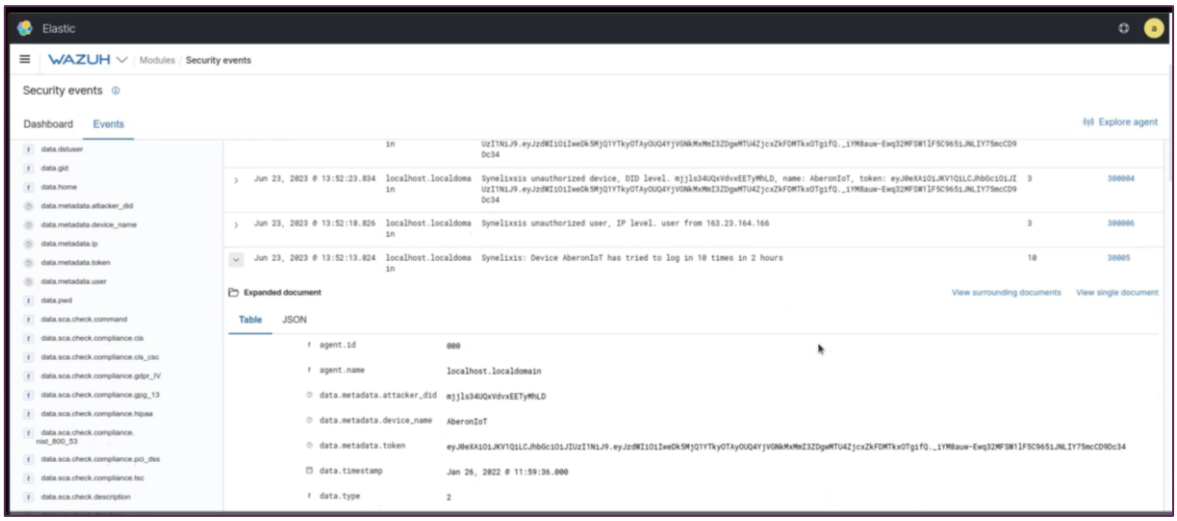


Figure 130: Printscreen from the dashboard of Wazuh that detects a brute force attack

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).

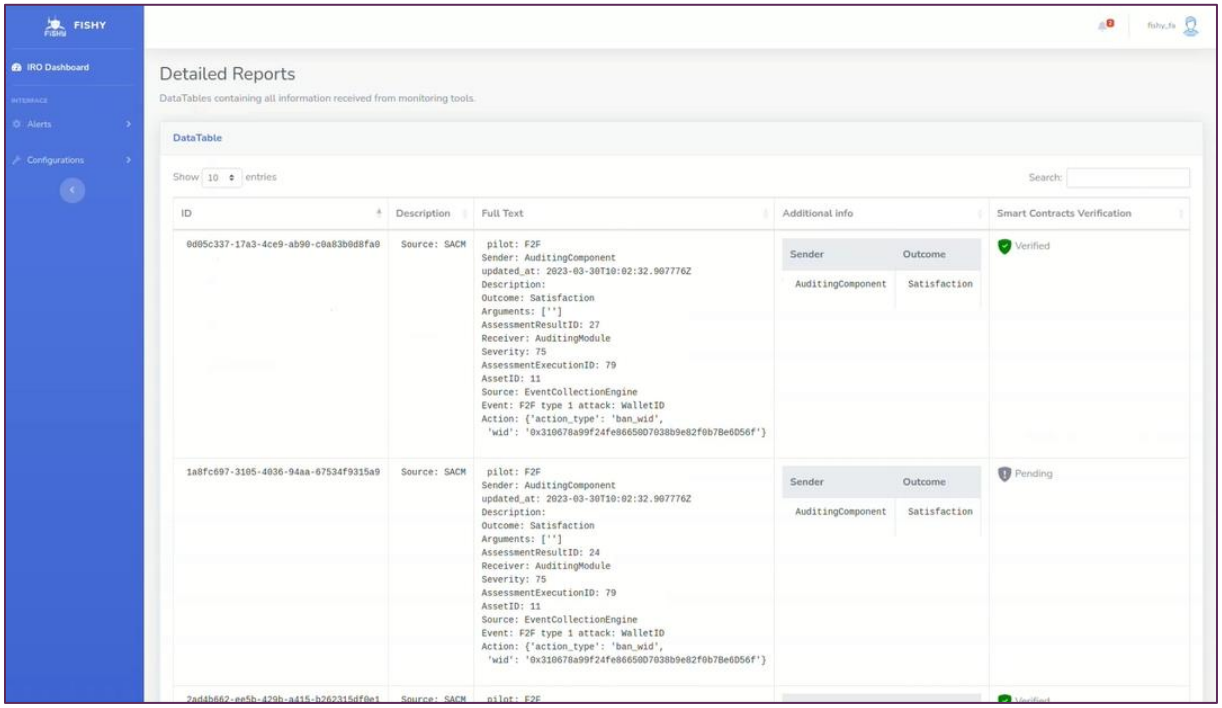


Figure 131: Printscreen from the dashboard of SACM that detects the wallet ID attack

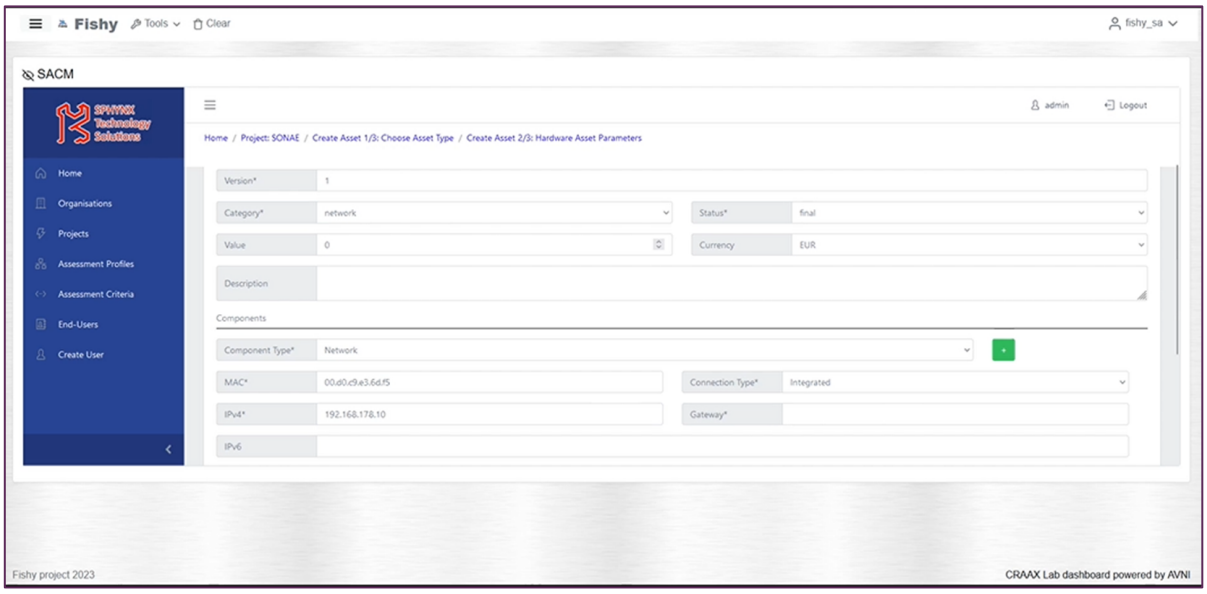


Figure 132: Printscreen from the dashboard of SACM on configurating new assets to monitor

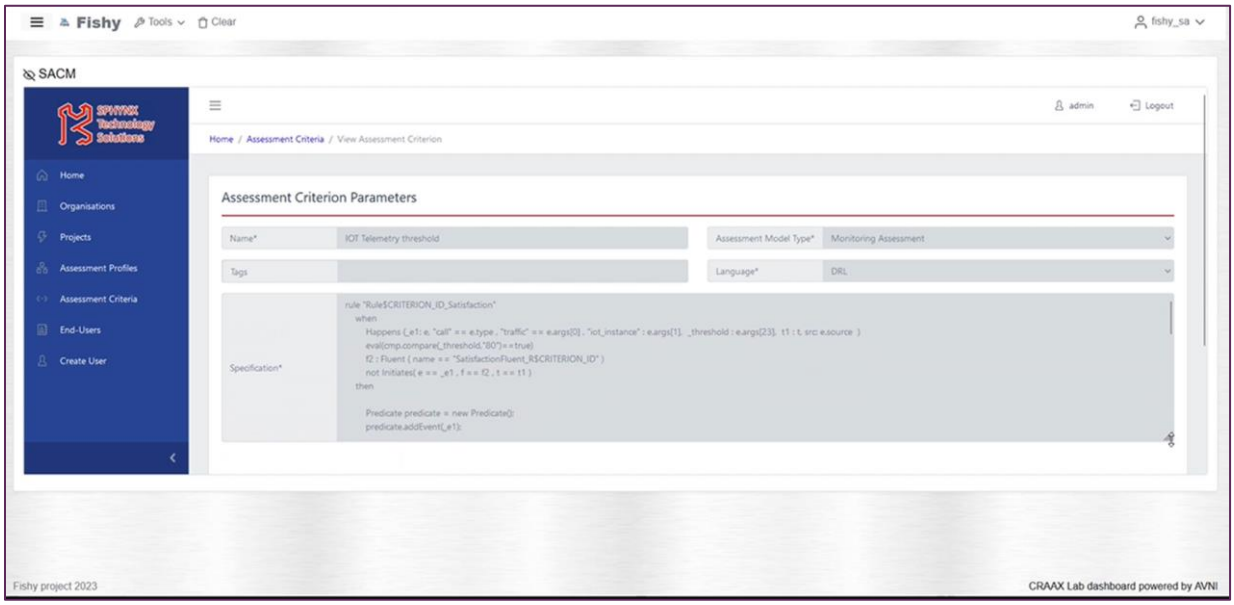


Figure 133: Printscreen from the dashboard of SACM on configurating new rules to monitor the assets

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.

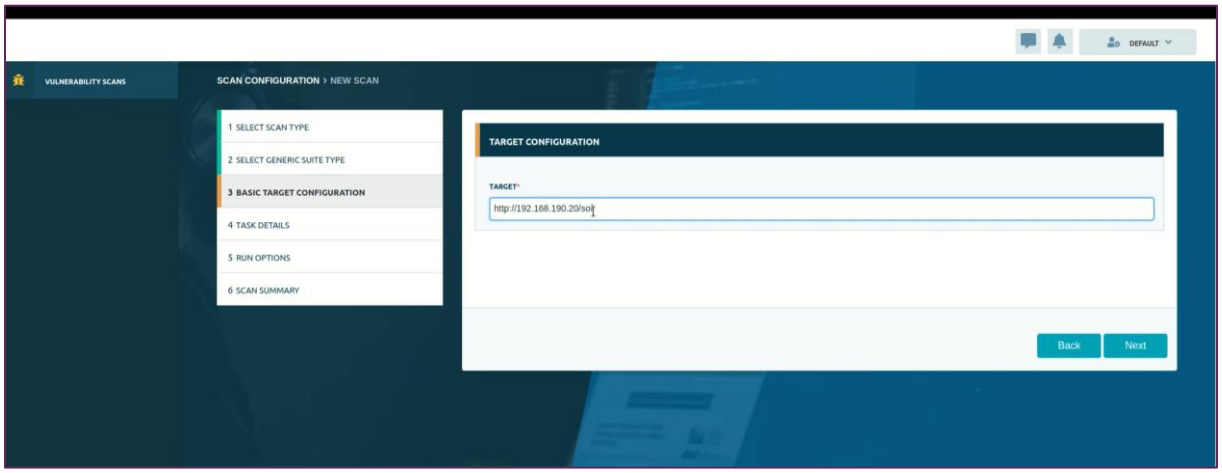


Figure 134: Configuration of VAT to scan a specific platform

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.

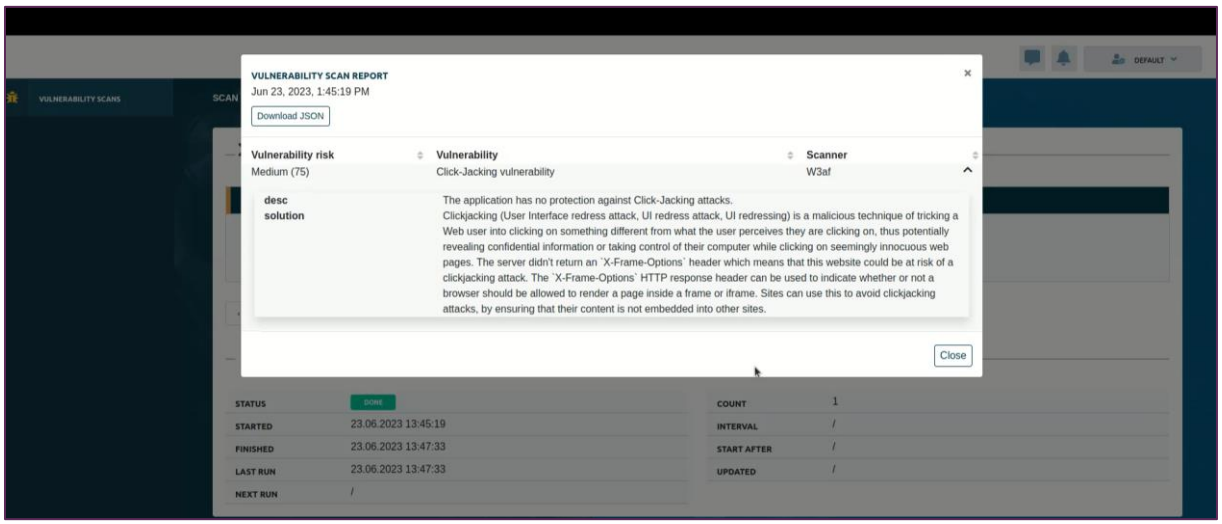


Figure 135: Results of the VAT scan of the F2F platform

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

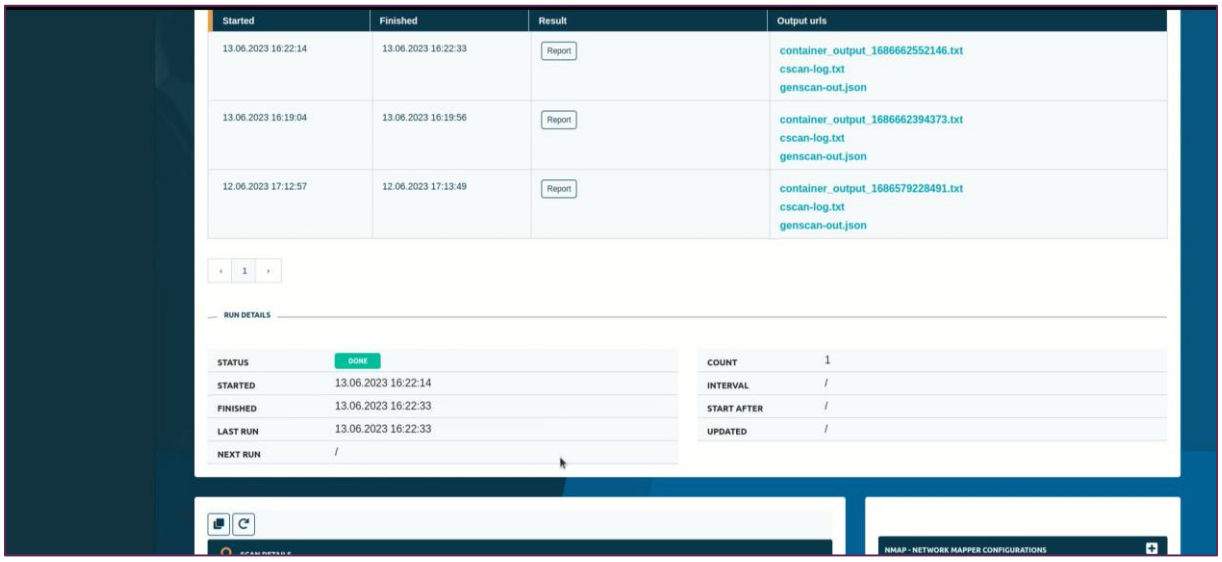


Figure 136: VAT monitors the availability of nodes

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.

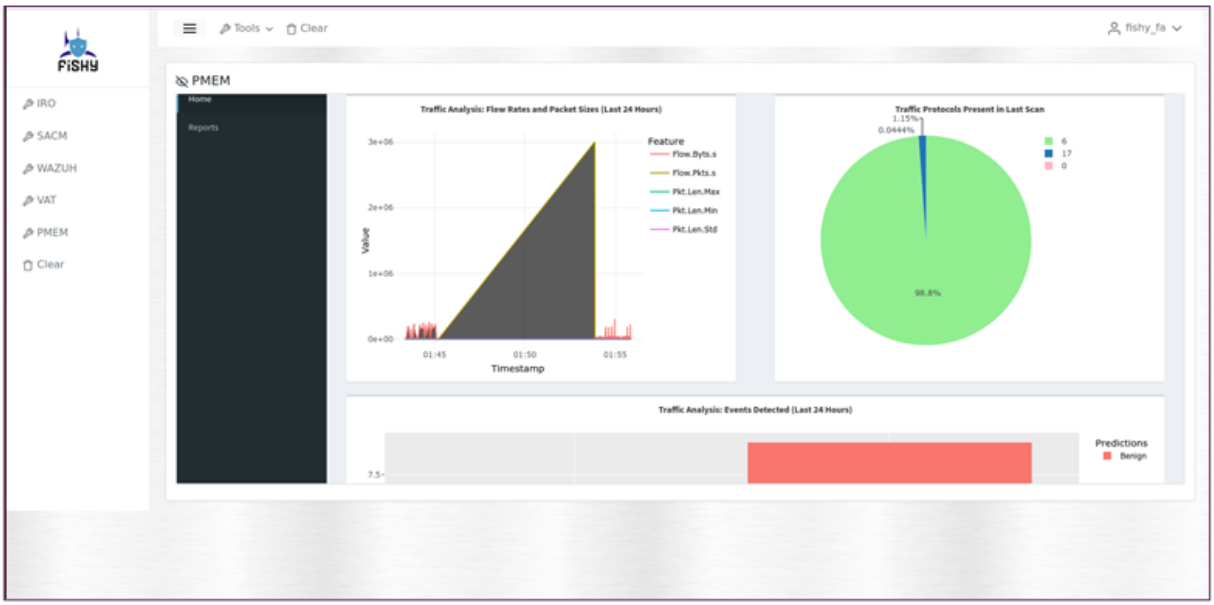


Figure 137: PMEM front end showing different status

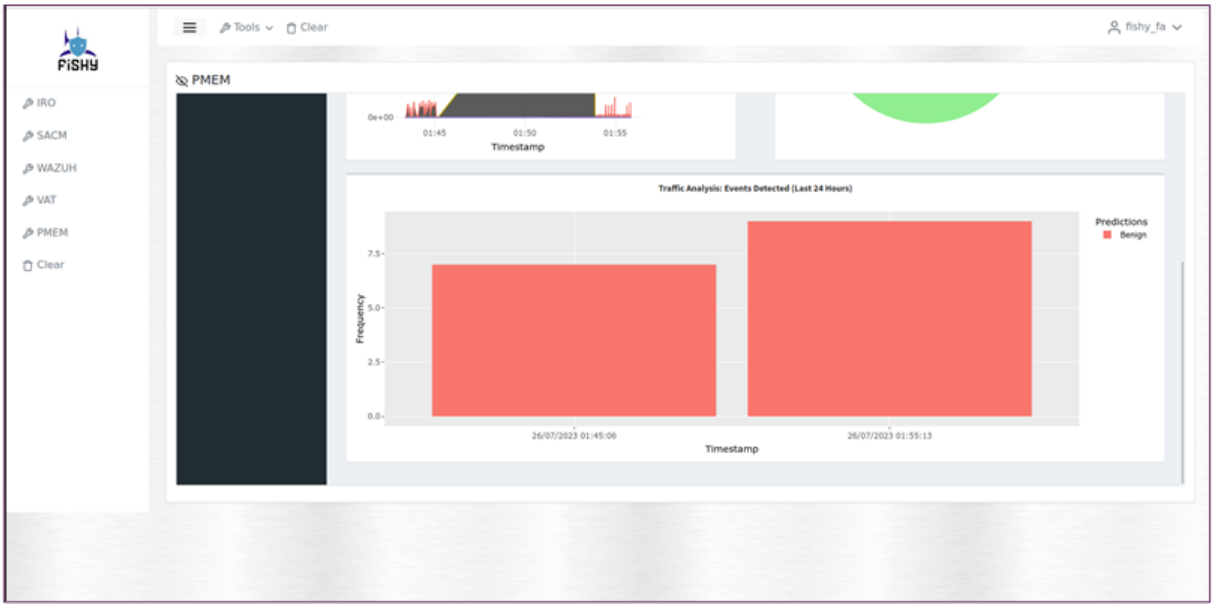


Figure 138: PMEM showing events detected in the last 24 hours.

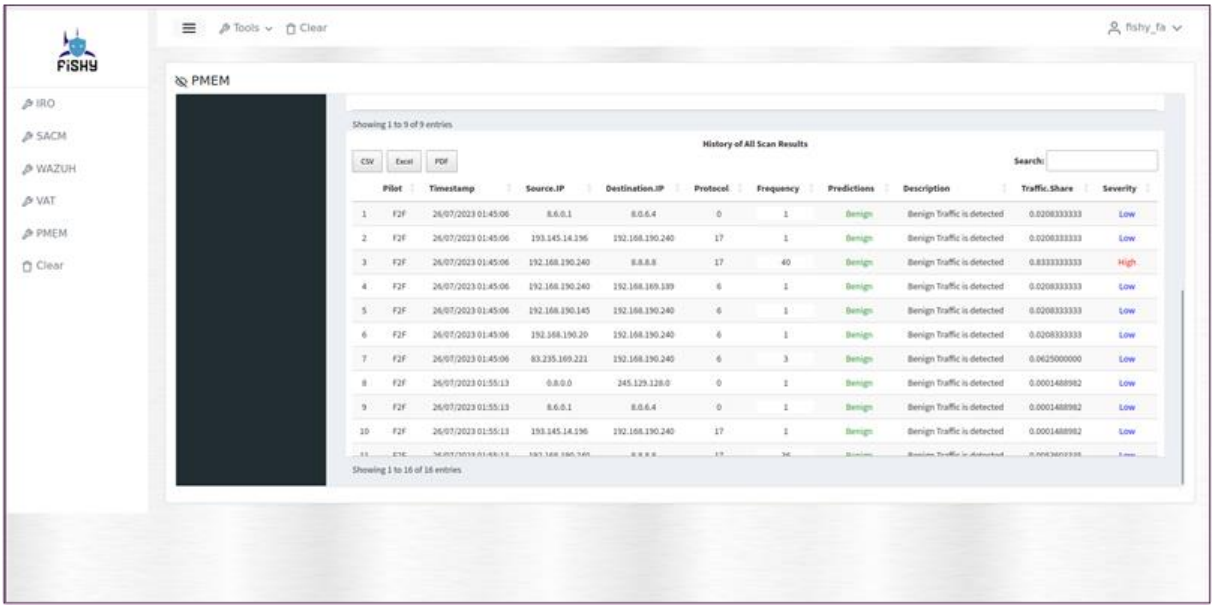


Figure 139: PMEM showing different scan results reports.

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.

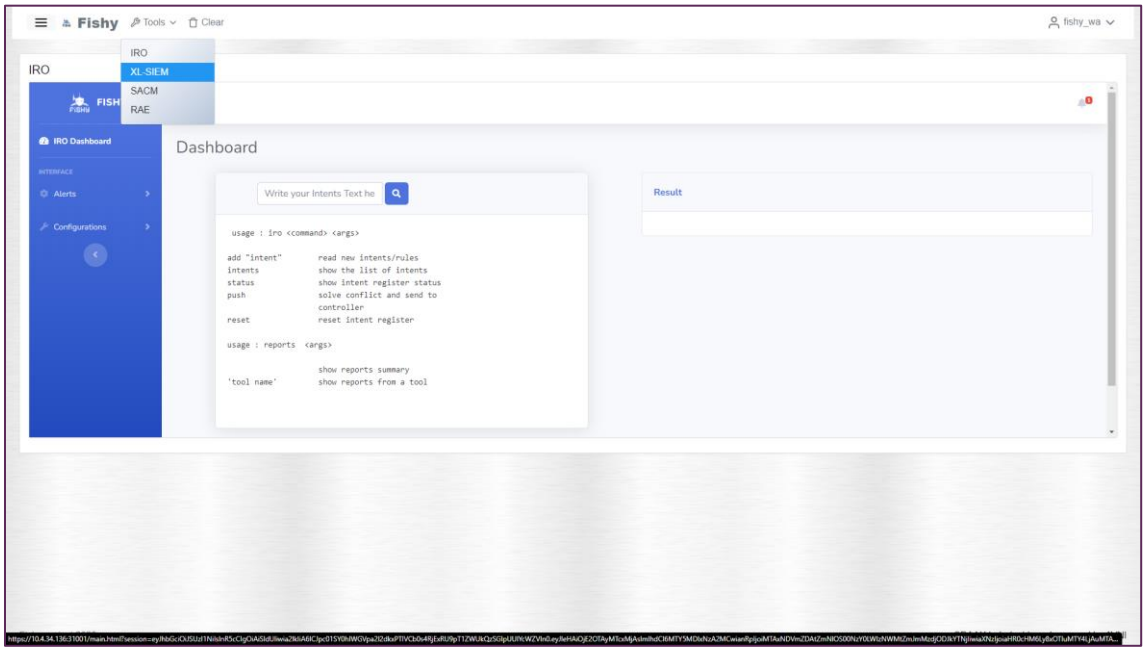


Figure 140: IRO in the main FISHY Dashboard

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.

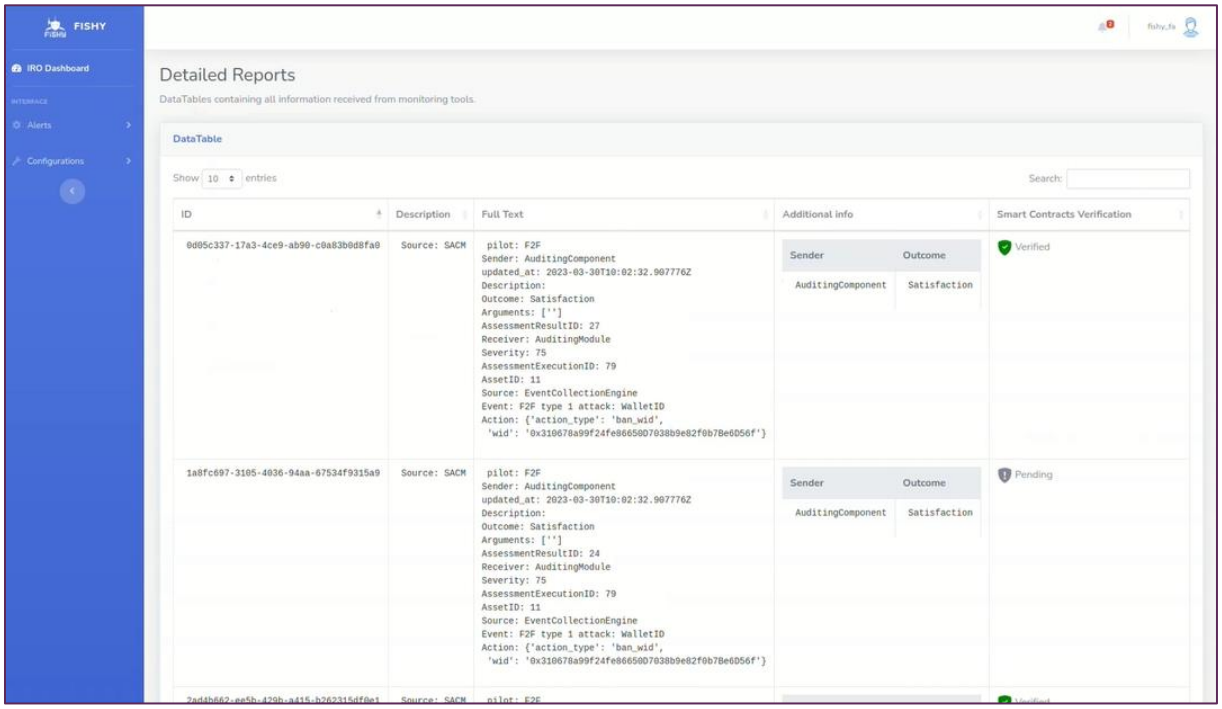


Figure 141:List of alerts on the dashboard from different tools (e.g.SACM detects wallet ID attack)

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.

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;

- 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.

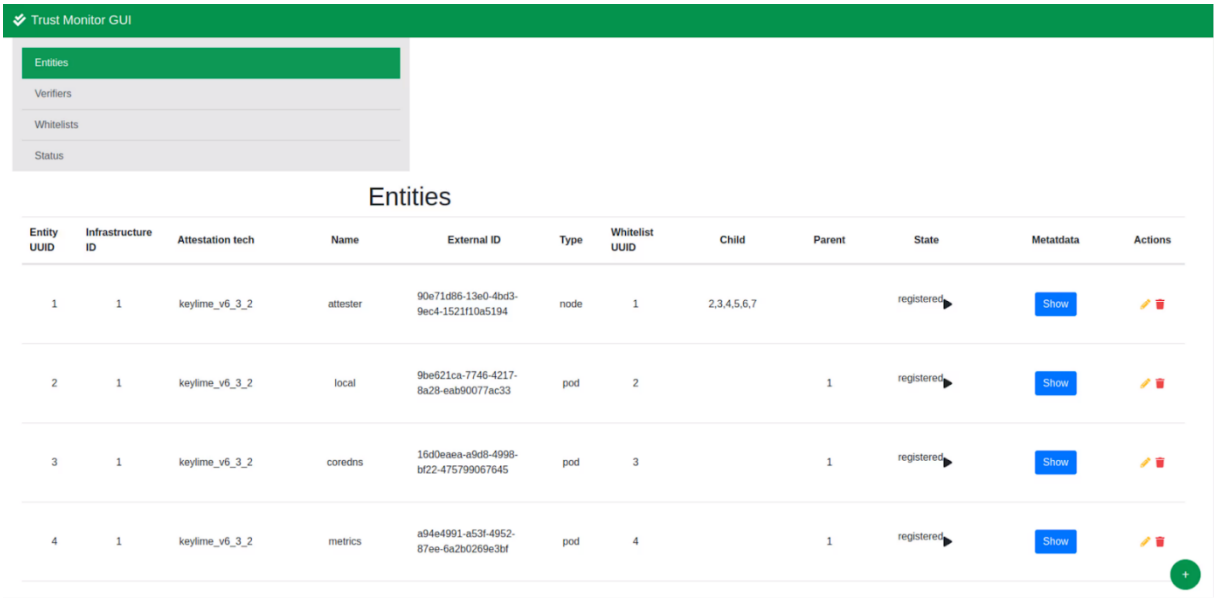


Figure 143: Trust Monitor listing the monitored nodes

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

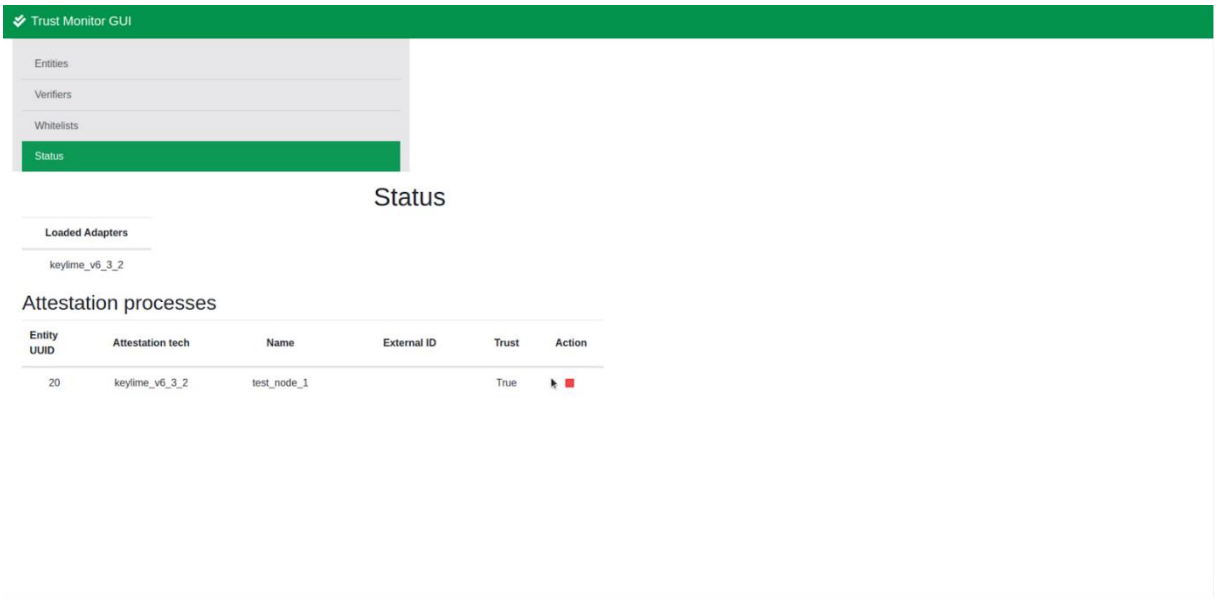


Figure 144: Trust Monitor during a Remote Attestation execution