D7.3 Pilot execution report in Tallinn

Work Package	7
Task	7.2
Authors	A. Roberts, L. Luts, F. Pornet, R. Mancilla, L. Bianconi, L. Tarchi, S. Haddad, A. Giannakoulias, P. Devito, D. David
Dissemination Level	Public
Status	Final
Due Date	15.08.2022 (review) 31.08.2022 (initial)
Document Date	29.08.2022
Version Number	1.0

Quality Control

	Name	Organisation	Date
Editor	L. Luts	TALLINN	15.08.2022
Peer review 1	Konstantinos Maliatsos	UPRC	29.08.2022
Peer review 2	Amedeo D'Arcangelo	KSP	29.08.2022
Authorised by (Technical Coordinator)	Jason Sioutis	ICCS	30.08.2022
Authorised by (Quality Manager)	Vasileios Sourlas	ICCS	30.08.2022
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	31.08.2022

Contributors

Name	Organisation	Date
L. Luts	TALLINN	01.08.2022
A. Roberts	TALTECH	15.08.2022
F. Pornet	ACS	15.08.2022
R. Mancilla	ENG	18.08.2022
L. Bianconi	SIGLA	23.08.2022
L. Tarchi	SIGLA	23.08.2022
S. Haddad	OPPIDA	22.08.2022
A. Giannakoulias	ED	22.08.2022
P. Devito	STAM	15.08.2022
D. David	DNSC	23.08.2022

Document Revision History

Version	Date	Modification	Partner
0.1	01.08.2022	Creation of ToC	TALLINN
0.2	17.08.2022	Added contents	TALLINN, TALTECH
0.3	22.08.2022	Document reviewed for second iteration of contributes	TALLINN, TALTECH, ICCS,
0.4	25.08.2022	Added contents	TALLINN, TALTECH, STAM, ED, OPPIDA, ENG, DNSC, SIGLA, ACS
0.5	29.08.2022	Added contents	TALLINN, TALTECH, STAM, ED, OPPIDA, ENG, DNSC, SIGLA, ACS
0.6	29.08.2022	Final version of the document internally reviewed	TALLINN, TALTECH, ICCS,
0.7	30.08.2022	Final version of the document ready for final quality control	TALLINN
0.8	30.08.2022	Quality control	ICCS
Final version 1.0	31.08.2022	Final version of the document ready for submission	ICCS

Legal Disclaimer

Table of Contents

List of Tables

LIST OF FIGURES

List of Abbreviations and Acronyms

Abbreviation	Meaning
ACS	Airbus Cyber Security
AV	Autonomous Vehicle
AMT	AMT Genova
BiBo	Bounded-input, Bounded-output
CBA	Cost-Benefit Analysis
CERT/CIRT	Computer Emergency Response Team/ Cyber Incident Response Team
CPaaS	Communications Platform as a Service
CSIRP	Collaborative security incident response platform
CTI	computer-telephony integration
CTIP	Collaborative threat investigation platform
DNSC	DNSC Romania
DoA	Description of Action
ED	European Dynamics
ENG	Engineering
FIMCA	Financial impact assessment engine
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GUI	Graphical user interface
HTTP	Hypertext Transfer Protocol
ICCS	Institute of Communication and Computer Systems
ICCS	Institute of Communication and Computer Systems
IDS	Intrusion Detection Systems
IOC	Indicators of Compromise
IPS	Intrusion Prevention Systems
KSP	Kaspersky
LAN	Local area network
MISP	Malware Information Sharing Platform
OPP	Oppida
PT	Public Transport
RITA	Risk analysis and impact assessment engine
RTLS	Real-time location system
SFTP	Secure file transfer protocol
SIEM	SIEM as a Correlation engine with backlog of markers
SIGLA	Gruppo Sigla

SOAR	Security orchestration, automation and response
XSOAR	Comprehensive security orchestration, automation and response (SOAR) platform
STAM	StamTech
Tallinn	City of Tallinn
TalTech	Tallinn University of Technology
UPRC	University of Piraeus Research Center
VPN	Virtual Private Network
XSOAR	Comprehensive security orchestration, automation and response platform

Executive Summary

This deliverable presents the results of the work conducted during Task 7.2 entitled “Pilot demonstrator - Tallinn”. The main objectives of the task were to demonstrated cybersecurity test cases on the multi-modal transportation business services and assets in the Tallinn transportation ecosystem. Current deliverable specifies the procedures of the conducted Tallinn pilot with a detailed description of the progress.

The first part of the deliverable includes Tallinn CpaaS infrastructure with assets and interactions, to have a better overview of the nature of the test-case. Involvement of the modules from CitySCAPE toolkit are presented in detail.

The second part of the document is dedicated to a comprehensive overview of the conducted pilot with low-level timelines, high-level outcomes and description of the activities performed in preparatory phase from 1st of July and during actual testing on 24th and 25th of August.

The final part of this deliverable breaks down each test-case into details, including scenario description, assets involved, defined attack scenarios and modules used in demonstration.

This document reports the results of demonstrating the benefits and usability of the CitySCAPE toolkit for detecting cyber-attacks and for cyber incident response in the multi-modal transport environment.

1 INTRODUCTION

1.1 Project Introduction

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation.

CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which consists of 15 partners from 6 European countries united in their vision to cover the cybersecurity needs of the multimodal transportation.

More specifically, the CitySCAPE software toolkit will:

- ✓ Detect suspicious traffic-data values and identify persistent threats
- ✓ Evaluate an attack's impact in both technical and financial terms
- ✓ Combine external knowledge and internally-observed activities to enhance the predictability of zero-day attacks
- ✓ Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay

The project duration extends from September 2020 to August 2023.

1.2 Deliverable Purpose

The purpose of this deliverable is to provide a comprehensive progress description of the conduct of the Tallinn pilot. The report will cover the system level evaluation of the pilot that is based on the integrated software system specified and developed in WP5 and WP6.

2 METHODOLOGY

The pilot deployment methodology is fully described in D7.1 "Site Surveys & Scenario Planning", it is structured as follows:

Step 1: Exercise objectives definition.

Step 2: Scenario elaboration (definition of scenario and chronological elements and events).

Step 3: Technical definition (definition of components to be used, definition of what will be simulated and what real hardware will be used, definition of technical events and attack paths).

Step 4: Technical implementation (clones' creation and deployment, attack scenarios implementation).

Step 5: CitySCAPE installation in pilot location, interconnection with cloned CPaaS when relevant, interconnection with remote CitySCAPE services when relevant.

Step 6: Platform test and pilot dry run.

Step 7: Pilot run phase.

Step 8: Pilot results analysis and feedback.

This document concerns Steps 4-8 where the technical definition of the test was carried out.

3 INFRASTRUCTURE DEPLOYMENT

3.1 Tallinn CPAAS infrastructure table

The TALLINN pilot environment consisted of infrastructure depicted in Figure 1.

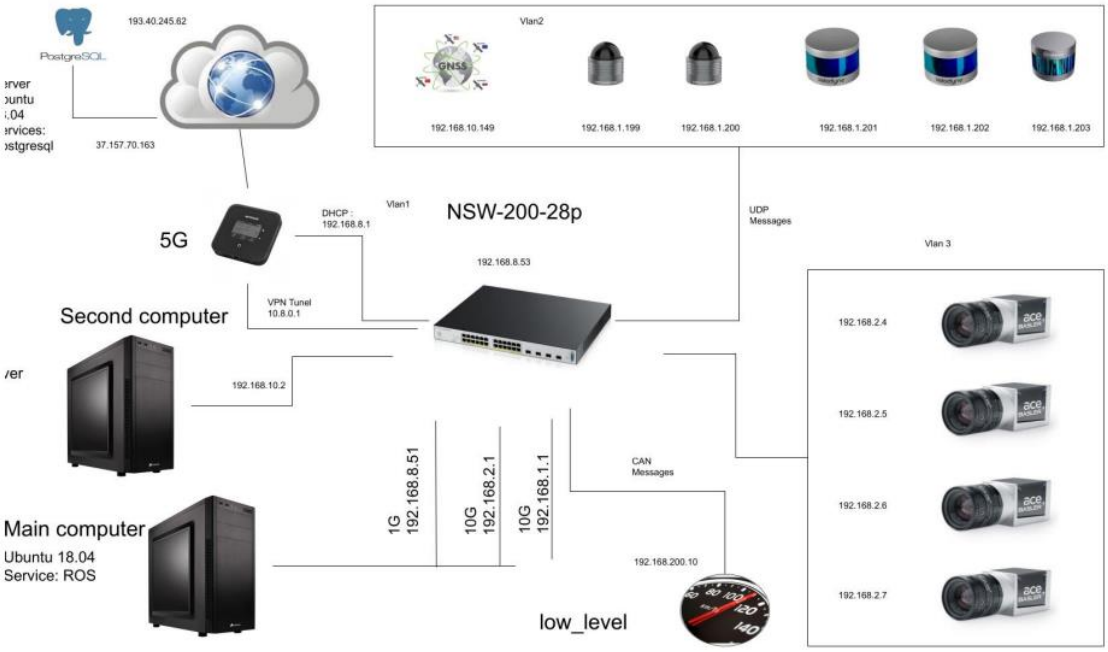


Figure 1. Tallinn CPaaS infrastructure

The “Control Room server” in the Firgure is denoted as the Cloud, which contains multiple important applications and services of the CPaaS and CitySCAPE Toolkit such as Teleoperation, Data Logging, Transportation Ticket Validator Application, IDS/IPS, SIEM, etc.. The AV Shuttle is represented by the network part segmented by the switch (NSW-200-28P), and a set of sensors is depicted (Camera and LiDAR). The control of the AV (where the self-driving modules (algorithms) are contained) is located on the main computer and the secondary computer.

The high-level infrastructure as related to the multi-modal transportation journey is represented in Figure 2.

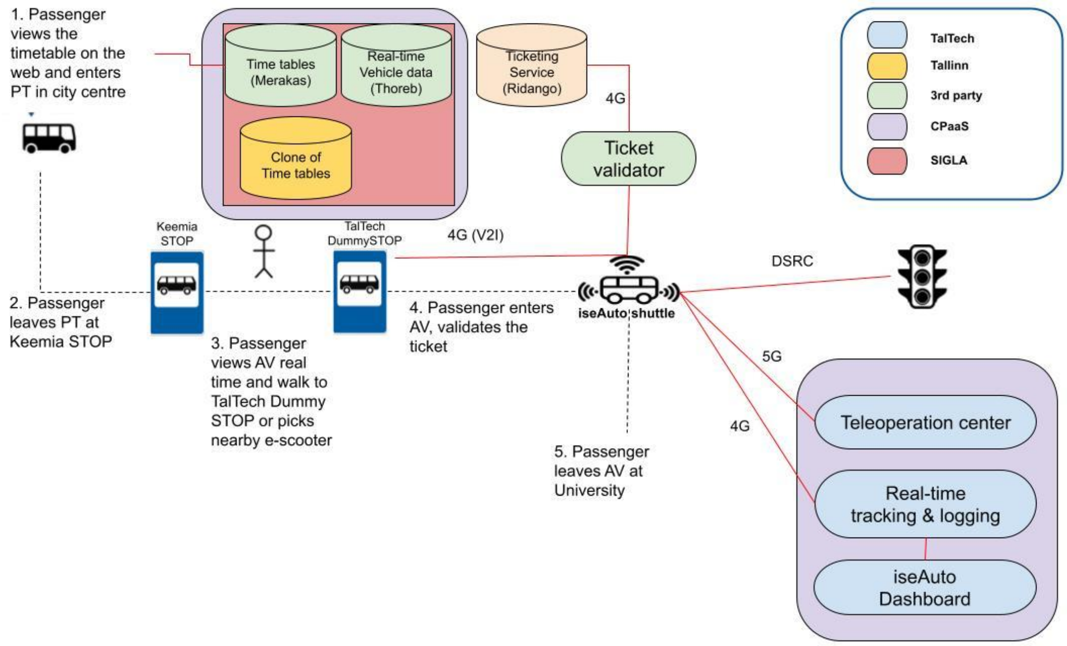


Figure 2. Tallinn High-Level CPaaS Assets

3.2 CitySCAPE toolkit

The CitySCAPE toolkit components are involved in the Test Case scenarios as depicted in Table 1.

Test Case	SIEM	IDS	RITA	FIMCA	CTIP	CSIRP
Test Case 1	X	X	X	X	X	X
Test Case 2	X	X	X	X	X	X
Test Case 3	X		X	X	X	X
Test Case 4	X		X	X	X	X
Test Case 5	X		X	X	X	X

Table 1. CitySCAPE toolkit modules used in Tallinn pilot

The X represents the functionality able to be reported in the TALLINN Pilot deployment during the 24th to 25th of August. The red X represents the functionality which will be demonstrated on the completion of the TALLINN Pilot and will be detailed in the final report in D7.5 “Pilot Evaluation and Knowledge capitalisation”. Since the IDS is a network monitoring engine, not all test cases involve its use.

4 CITYSCAPE TALLINN PILOT

4.1 Overview

The TALLINN Pilot started on 1st of July, commencing with a 2-week period where the AV shuttle was in operation in the TalTech campus area, collecting data. Based on the collected data, partners started to develop modules and interfaces among CitySCAPE toolkit components in order to perform attacks and develop mechanisms to detect them. After 5 weeks of preparatory works, all relevant partners gathered in Tallinn to perform live demo. On the first day of the demo, technical partners carried out comprehensive training for internal and external experts on the following subjects:

- how to use CitySCAPE tools in real conditions;
- how to operate scenarios in Cyber Range;
- how to exchange CTI using MISP or SFTP (see Annex IV).

In the trainings there were 29 participants from DNSC, ENISA – European Union Agency for Cybersecurity, CERT France and CSIRT Greece and local experts from TalTech and TALLINN.

After the training sessions, technical partners performed and then showcased live demo with 2 pre-defined scenarios in real conditions (Test-Case 1 & Test-Case 2). Intrusion attacks were performed on the live iseAuto systems, and the performance of the CitySCAPE modules was evaluated. When conducting test-case 3 and 4, unexpected issues with the integration of CitySCAPE modules were found. Furthermore, the SIEM required more data ingestion and analysis to adequately create detection rules for test-case 3 and 4 attacks. To ensure the ability to demo the remaining 3 scenarios (Ticketing system, GNSS Spoofing and SiglaMoving transport data) the pilot group identified the scope, and the preparatory works have been successfully completed. However, due to the unexpected problems with integration of the modules during the Tallinn pilot period, it was impossible to finalize all scenarios on time. Within upcoming weeks, project partners will continue working with the remaining three scenarios and results of all scenarios will be reported in the respective deliverable 7.5 "Pilot Evaluation and Knowledge capitalisation".

4.2 Low-Level Deployment Timeline

Week	Activity	Resource Required
July 4 to 8	AV Shuttle Operational – Monday Tuesday Wednesday Thursday IDS Monitoring of Data Collection	AV Shuttle Engineer. IDS Engineer. ACS Engineer.

	Preparation of Cyber Range Environment	
July 11 to 15	Prepare Training Scenarios Test/Prepare Cyber Attacks (Test Case DDoS & RSU) AV Shuttle Operational – Monday Tuesday Wednesday Thursday IDS Monitoring of Data Collection Preparation of Cyber Range Environment	ACS, TalTech, CitySCAPE Tool Owners, DNSC. Oppida, TalTech. AV Shuttle Engineer. IDS Engineer. ACS Engineer.
July 18 to 5 August	Any remediation of the IDS & SIEM (CitySCAPE Platform) Any remediation of the iseAuto network and infrastructure	CitySCAPE Tool Owners iseAuto team
August 8 to 12	Setup/preparation of the Tallinn Pilot Environment	TalTech, Oppida, CitySCAPE Tool Owners.
August 15 to 18	Setup/preparation of the Tallinn Pilot Environment SIEM & IDS monitoring of data collection	TalTech, Oppida, CitySCAPE Tool Owners. SIEM & IDS engineer.
August 24	Cybersecurity testing in the CyberRange environment and Tallinn Environment	Oppida, TalTech, ACS.
August 24	Tallinn Pilot Demonstration CitySCAPE Training	CitySCAPE Consortium. DNSC, ACS, ED, Tallinn Stakeholders.
August 24 to 25	Tallinn Pilot Demonstration CitySCAPE Training	CitySCAPE Consortium. DNSC, ACS, ED, Tallinn Stakeholders
	Draft Pilot Report	

Table 2. Low-Level Deployment Timeline

4.3 Cybersecurity Test Case Scenarios

Tallinn test cases focused on the following cybersecurity aspects:

1. Improved confidence of efficient handling of day-one and specific DoS attacks.

2. Minimizing security risks introduced by (less security-aware) external service providers.

3. Improving the fraud prediction caused by recent EU finTech market opening directives and technological advancements.

4. Minimizing the risks to personal privacy related to fraud prevention and new ticketing services like GNSS/ indoor RTLS based BiBo.

These test-cases involve a diverse range of transportation technologies, from AV shuttles to transportation fare card validation and from adaptive traffic management, from vehicle to infrastructure (V2I) communications. The Tallinn pilot described attacks on each of the transportation areas, and deployed attacks on all, except the Test-Case 4 (GNSS) which required further investigation in order to conduct the attack, and Test-Case 3 (Fraud Detection), which required further exploration of the logs by the SIEM operators to construct effective detection rules. Also, Test-Case 5 (Mobile Application) required further log analysis by the SIEM operators to construct detection rules and develop the playbooks for security orchestration.

4.3.1 Test Case 1: Availability of AV Shuttle Network Communication

4.3.1.1 Pilot scenario description

In this scenario, the passenger is able to move seamlessly from the city transportation modes to the last-mile services (AV Shuttle). The passenger interactions to achieve this are listed below:

1. Passenger departs from the city-transport mode and reaches the AV Shuttle.
2. The AV Shuttle drives the passenger to the end destination.

The desired behaviour of the system is described below:

1. The remote operations center of the AV Shuttle monitors the operation of the AV Shuttle.
2. The remote operations center monitors the passenger in the AV Shuttle.
3. If there are any safety events, the emergency stop can be used to stop the AV Shuttle, or the remote operator can assume control and make driving decisions.

The following table describes the assets involved in the scenario and the scope of each of them.

Autonomous Self-Driving Shuttle					
Vehicle on-board Computer	Hardware	Taltech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Applications (ROS, Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.
Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is stored in the ROSBag logging system.	The video files from on-board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo-location/ SLAM.
IMU	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communication modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on-board unit, sensors and router. Manages access to the network and segments network in VLANs).
AV Shuttle Operating System	Middleware/Firmware OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self-driving application	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services Database connectors	Autoware.ai Application framework for self-driving vehicles.

Teleoperation services	Hardware, Middleware, Software, Data, Redundancies	Teleoperation services provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperation Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
Actuators	Hardware, Firmware, Software	Taltech		Network interface (Ethernet, CAN)	Actuators

Table 3. Assets involved in the scenario 1

4.3.1.2 Attack scenarios

The aim of Test Case 1 (Availability of AV Shuttle Network) is to test the ability of the CitySCAPE toolkit to detect cyber-attacks that impact the availability of the AV Shuttle teleoperation network. Without communication of the AV Shuttle to the teleoperation server, the AV cannot be safely monitored and controlled by the teleoperator and thus the last mile extension journey of the passenger is either not possible or unsafe. The aim of this test case was to assess the CitySCAPE toolkit against availability attacks such as DDoS, and this includes techniques within the cyber-attack kill chain, from reconnaissance (scanning and fingerprinting) to exploitation (delivery of DDoS packets).

In order to perform Test Case 1 and try to affect the AV communication availability, OPPIDA has performed the following tests scenario steps:

- Fingerprinting
  - o Try to identify targets and potential vulnerabilities
- DoS Attacks
  - o From the internet
  - o From inside the vehicle (inside attacker simulation)

To perform these scenarios and after several preliminary test, Oppida has finally used the following tools:

- Nmap
- Metasploit
- Command line
- Exploit scripts available on the internet for specific identified service with potentially known vulnerability

Two different sub scenarios have been played.

The first one (sub-testcase 1.1) consisted of identifying and attack targets from the internet (system elements with public IPs) which is actually equivalent to targeting the control server (see Figure 1) as depicted in Figure 3.

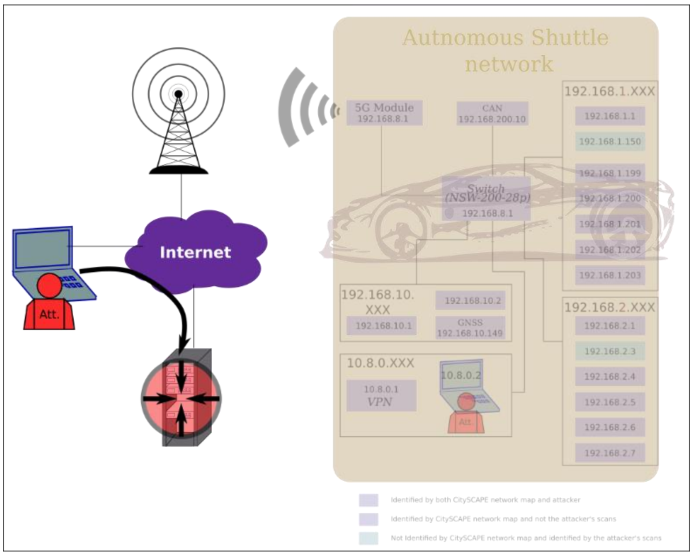


Figure 3. Sub-testcase 1.1 involved element

The second test case (sub-testcase 1.2) simulated inner vehicle attacks. This was performed through a VPN connection to the AV network, provided by a VPN server installed in the vehicle (see Figure 1). Thus, enabling Oppida to lunch sub-testcase 1.2 steps from the AV LAN, allowed to simulate an attacker able to get access to the AV LAN, either physically connected to the vehicle (e.g. a passenger able to find an accessible physical port) or a roadside attacker, able to hack the AV communication device.
From this position we performed in sub-testcase 1.2 a complete scan of the accessible sub-networks and then performed a targeted DoS attack on its most significant equipment - the communication unit (see Figure 1), as depicted in Figure 4 and Figure 5.

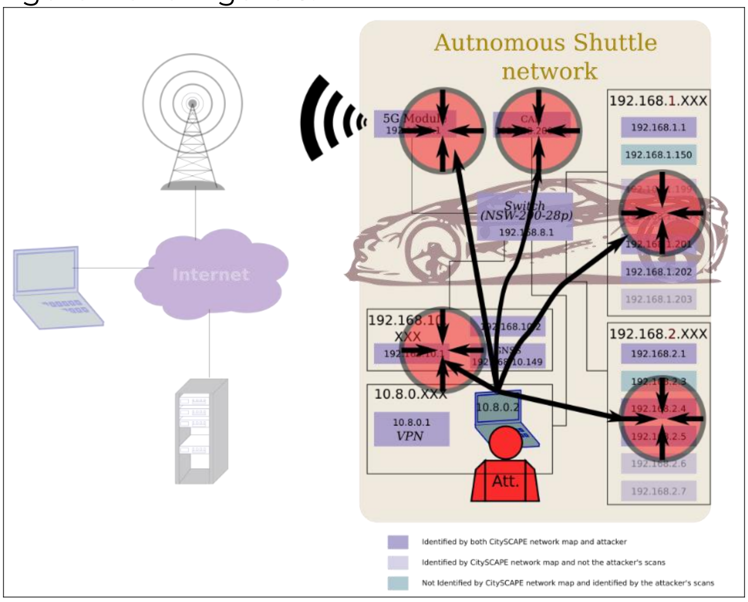


Figure 4. Sub-testcase 1.2 scanning targets

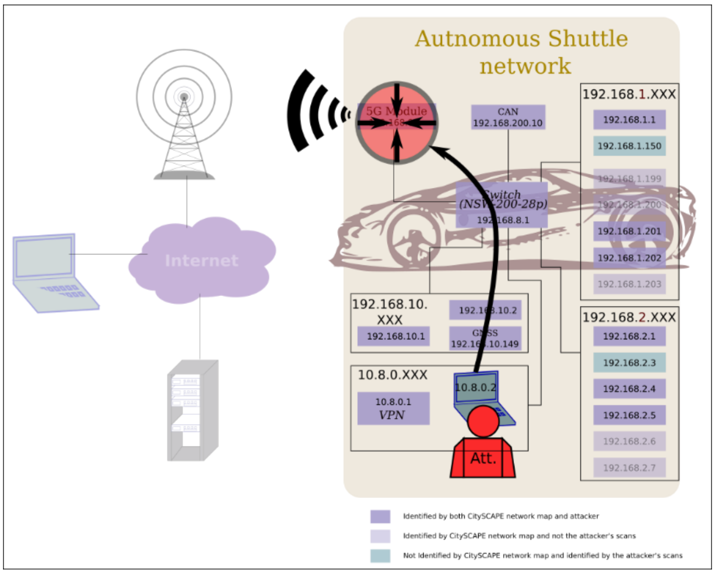


Figure 5. Sub-testcase 1.2 DoS target

Classic synflood attacks have been performed, running the dedicated Metasploit plugin plus command line hping as well as a scprit dedicated to attack the specific version of the ftp server of the control server.

4.3.1.3 Modules behaviour

4.3.1.3.1 SIEM

Graylog - Graylog receives alerts from the IDS/IPS component, as represented in the following picture.

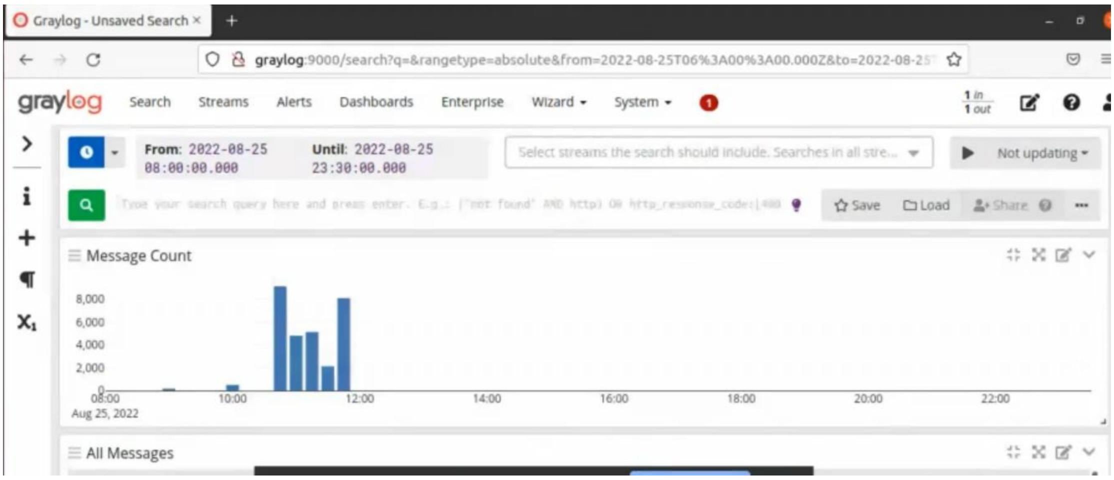


Figure 6. Alerts received to Greylog

In particular, during the first SYN flood attack, several messages concerning TCP sessions without 3-way handshakes were received and aggregated into an alert sent to the XSOAR component., as detailed in the picture below

Figure 7. Aggregated alert sent to the XSOAR component

The same kind of messages was received, aggregated, and transmitted to the XSOAR component when the second iteration of the SYN flood attack was executed, as shown in the following picture.

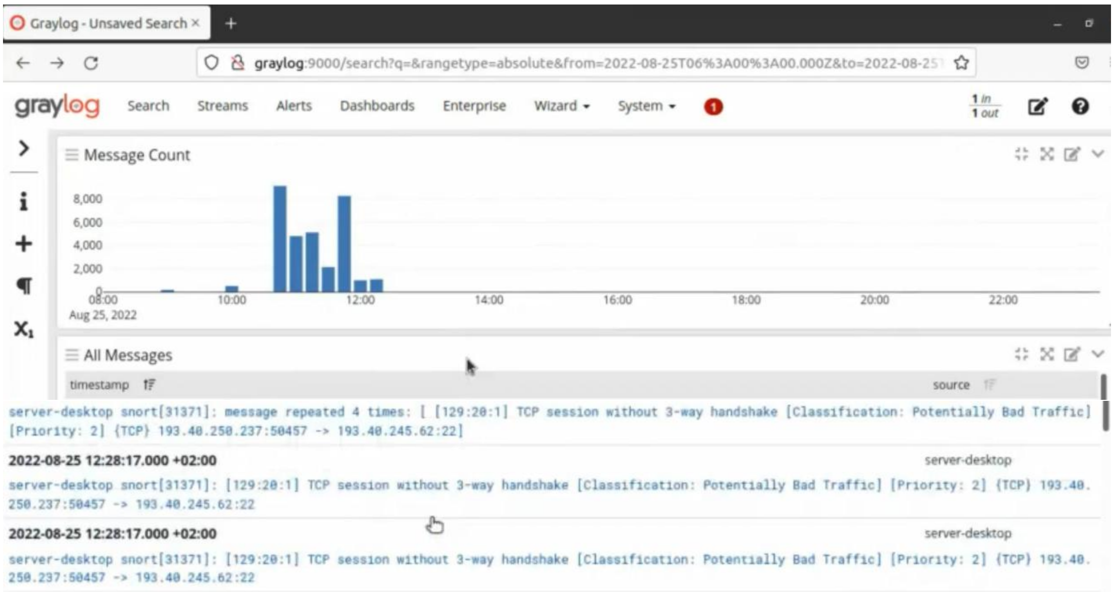


Figure 8. Received messages transmitted to XSOAR component

XSOAR - XSOAR receives alerts from Graylog, maps them to its internal data model, and assigns them to a user. In the picture below, the dashboard of an analyst is detailed.

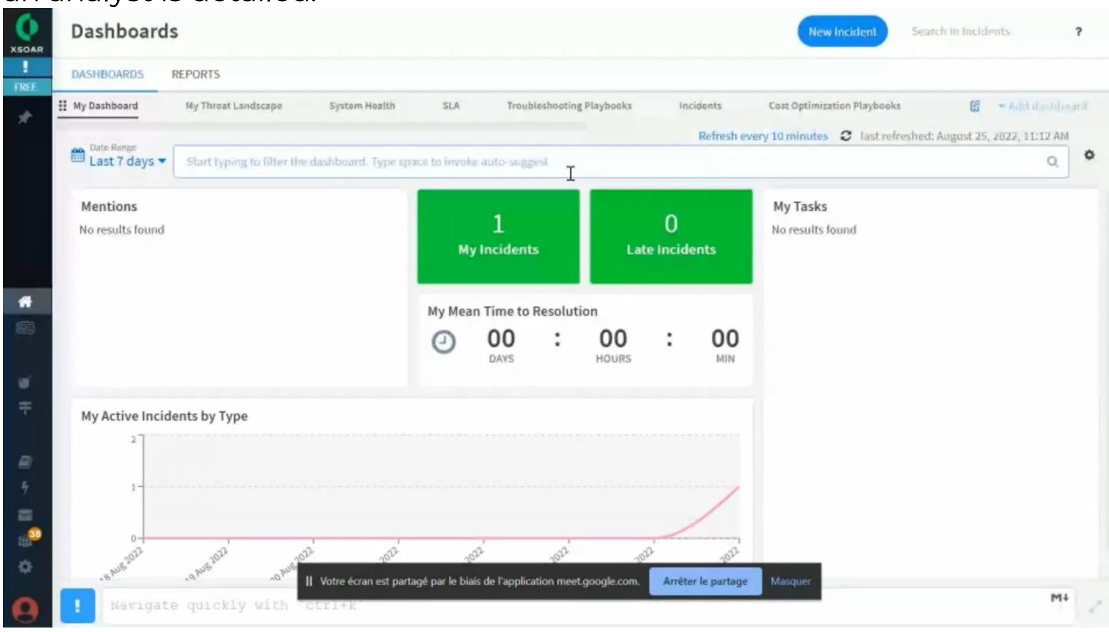


Figure 9. XSOAR receives alerts from Graylog

The alert received following the first SYN flood attack is displayed in the incident dashboard, as detailed in the screenshot below.

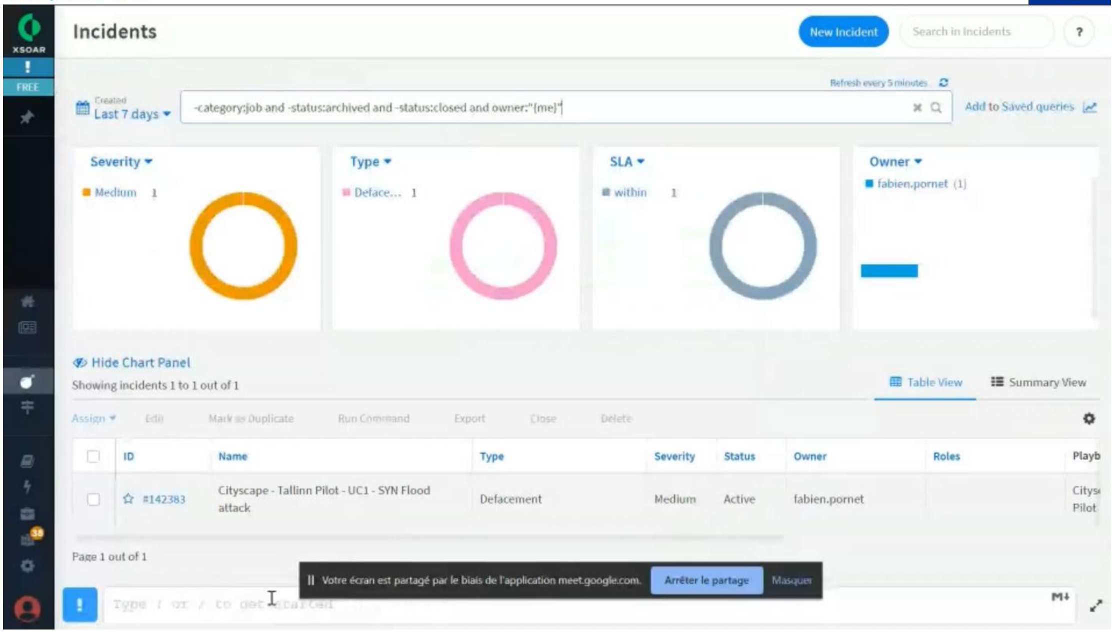


Figure 10. Alerts displayed in incident dashboard

The description of this incident is available in the following interface.

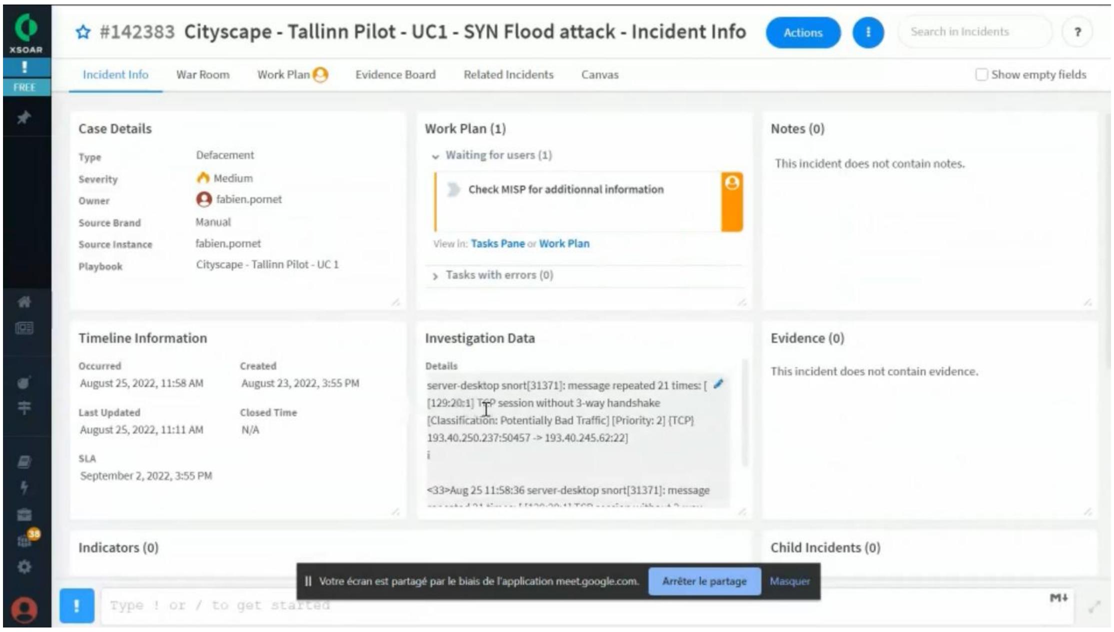


Figure 11. Incident description

XSOAR associated the incident with a playbook, i.e. a description of the actions to be executed automatically or manually by the analyst to accelerate the handling of the incident, as represented below.

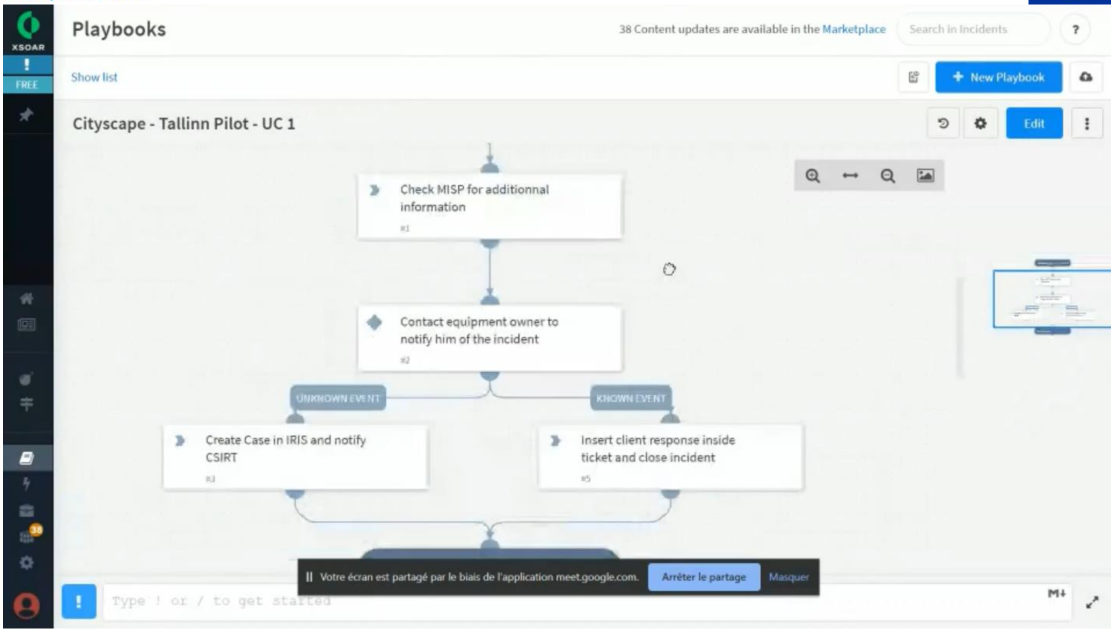


Figure 12. XSOAR provided description of the actions to the handling of the incident

On the second iteration of the SYN flood attack, a new alert was created into XSOAR, while the old one was assigned to a service account in order not to "pollute" the analyst interface with data from the old alert, as showed in the following picture.

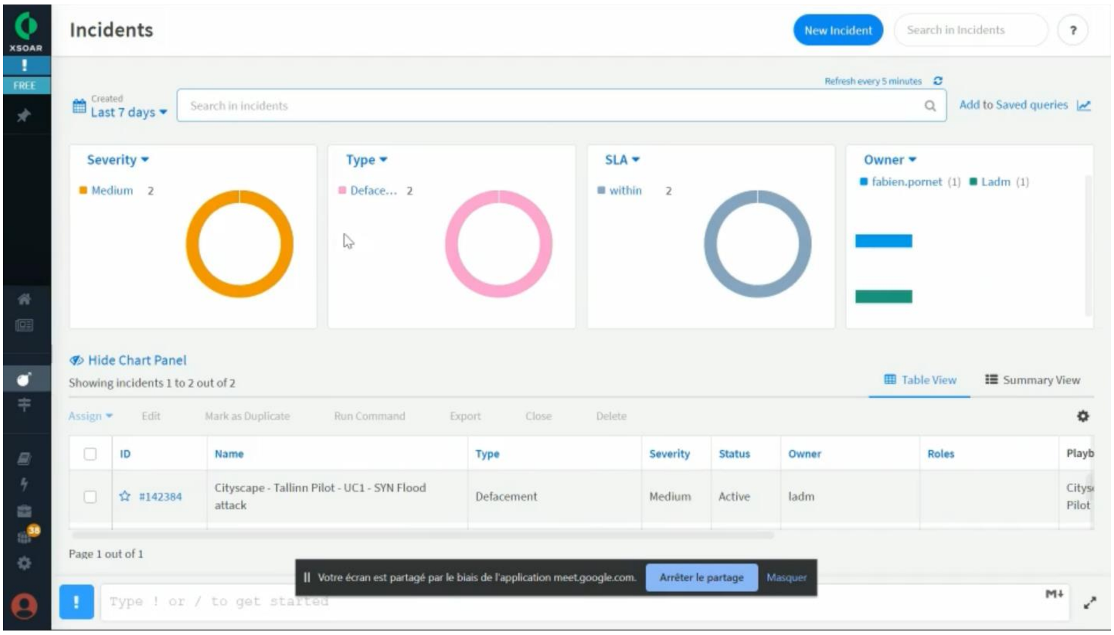


Figure 13. SYN flood attack

4.3.1.3.2 IDS/IPS engine

The solution version used for this demonstration is the alpha version, where the basic integration of the internal module has been developed and an initial version of the Anomaly Detection Procedure is implemented as a separate API.

The internal architecture of the CityScape IDS/IPS engine is depicted in Figure 14 , details are available in deliverable D5.4 "IDS/IPS final prototype".

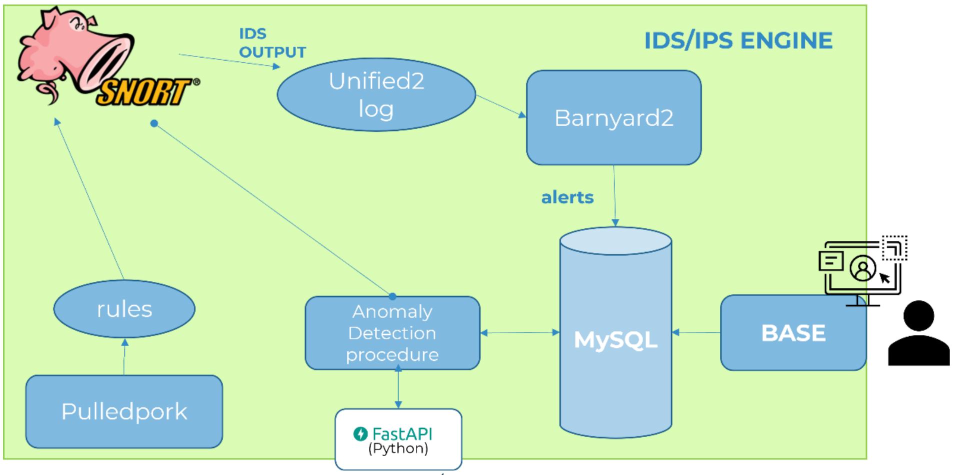


Figure 14. CityScape IDS/IPS engine internal architecture

The deployment has been executed during month M24 by ENG IDS engineers using the bash files provided in the code repository.
As mentioned in D7.1 "Pilot scenarios, validation plan, and Pre-piloting preparation", the IDS/IPS engine is used in the first two test case scenarios (sections **Error! Reference source not found.** and section **Error! Reference source not found.**):

1. AV Shuttle Network Communication;
2. Integrity of RSU;

In both test cases, the IDS/IPS is used to identify possible threats, in particular in the first test case the IDS/IPS engine should be used in ON-LINE mode while for the latter one the OFF-LINE mode:

- Online: the IDS/IPS engine is running and analysing in real-time the traffic that is passing through a specific interface,
- Off-line: the IDS/IPS engine analyses a pre-recorded traffic dataset pcap file) and identifies potential threats, then the idea is to try to use the ADP-API to test the Anomaly detection Procedure with to pre-recorded dataset, the first one to train the procedure and create the ADP model and the second one to test the model.

For the TALLINN pilot the IDS/IPS engine has been deployed on the TALLINN Control Room Server (See Figure 1 in section 3.1).

The TALLINN Control Room Server is connected to AIRBUS VPN through OpenVPN client to be able to forward the engine alerts to the CityScape SIEM which is, for this pilot, deployed into the AIRBUS servers.

In the following table, additional technologies used for this pilot are listed with a short description.

#	Name	Description	Use in the pilot
0	Apache2[1]	Open-source HTTP server for modern operating systems	Used to expose the GUI to view alert (BASE)

[1] https://httpd.apache.org/

		including UNIX and Windows	
1	SNORT[2]	Open-source IDS/IPS	Used to implement rule-based capabilities
2	FastAPI[3]	Open-source web framework for building APIs with Python 3.6	Used to expose Anomaly Detection Procedure API
3	OpenVPN Client[4]	Client software for connecting to a VPN	Used to connect to AIRBUS VPN

Table 4. Additional Technologies used in Tallinn pilot

During the first day of TALLINN's Pilot live demo, August 24, 2022, the ENG colleagues illustrated a brief guide on the usage of the IDS/IPS engine sub-modules to the pilot's participants based on the type of users. The presentation used is available in ANNEX I - IDS/IPS engine user guide.
Then the IDS/IPS engine has been activated in Online mode the day after, August 25, 2022, monitoring the enp2n0 interface.

The IDS/IPS engine, as mentioned before, was running in Online mode and the following alerts have been generated (see Figure 15):

a. TCP session without 3-way handshake [Classification: Potential Bad Traffic] [Priority: 2]
b. (spp_ssh) Protocol mismatch [Classification: Detection of non-standard protocol or event] [Priority: 2]

The first type of alert was generated with a huge number of instances, indicating that the alerts are related to a potential SYN flood attack, while the second type of alert had a limited number of records.
In Figure 16 is depicted the GUI to view the generated alerts.

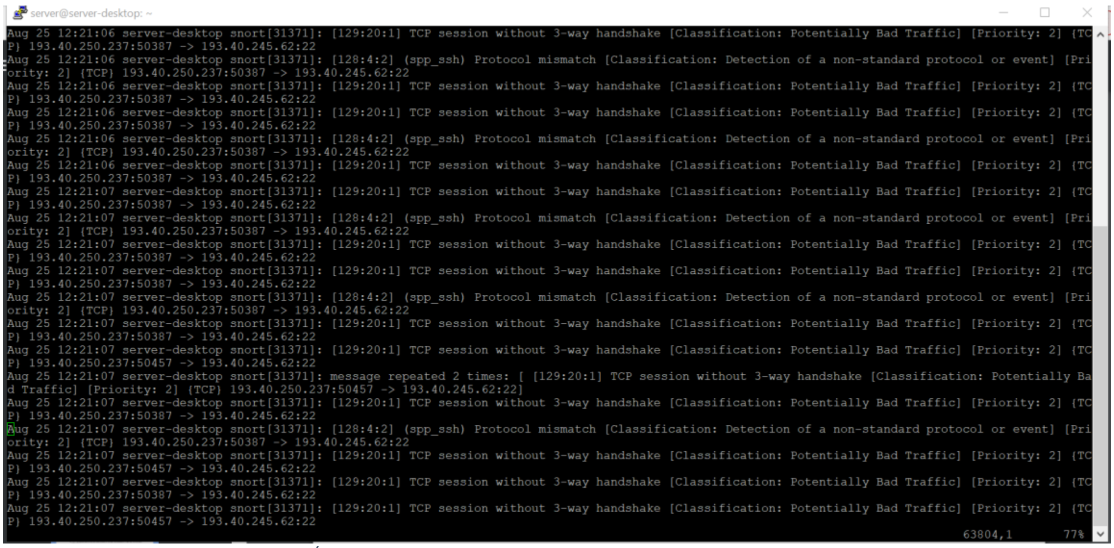


Figure 15. IDS/IPS engine log with the alerts generated for test case 1

[2] https://snort.org
[3] https://fastapi.tiangolo.com/
[4] https://openvpn.net/vpn-client/

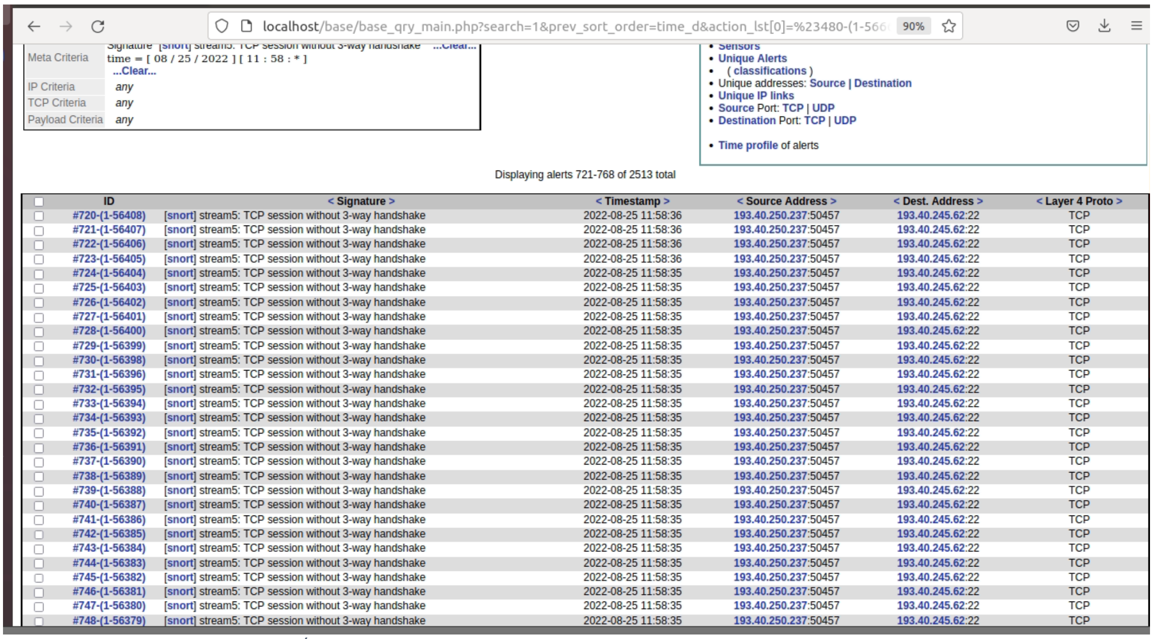


Figure 16. IDS/IPS engine alerts viewed through the GUI for Test case 1.1

For sub-testcase 1.2, alerts related to the attack on the communication unit (previously described) have not been generated; mostly due to the fact that the IDS/IPS engine was deployed on the server machine and was not receiving all the traffic in the subnetwork.

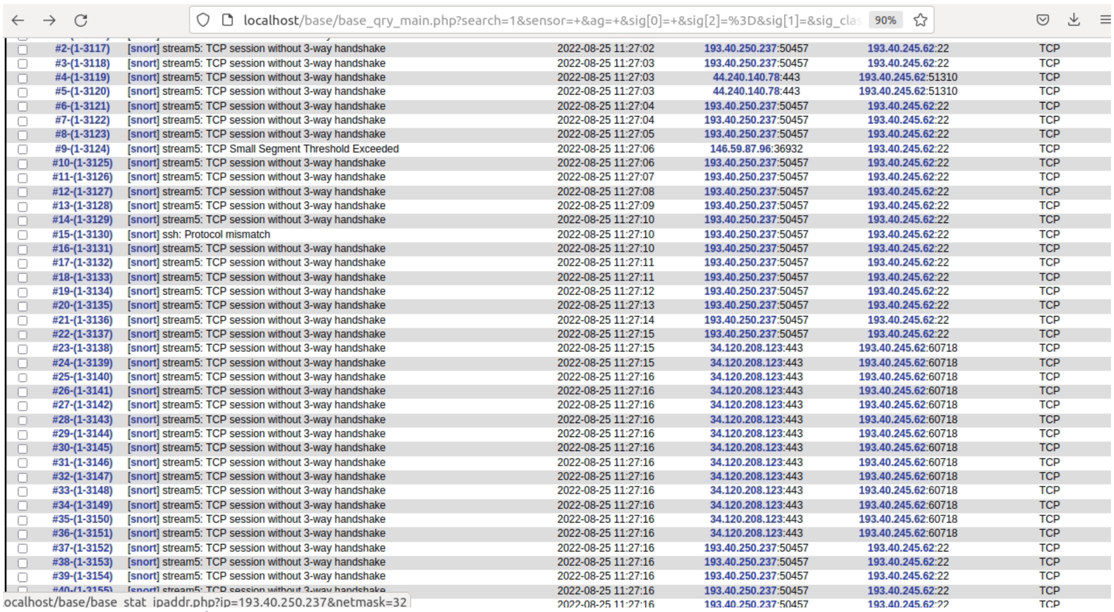


Figure 17. IDS/IPS alerts generated during test case 1.2, no alerts related to FTP protocol

4.3.1.3.3 RITA

Prior to the attack, the RITA operator had already modeled the multimodal transport ecosystem in order to get the business service (namely Taltech-Teleoperation) overall risk and impact, as shown in Figure 18.

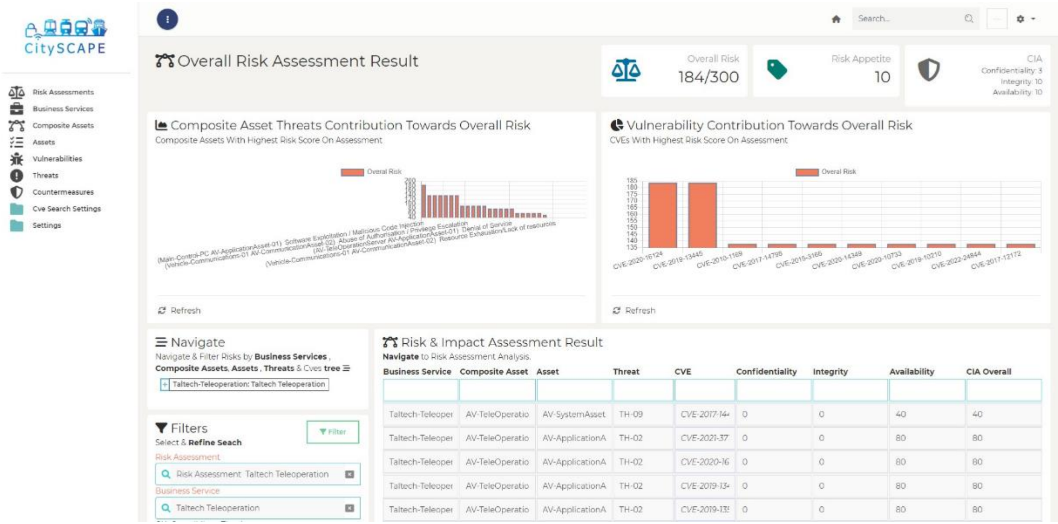


Figure 18. Overall Risk and Impact

For that reason the risk assessor has decomposed the business service to the list of composite assets as shown in Figure 19 and Figure 20.

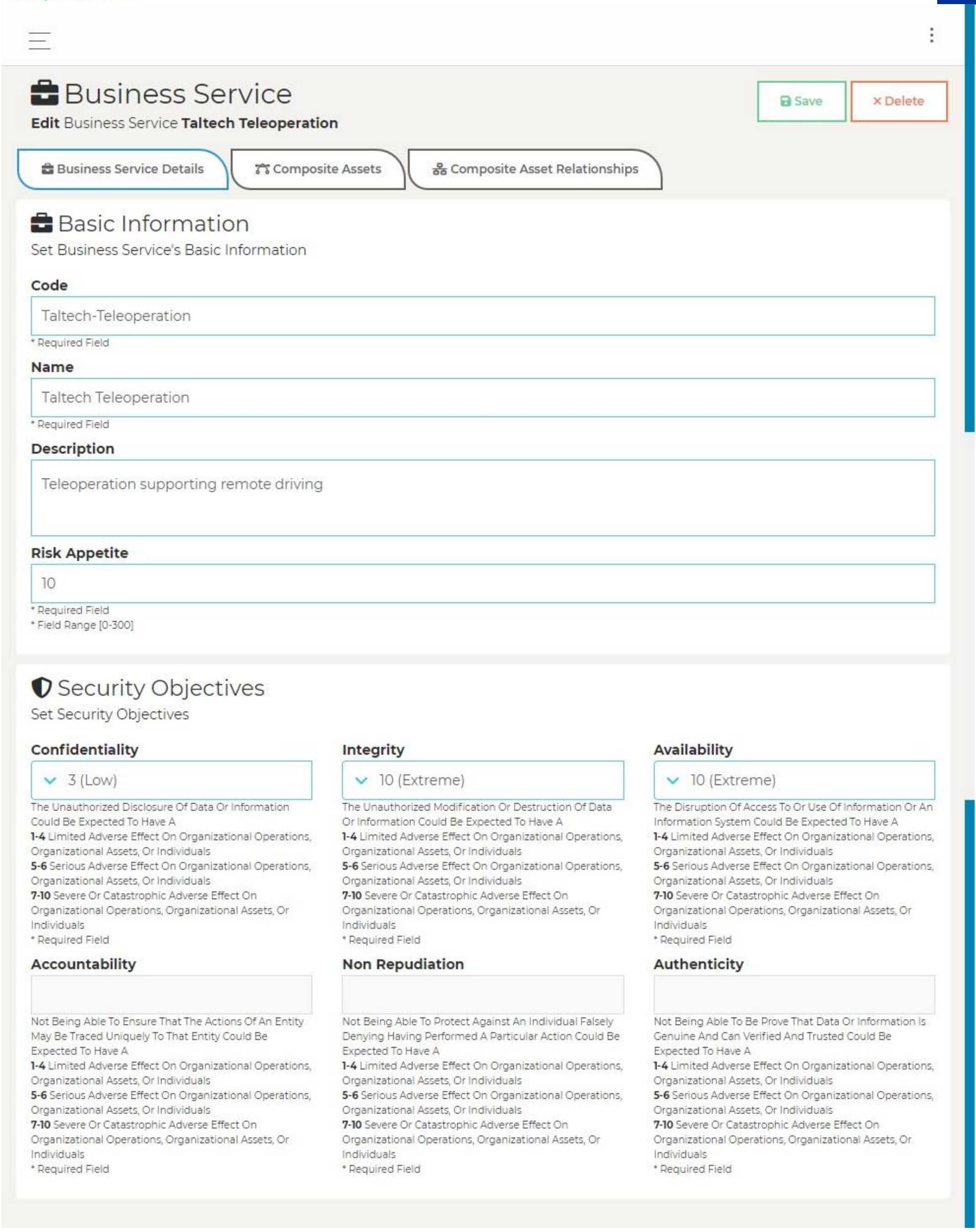


Figure 19. Taltech TeleOperation Business Service (Basic Information)

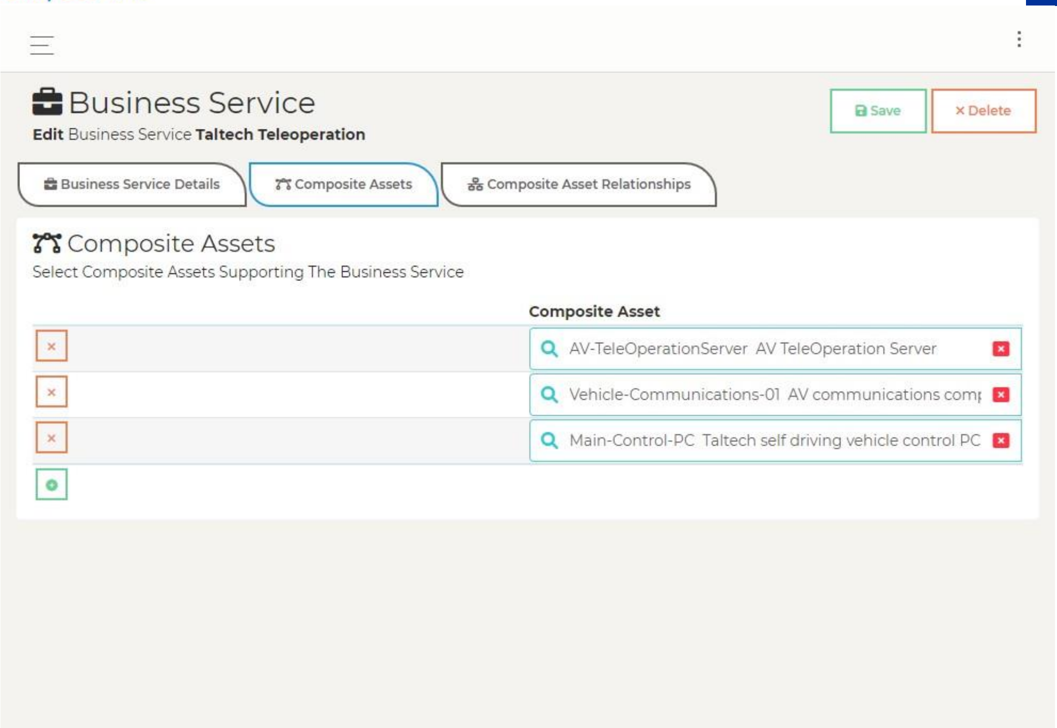


Figure 20. Taltech TeleOperation Business Service (Composite Assets)

Following that, the risk assessor decomposed each composite asset to its basic assets, including the identified threats, their likelihood and any applicable counter measures. TalTech AV TeleOperation Server Threats and Countermeasures are shown in Figure 8.

During the Pilot Demo, as soon as the CSIRP operator has finished their incident analysis, the identified threats and vulnerabilities (included in the IRIS incident reports) were sent to RITA. As a result, the risk assessor had to re-evaluate the security posture and impact of the business service by reviewing and updating the threat probabilities and any available countermeasures. This is depicted also in Figure 21.

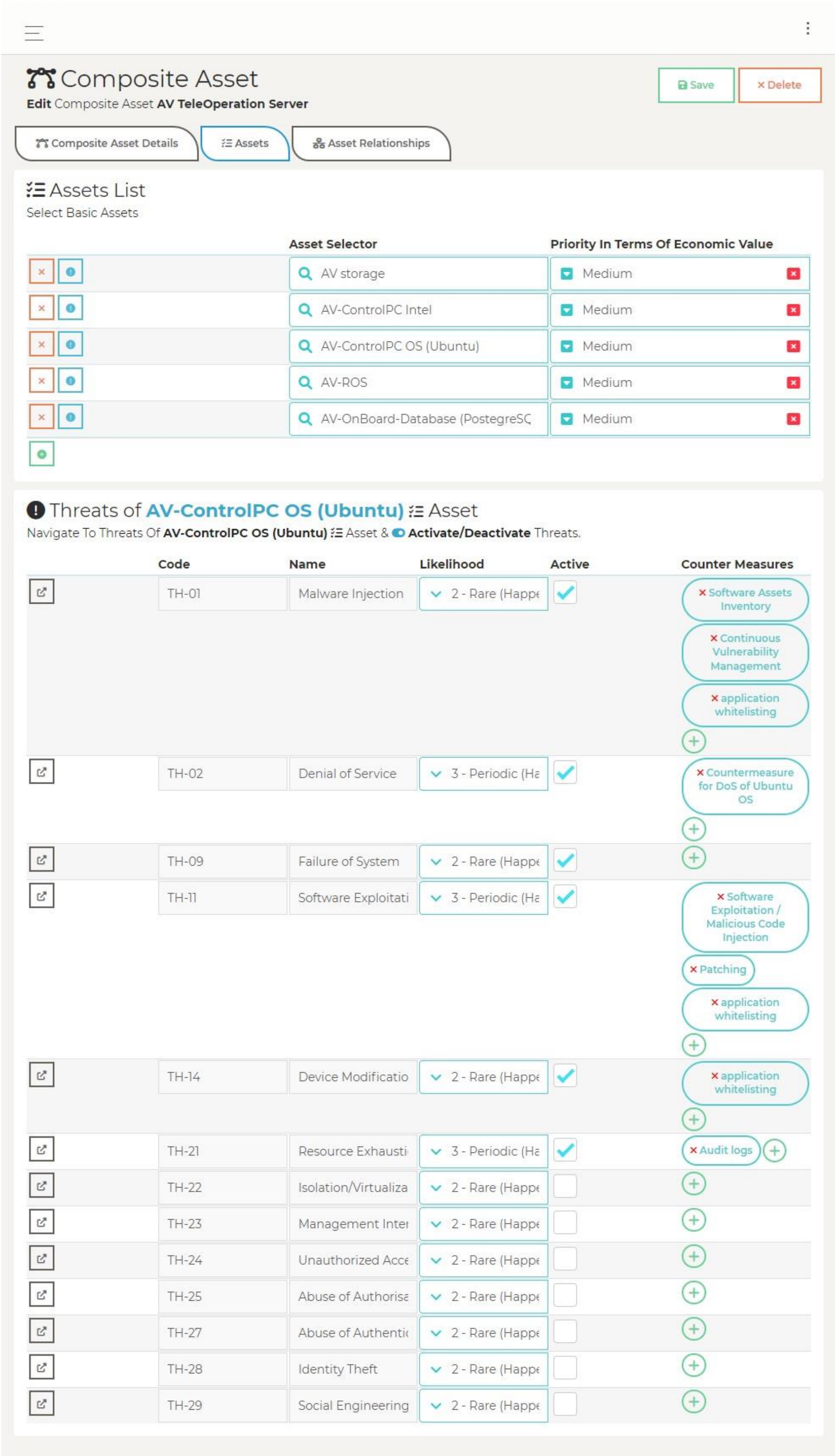


Figure 21. AV TeleOperation Server (AV Control PC OS-Ubuntu Threats and Likehoods)

Additional Figures demonstrating the RITA functionality for the TALLINN Pilot are contained in Annex II.

- For AV TeleOperation Server (AV-TeleOperationServer), this is shown in Annex II *Figure*1, **Error! Reference source not found.**2, **Error! Reference source not found.**3, **Error! Reference source not found.**4, and **Error! Reference source not found.**5, including the assets relationships shown in **Error! Reference source not found.**6.

- For AV communications (Vehicle-Communications-01), this is shown in Annex II **Error! Reference source not found.**7, **Error! Reference source not found.**8, **Error! Reference source not found.**9 and **Error! Reference source not found.**10, including the assets relationships shown in **Error! Reference source not found.**11.

- For Taltech self-driving vehicle control PC (Main-Control-PC), this is shown in Annex II **Error! Reference source not found.**12, **Error! Reference source not found.**13, **Error! Reference source not found.**14, **Error! Reference source not found.**15, **Error! Reference source not found.**16, **Error! Reference source not found.**17 and **Error! Reference source not found.**18, including the assets relationships shown in **Error! Reference source not found.**19.

4.3.1.3.4 FIMCA

4.3.1.3.4.1 Tangible assets

During the Tallinn demo, STAM demonstrated a first release of the FIMCA component, related to the assessment of the financial impact on the tangible assets. FIMCA aims to assess the economic losses associated with the risk assessed by RITA, which instead estimates the risk using qualitative scales. The details about the architecture, version, and deployment of the CitySCAPE FIMCA (Intangible Assets) engine for the Tallinn pilot are shown in chapter 4.3.1.3.4.2.

The user accessed the tool from RITA, after having successfully filled the data related to business services, assets, threats and countermeasures and after having performed a risk assessment of the organization (see chapter 4.3.1.3.3).
In FIMCA, the user found in the Homepage two configurations: the “baseline” and the “secured”. The first configuration included the data that have been set in RITA, in particular the countermeasures currently applied. The second one included the countermeasures that the user aim to implement in its organization. These two configurations are then compared in the Cost Benefit Analysis to assess the sustainability of the “secured” configuration that has been created.

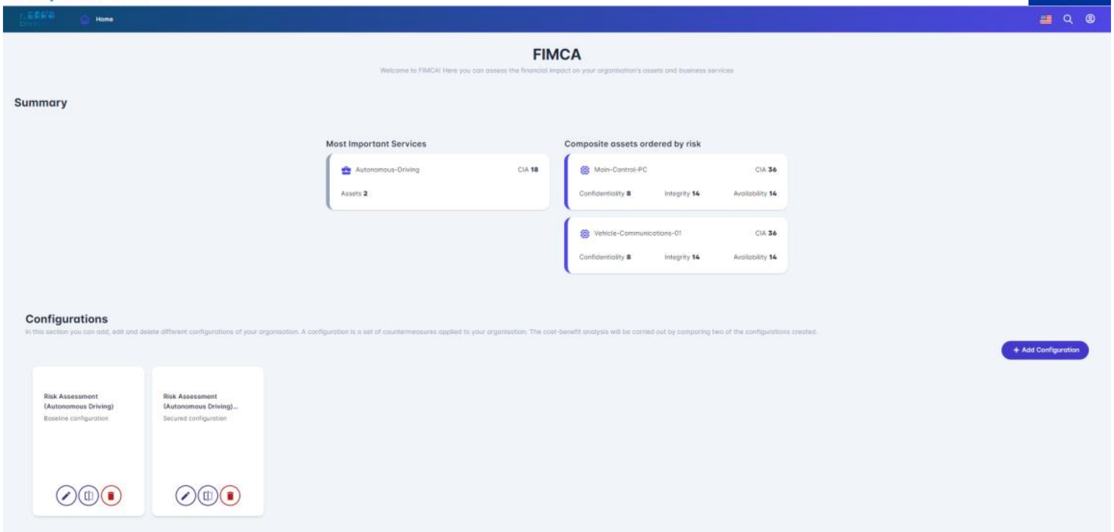


Figure 22. FIMCA Homepage

To perform the CBA, the user inserts additional data on FIMCA regarding to his organization. The data are related to company size, the number of employees and the personnel costs (both internal and external). The remaining information is related to the costs of the Composite Assets (defined in RITA) and the financial weight of the investigated service on the company turnover.

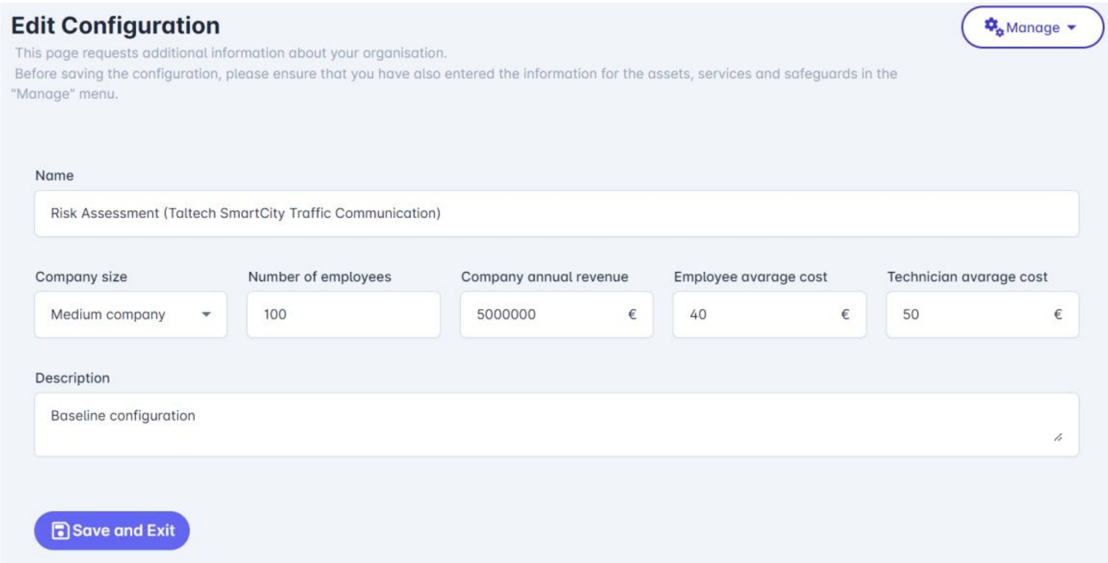


Figure 23. Input data (i)

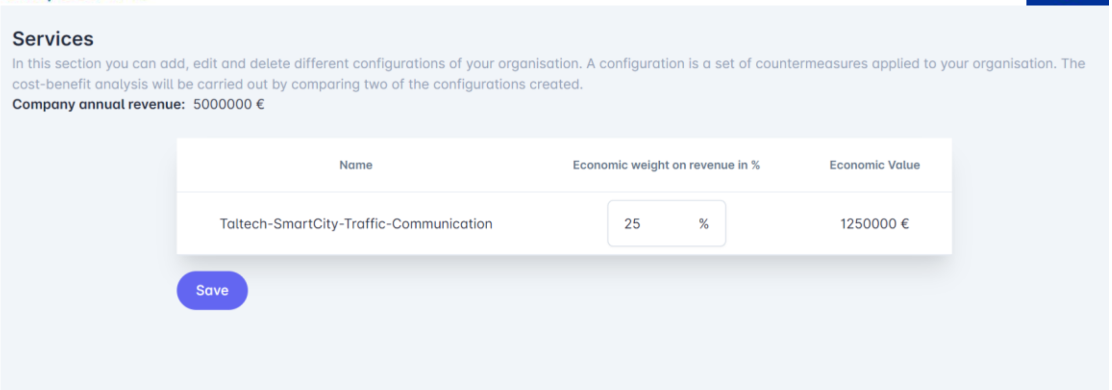


Figure 24. Input data (ii)

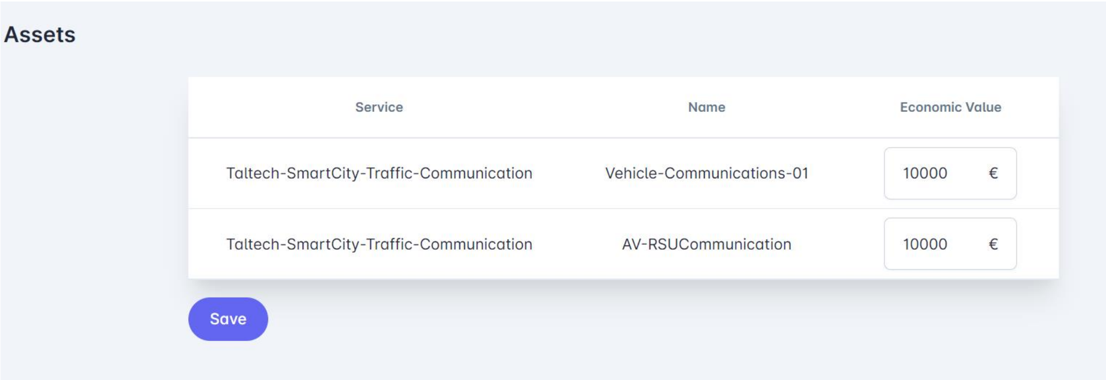


Figure 25. Input data (iii)

Once the required data is inserted, the user selects the countermeasures he aims to apply to the organization. For demonstration reasons, the initial set of countermeasures present in the "baseline" configuration was empty (no countermeasure applied). The "secured" configuration is populated with new cyber-security solutions (provided by the CIS Controls). FIMCA allows the possibility to apply the measures globally (for the whole organization) or for each single asset. During the demo, they have been globally applied to the whole organization. In addition, FIMCA allows the user to modify the costs and mitigation factors of the countermeasures to have more accurate results in the financial impact estimation. However, during the test, information on these costs and these mitigation factors were not modified by the user because he did not have the means and knowledge to do it. The table below shows the information related to the countermeasures selected for the "secured" configuration.

Table 5. Countermeasure's data for "secured" configuration

source_id	confidentiality	integrity	availability	CAPEX	OPEX	Applied
1,2	40	60	50		500	Y
1,3	30	30	20	100		Y
2,3	30	30	15	300	100	Y
2,6	20	25	20		600	Y
2,7	25	0	0	830		Y
3,1	40	40	15		200	Y
3,4	20	25	20		200	Y
3,6	40	35	30	50	108	Y
3,9	30	25	20		100	Y
4,4	30	25	15	2150	300	Y
4,5	45	40	20	2150	300	Y
4,6	40	35	20	100	150	Y
4,9	45	40	30		100	Y
5,4	30	25	30	800		Y
6,2	40	40	30		250	Y
6,3	60	60	40		385	Y
6,7	25	25	15		460	Y
7,2	20	25	15		600	Y
7,3	25	20	25		600	Y
7,5	25	0	0	200	3500	Y
7,6	30	0	0	200	3500	Y
7,7	50	0	0		1000	Y
8,1	35	25	20		200	Y
8,5	50	50	50	200		Y
8,8	25	40	50		600	Y
9,1	25	20	20	100		Y
9,2	40	45	30	100	215	Y
9,3	45	40	35		200	Y
9,4	40	45	40		100	Y
9,5	40	40	40	100	100	Y
9,6	30	35	20		100	Y
9,7	30	35	25		260	Y
10,1	45	45	45	100	45	Y
10,2	40	40	40	50		Y
10,3	45	45	45		50	Y
10,4	35	35	35	100		Y
10,5	50	45	40	50		Y
10,6	40	40	40		50	Y
10,7	30	30	30	200	120	Y
11,2	0	40	30	50		Y
12,3	50	30	30	5000	200	Y
12,5	60	35	30	1300	100	Y
12,7	60	40	30	4400		Y
13,1	70	40	35	2400		Y
13,1	0	30	25		600	Y
13,11	60	55	55	2700	500	Y
15,5	10	10	10		100	Y
15,6	10	10	10		200	Y
15,7	40	30	30		200	Y
16,1	60	55	55		100	Y
16,3	40	40	40		100	Y

source_id	confidentiality	integrity	availability	CAPEX	OPEX	Applied
16,5	30	30	30		200	Y
16,12	75	60	60		600	Y
16,13	50	50	50		1200	Y
16,14	50	50	50		1200	Y
17,1	0	30	30		200	Y
17,2	0	30	30		100	Y
18,2	60	60	60		200	Y
18,3	80	80	80		100	Y
18,4	85	80	80		200	Y
18,5	65	60	60		400	Y

Through the ROSI index, the results of the cost-benefit analysis show the quality of the changes made to the set of countermeasures. The ROSI takes into account the financial impact of the original configuration (the "baseline"), the "secured" one and the cost of the solutions adopted (the countermeasures implemented in the "secured" one). If the ROSI is negative, then the solutions are ineffective, because the balance is negative. On the other hand, if the ROSI is positive, it means that the new configuration is effective and has an overall reduction in the organisation's costs. The FIMCA results also show an overview of the applied countermeasures, indicating the number of controls of the different CIS control groups applied to the different configurations.

Figure 26. Results of FIMCA - tangible assets

4.3.1.3.4.2 Intangible assets

The details about the architecture, version and deployment of the CitySCAPE FIMCA (Intangible Assets) engine for the Tallinn pilot are provided in this section.

Infrastructure - The architecture of the FIMCA engine is based on an Angular user interface, consuming the REST API endpoints of a Spring-Boot service.
The exposed API are well documented using the OpenAPI standard and secured via the shared authentication, thatauthentication, which is the Single Sign-On, thanks to the OpenID Connect and OAuth 2.0 protocols.

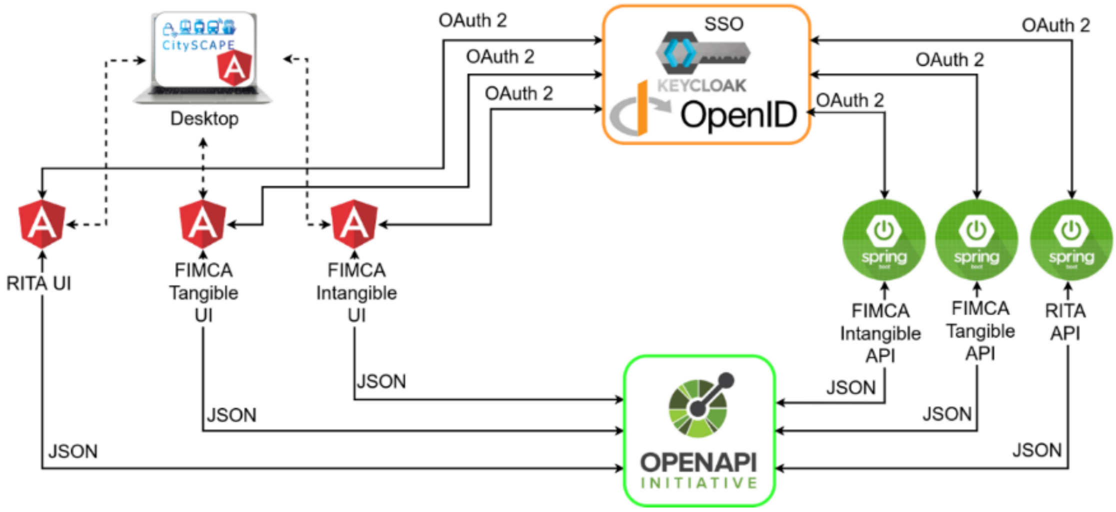


Figure 27. FIMCA Integration Architecture

The authentication mechanism is therefore possible thanks to the adoption of a mature and reliable Identity and Access Management (IAM) system such as Keycloak. However, it can be easily replaced by any other IAM supporting the OpenID Connect standard.

Version - The version of the engine used for this demonstration is tagged as 1.0.0 and includes all the main features, as well as the required scripts to Dockerize and deploy the tool on any system supporting the Docker engine.

Deployment - Thanks to the Docker images available for both the Angular app and the Spring-Boot service, deploying the FIMCA engine for Intangible Assets is just a matter of configuring a few environment variables and running two docker-compose commands.
The deployment has been executed on an ENG server by using the provided Docker-Compose file and instructions. As a result, the bare minimum to run the FIMCA engine is to have a machine with Docker and Docker-Compose installed.

Demonstration - At the Tallinn demonstration, ENG provided a detailed overview of the FIMCA engine for intangible assets. Starting from the security configurations, coming from the RITA and FIMCA for tangible assets engines, and listed in the following picture, the goal is to evaluate the economic impact in case of an intangible asset being compromised.

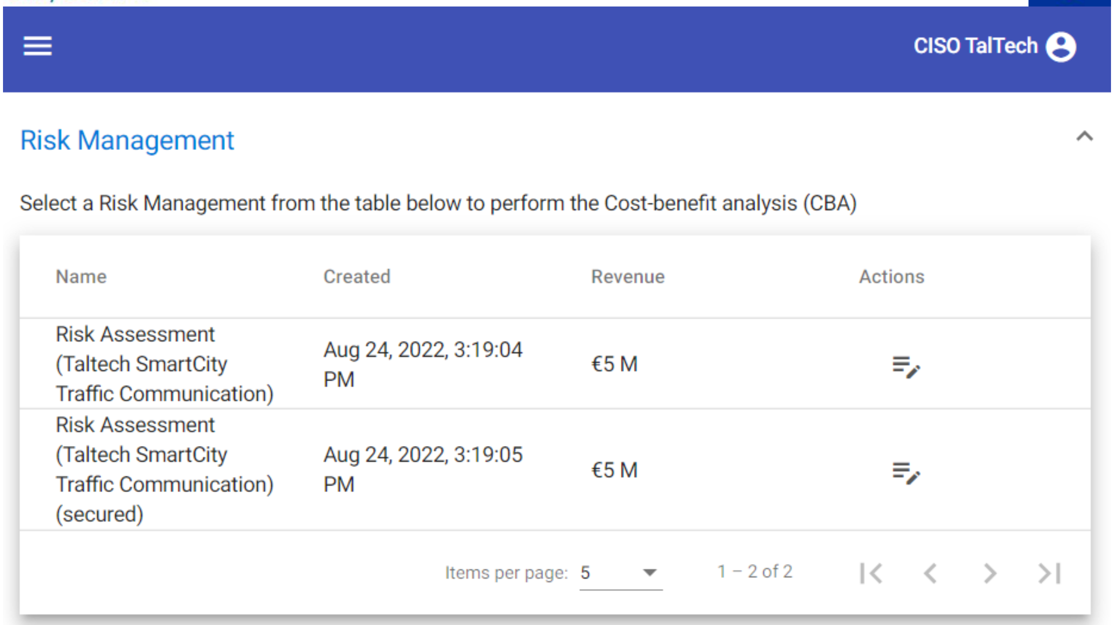


Figure 28. FIMCA Security configuration

The user can therefore select one of the risk-assessment configurations from the list and proceed with the impact evaluation step of a business service.

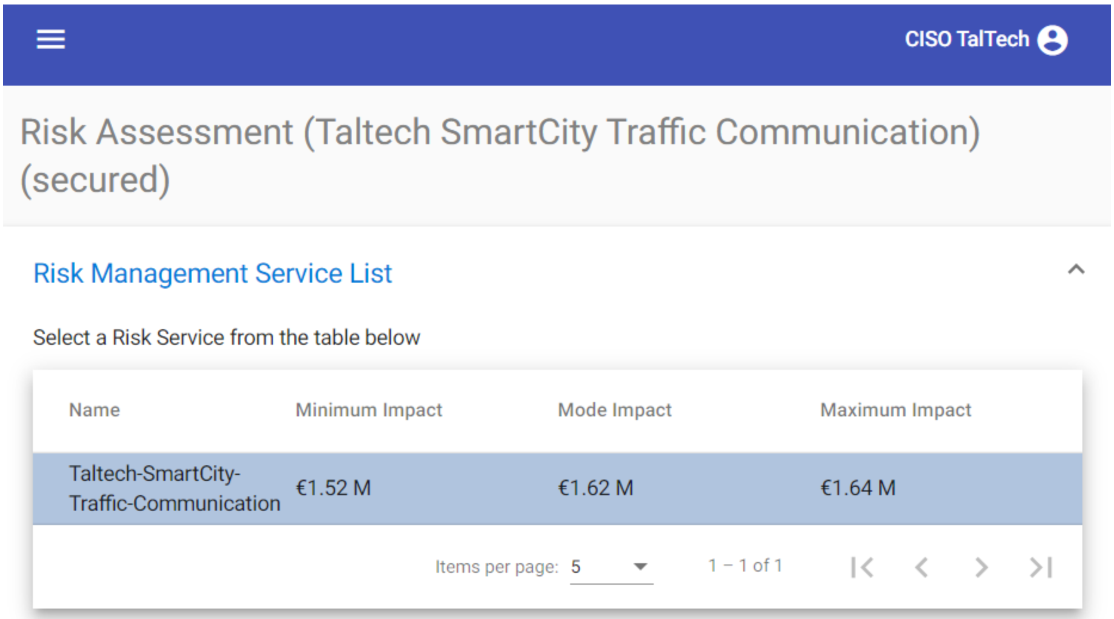


Figure 29. FIMCA impact evaluation

Each business-service can contain different composite assets and each one can be analysed on its own for the impact evaluation.

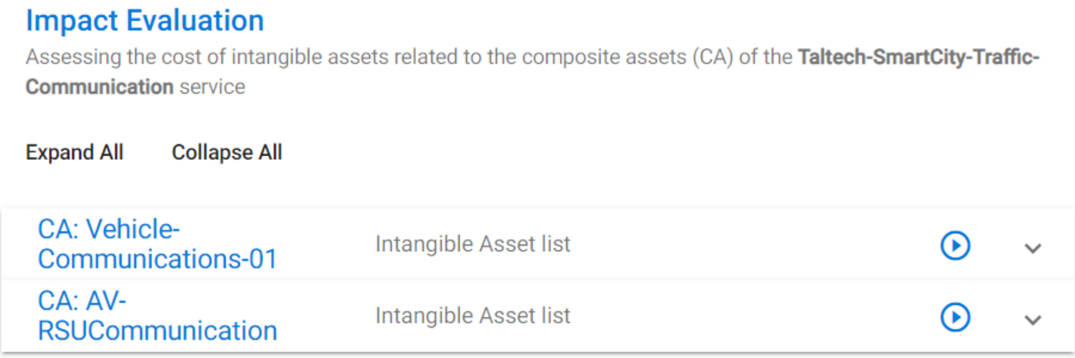


Figure 30. FIMCA list of composite assets

Once selected a composite asset, the engine lists all the connected intangible assets that could be indirectly compromised. For each intangible asset, the engine provides a suggestion of the possible impacts (minimum, mode, maximum) in case of attack, based on the revenue of the organization. The user can then customize the initial values as desired if he has deeper knowledge about them. When the user has completed the definition of the different impact values, at first, he can proceed to the definition of the resulting PERT distribution and then he can execute the Monte-Carlo simulation for the possible impacts.

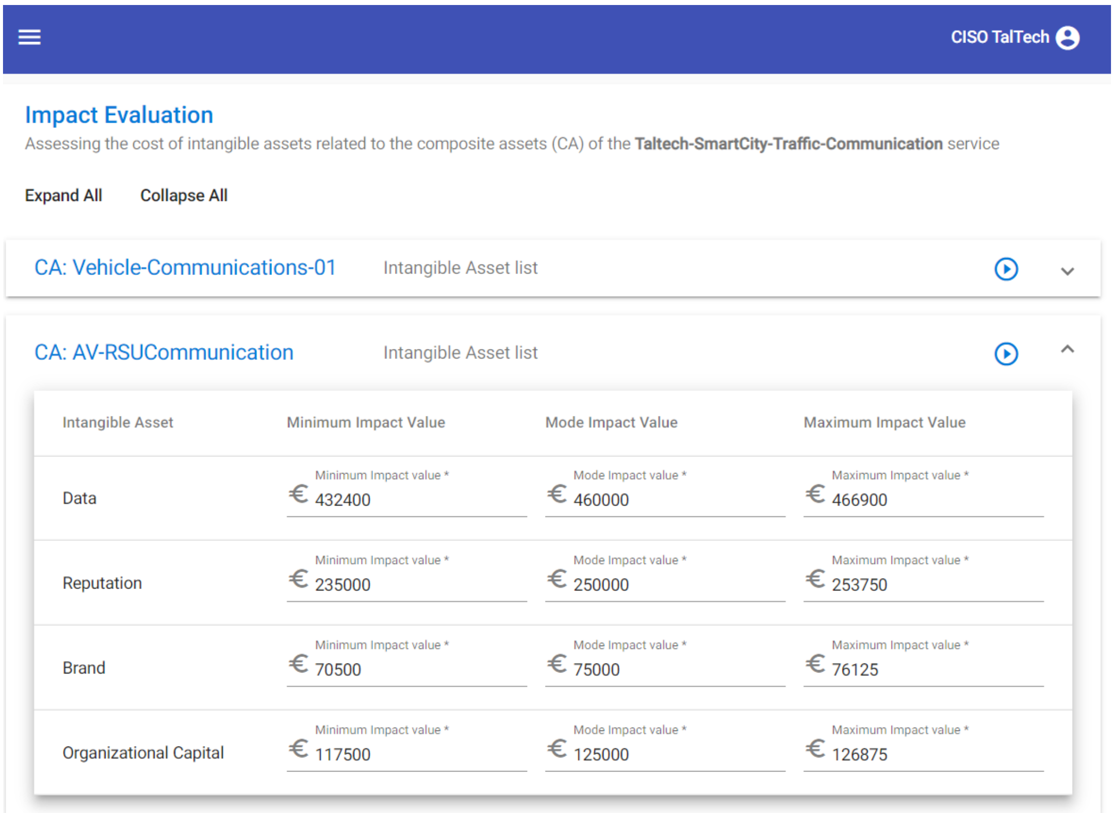


Figure 31. FIMCA suggestion of the possible impacts

The results of the Monte-Carlo simulation are displayed both in tabular and chart format.

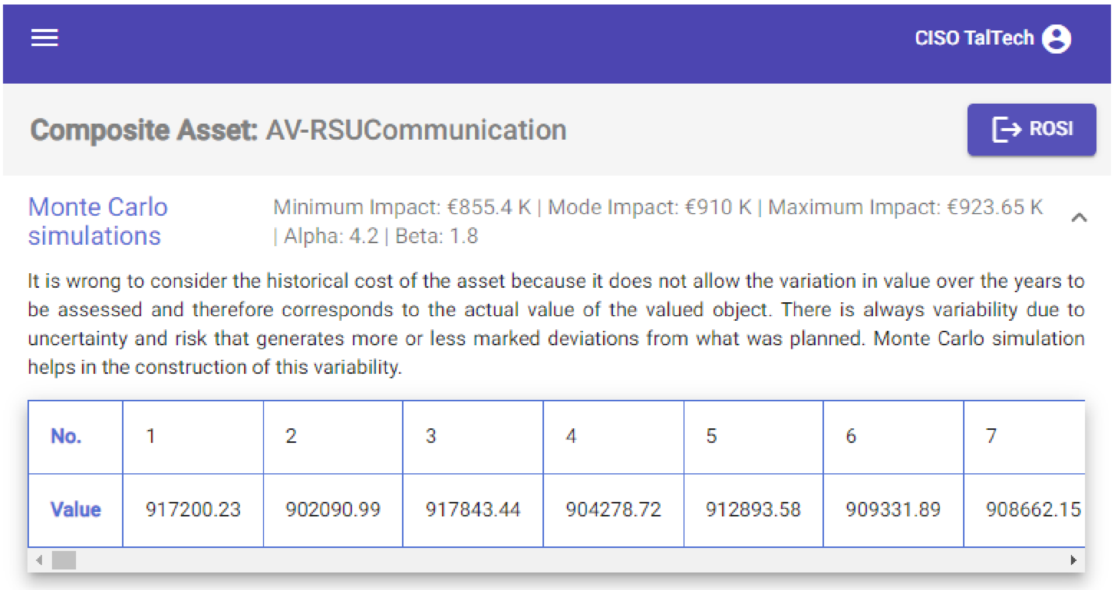


Figure 32. FIMCA Mont-Carlo simulation results

Taking into account all the generated values for the possible impacts, the engine calculates some representative statistics, useful for the next step of the cost-benefit analysis, that are visible after clicking on the ROSI button positioned on the top-right corner of the page.

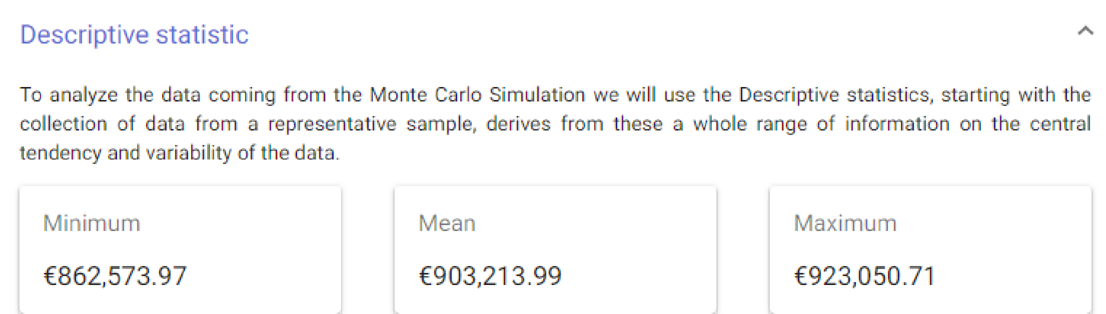


Figure 33. FIMCA calculated statistical values for CBA

At the beginning of the ROSI Analysis page, a brief description of the ROSI formula and its parameters can be found, before moving to the actual results.

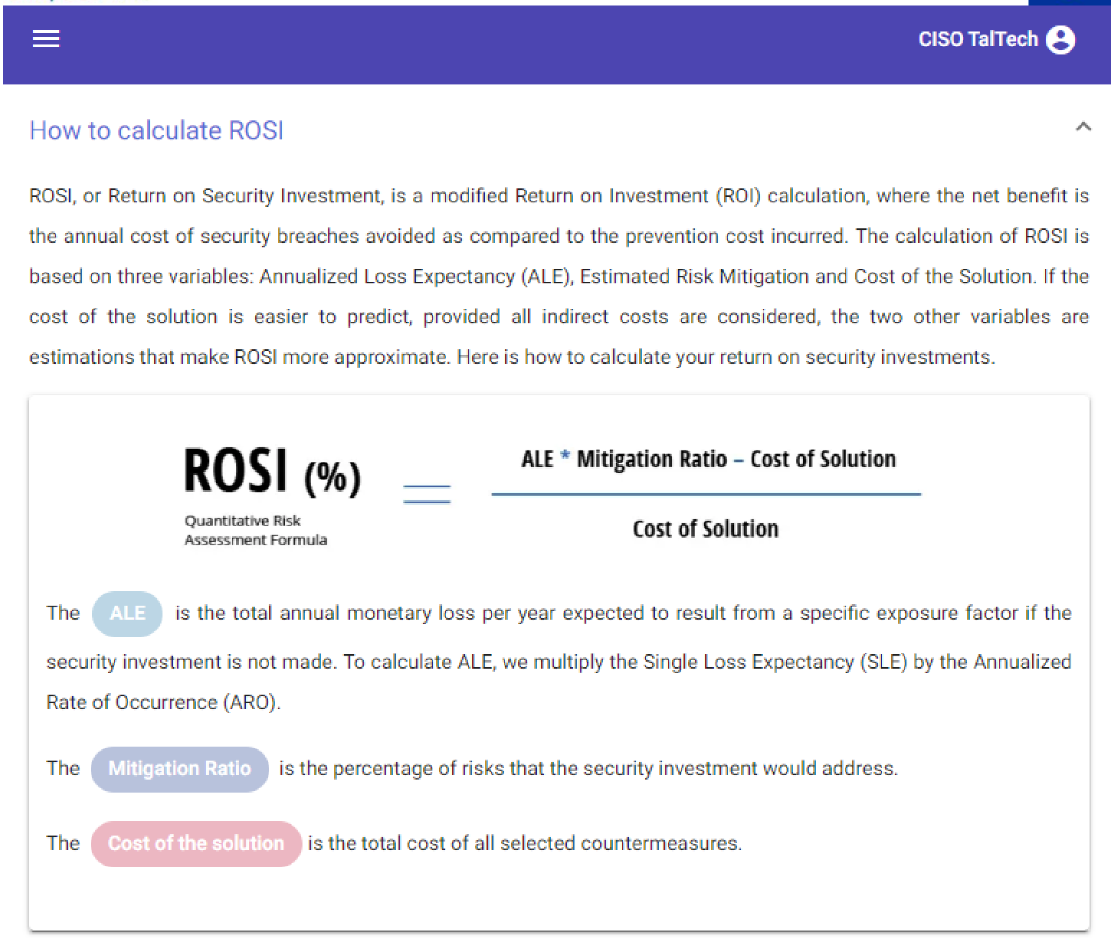


Figure 34. ROSI formula and its parameters

The ROSI analysis considers a single composite asset at each time and all its interconnected intangible assets.

The cost of the countermeasures and their individual values of mitigation ratios for confidentiality, integrity, availability are used to calculate the total cost, the total mitigation ratios, as well as an average overall mitigation ratio. These values are then used to calculate the three different values (confidentiality, integrity, availability) of ROSI and an average ROSI that considers all of them.

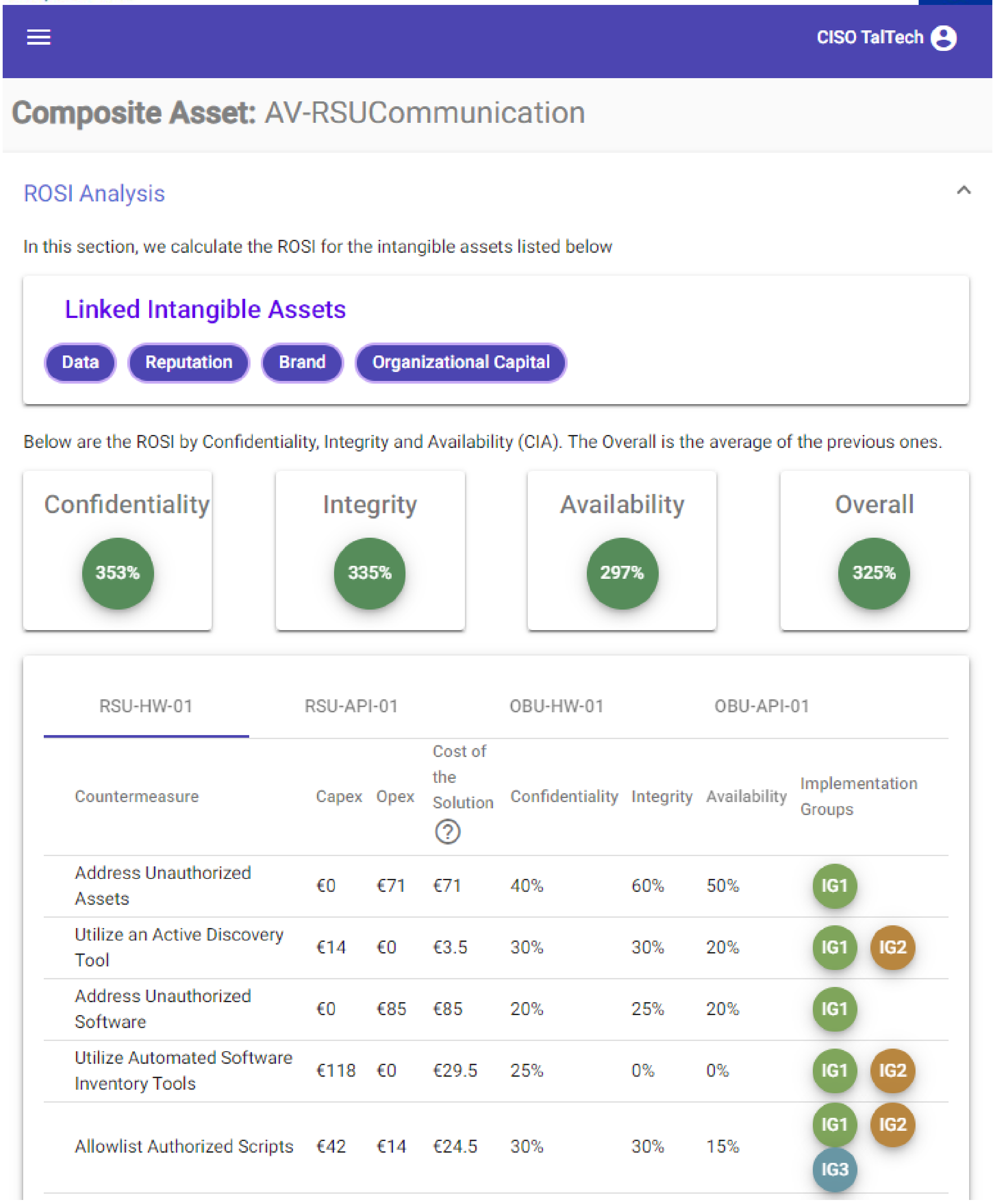


Figure 35. Three different values of ROSI (confidentiality, integrity, availability)

The evaluation of the FIMCA results found issues with its integration with RITA and with the ingestion of intangible assets. The shortcomings have been identified and will be remediated in September and October, to allow the demos to be conducted again.

4.3.1.3.5 CTIP

CTIP was not active in this test-case. In the background, Graylog periodically launches requests to the CTIP to gather relevant IOCs. Since the attacker in the test-case 1 was a new unknown actor, no data was available to enrich the alert generated.

4.3.1.3.6 CSIRP

CSIRP was displayed as a stand-alone application in this test-case, where an analyst created a case to continue investigations.

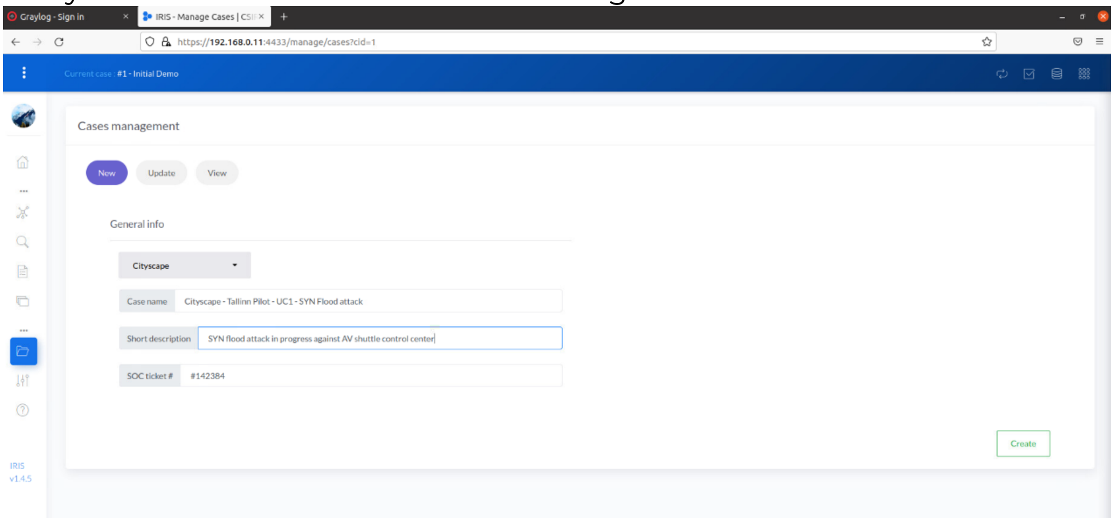


Figure 36. CSIRP analyst created

4.3.2 Test Case 2: Integrity of Multi-Modal Intelligent Road Sign Infrastructure

4.3.2.1 Pilot scenario description

The defined scenario for the Tallinn Adaptive Traffic Control test-case is as follows:

1. A city bus/trolley and the autonomous vehicle shuttle travel through the smart campus roadway of the TalTech Mektory.
2. The Autonomous vehicle shuttle reaches an intersection.
3. The Autonomous vehicle shuttle communicates with the smart city traffic management road sign unit.
4. The traffic management node then receives communication from the RSU and a traffic control decision is made. This is communicated back to the RSU and then from the RSU to the AV Shuttle.
5. The TalTech Smart Campus Traffic Management monitors the traffic environment, and the teleoperation operator monitors the safety of passengers on the AV shuttle.

The assets involved in this scenario are listed below:

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Mobile Network (4G/5G/)	Network	TalTech	4G and 5G Router	Via network (DSRC, UDP, TLS1.3) to anyone having a valid subscription to the network (Access via 2F Authentication using FIDO tokens and VPN).	Communication between Remote Operations Center and AV Shuttle.

Adhoc vehicular network	Network	Taltech	-	Via ITS messages to anyone part of the ITS-V2X network OBU (CohDA Mk5) RSU (CohDA MKx) CAMS Messages (CohDA proprietary protocol (MAP, SPAT, etc.), ITS-G5 Application Compliant).	Direct adhoc communication between vehicles and roadside units.
Autonomous Self-Driving Shuttle					
Vehicle on-board Computer	Hardware	Taltech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Applications (ROS, Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.
Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is part of ROSbag logging system.	The video files from on-board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo-location/ SLAM.
IMU	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS.	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communication modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on-board unit and sensors and router. Manages access to the network and segments network in VLANs).
AV Shuttle Operating System	Middleware/Firmware OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self-driving application	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services	Autoware.ai Application framework for self-driving vehicles.

				Database connectors	
Teleoperation services	Hardware, Middleware, Software, Data, Redundancies	Teleoperation Services Provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperation Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
AV OBU	Hardware, Firmware, Software	TalTech	Hardware – Network ports, Firmware/Router OS, web application	CAMS (SPAT, MAP) CohDA proprietary protocol (ITS-G5)	On-board unit for communication with CohDA MKx smart RSU.
AV Shuttle Journey Planning Web Interface	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI Integrations with sensor/telematics data	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI	Uses the GNSS location data to present a web interface to track the AV shuttle .
HSM	Hardware, Firmware, Software	Taltech		Network interface (Ethernet) Physical access (USB, Serial) HSM interfaces (STM32)	Hardware security module for the certificates of the V2X/ITS PKI. HSMs are contained in the embedded STM controllers in the Autonomous Vehicle and embedded IoT devices such as OBU, RSU.
Actuators	Hardware, Firmware, Software	Taltech		Network interface (Ethernet, CAN)	Actuators
			Smart City Campus Infrastructure		
Smart RSU	Hardware Firmware, Software	TalTech	Hardware – Network ports, Firmware/Router OS, web application	CohDA proprietary protocol (ITS-G5)	Illuminated road side unit which contains the CohDA OBU.
Smart RSU Relay	Hardware	TalTech	Network-Arduino	CohDA proprietary protocol (ITS-G5)	Arduino relay device for traffic light.
Traffic Management Server	Hardware, Software	TalTech	Hardware – Network Ports, Physical Disk etc. Software – Application, OS, firmware	Intelligent Traffic Management Software.	Traffic management node for communication with RSUs.

Table 6. Assets involved in the scenario 2

4.3.2.2 Attack scenarios

The aim of Test-Case 2 (Adaptive Traffic Management) is to test the CitySCAPE toolkit's ability to detect cyber-attacks that target the integrity of the data and systems of the adaptive traffic management (V2X, OBU) process. The integrity of the adaptive traffic management data and systems is of utmost importance for ensuring safe navigation of multi-modal transportation components and users that use the traffic system. In this scenario, network traffic for V2X and AV OBU communication is enabled and the systems such as the AV OBU and V2X OBU are operational.

As in the previous test case, in order to perform test case 2 and try to attempt to affect the integrity of the roadside infrastructure, the following attack scenario steps were implemented:

1. **Fingerprinting -** Trying to identify targets and potential vulnerabilities;
2. **Getting in** - Trying to exploit vulnerabilities to break in;
3. **Modification of data** sent by the vehicle to the control server.

To perform this scenario and after several preliminary tests, Oppida has finally used the following tools in order to implement the attacks:

- Nmap,
- Wfuzz,
- Web browser,
- Postgres command lines,
- Hydra / crunch,
- Existing exploits scripts.

Due to the demonstrator configuration, it has not been possible to directly attack the roadside equipment. Attacks towards the ITS communication have been performed through the elements accessible by the central server and the vehicle network.

As in test case 1, this test case has also been divided into the same 2 sub test cases. The first case (sub-testcase 2.1) consisted in identifying and attacking targets from the internet (system elements with public IPs), which also targeted the control server (see Figure 1). In fact, this server hosts the postgresql database containing all the driving information sent by the vehicle to the server.

The second sub-testcase (sub-testcase 2.2) focused on identifying and targeting vulnerable vehicle sensors to modify their configuration or the data they transmit to the control server. This scenario focused on targeting the lidar administration web interface, as depicted in *Figure 37*.

More specifically for sub-testcase 2.1 a dedicated password list has been generated to brute force (with hydra) the PostgreSQL interface accessible from the internet to gain access to this data and then modifying it, while for the sub-testcase 2.2, the web administration interface has been used via web to modify the sensor configuration.

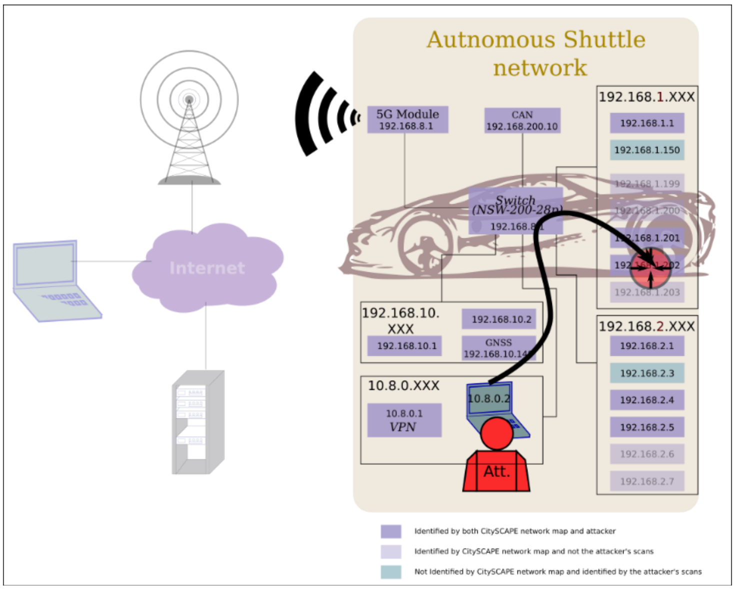


Figure 37. Sub-test case 2.2 involved elements

4.3.2.3 Modules behaviour

4.3.2.3.1 SIEM

Graylog - Graylog receives alerts from the IDS/IPS component. In particular, during the scanning activity, several messages concerning the 'reset outside window ' were received.

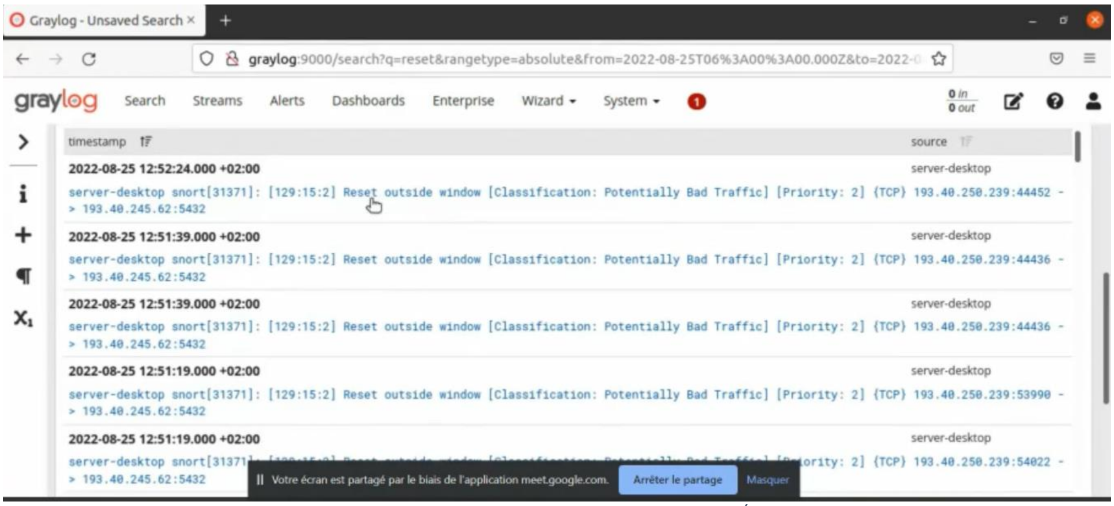


Figure 38. Graylog receives alerts from the IDS/IPS component

This alert was not enough to conclude that an attack was in progress.

4.3.2.3.2 IDS/IPS engine

In this test case, the IDS/IPS engine was still running in online mode. The new alerts identified during this attack were the following:

- Snort Alert [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [Classification: Potentially Bad Traffic] [Priority: 2]
- Stream5: Reset outside window [Classification: Potentially Bad Traffic] [Priority: 2]

In Figure 40, the summary of alerts generated during a specific time frame is depicted (12:59 CEET): the last one summarizes the alerts related to the PostgreSQL brute force.

In Figure 39, all the alerts have been generated during the whole sub-testcase 2.1.

Displaying alerts 1-5 of 5 total

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[snort] stream5: Reset outside window	bad-unknown	6610(7%)	1	2	2	2022-08-25 12:50:23	2022-08-25 12:50:59
[snort] stream5: TCP Small Segment Threshold Exceeded	bad-unknown	3577(4%)	1	1	1	2022-08-25 12:50:23	2022-08-25 12:50:59
[snort] ssh: Protocol mismatch	non-standard-protocol	80(0%)	1	1	1	2022-08-25 12:50:13	2022-08-25 12:50:59
[snort] stream5: TCP session without 3-way handshake	bad-unknown	1825(2%)	1	4	2	2022-08-25 12:50:00	2022-08-25 12:50:59
[snort] Snort Alert [1:2010939:3]	bad-unknown	5(0%)	1	1	1	2022-08-25 12:50:23	2022-08-25 12:50:23

ACTION

{ action } Selected ALL on Screen

Figure 39. IDS/IPS unique alerts generated during sub-testcase 2.1

Displaying alerts 1-27 of 27 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-88843)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:10	118.193.31.186:46200	193.40.245.62:5432	TCP
#1-(1-88839)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:09	118.193.31.186:46162	193.40.245.62:5432	TCP
#2-(1-88838)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:08	118.193.31.186:46130	193.40.245.62:5432	TCP
#3-(1-88832)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:59:04	118.193.31.186:45950	193.40.245.62:5432	TCP
#4-(1-88806)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:58:42	118.193.31.186:54350	193.40.245.62:5432	TCP
#5-(1-77712)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:51:46	193.40.250.239:44452	193.40.245.62:5432	TCP
#6-(1-77369)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:51:39	193.40.250.239:44436	193.40.245.62:5432	TCP
#7-(1-62180)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54330	193.40.245.62:5432	TCP
#8-(1-62179)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54246	193.40.245.62:5432	TCP
#9-(1-62178)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54250	193.40.245.62:5432	TCP
#10-(1-62177)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54326	193.40.245.62:5432	TCP
#11-(1-62176)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:50:23	193.40.250.239:54252	193.40.245.62:5432	TCP
#12-(1-61430)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:12	162.142.125.160:5189	193.40.245.62:5432	TCP
#13-(1-61429)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:11	162.142.125.8:43102	193.40.245.62:5432	TCP
#14-(1-61428)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:11	162.142.125.8:35286	193.40.245.62:5432	TCP
#15-(1-61423)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:11	162.142.125.8:42748	193.40.245.62:5432	TCP
#16-(1-61422)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:45:10	162.142.125.136:24619	193.40.245.62:5432	TCP
#17-(1-60762)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:38:27	193.40.250.239:58232	193.40.245.62:5432	TCP
#18-(1-60749)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:38:18	193.40.250.239:28285	193.40.245.62:5432	TCP
#19-(1-60343)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45492	193.40.245.62:5432	TCP
#20-(1-60342)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45490	193.40.245.62:5432	TCP
#21-(1-60341)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45542	193.40.245.62:5432	TCP
#22-(1-60340)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45496	193.40.245.62:5432	TCP
#23-(1-60339)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:35:28	193.40.250.239:45494	193.40.245.62:5432	TCP
#24-(1-58055)	[snort] Snort Alert [1:2010939:3]	2022-08-25 12:10:30	212.70.149.10:58026	193.40.245.62:5432	TCP
#25-(1-5395)	[snort] Snort Alert [1:2010939:3]	2022-08-25 11:41:05	36.139.53.192:54051	193.40.245.62:5432	TCP
#26-(1-5365)	[snort] Snort Alert [1:2010939:3]	2022-08-25 11:40:42	37.157.70.163:38404	193.40.245.62:5432	TCP

ACTION

{ action } Selected ALL on Screen Entire Query

Figure 40. All the IDS/IPS alerts related to PostgreSQL brute force generated during the sub-testcase 2.1

Like sub-testcase 1.2, in sub-testcase 2.2 alerts related to the attack on the sensors in the vehicle (previously described) have not been generated, mostly the reason was that the IDS/IPS engine is deployed on the server machine and was not receiving all the traffic in the subnetwork.

4.3.2.3.3 RITA

Prior to the attack, the RITA operator had already modeled the multimodal transport ecosystem in order to get the business service (namely Taltech-SmartCity-Traffic-Communication) overall risk and impact, as shown in Figure 41.

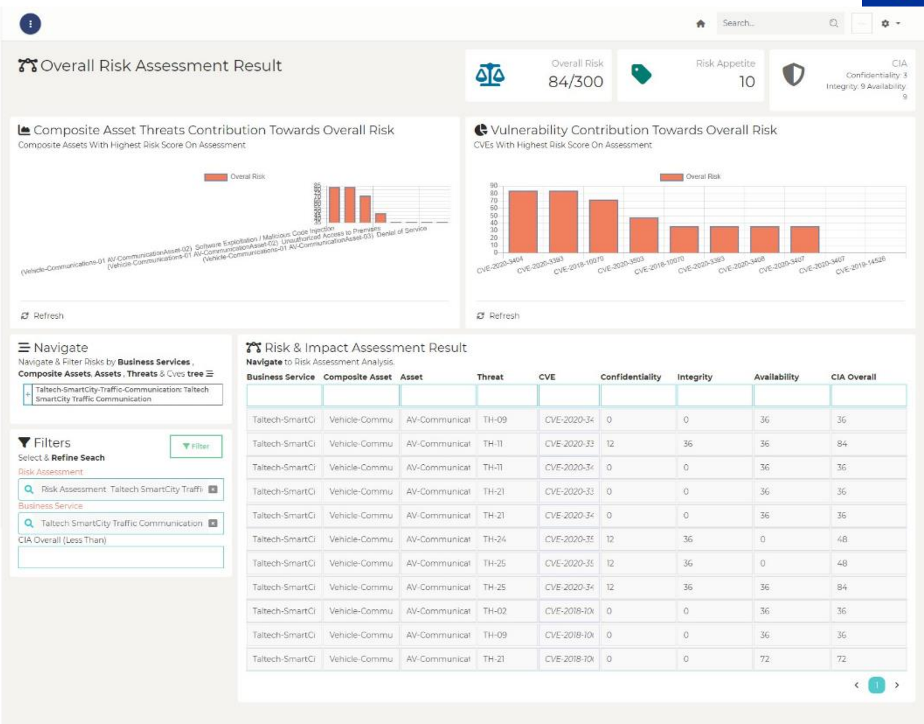


Figure 41. AV Shuttle Network Communication Overall Risk and Impact

For that reason, the risk assessor has decomposed the business service to the list of composite assets, as shown in Figure 42 and Figure 43.

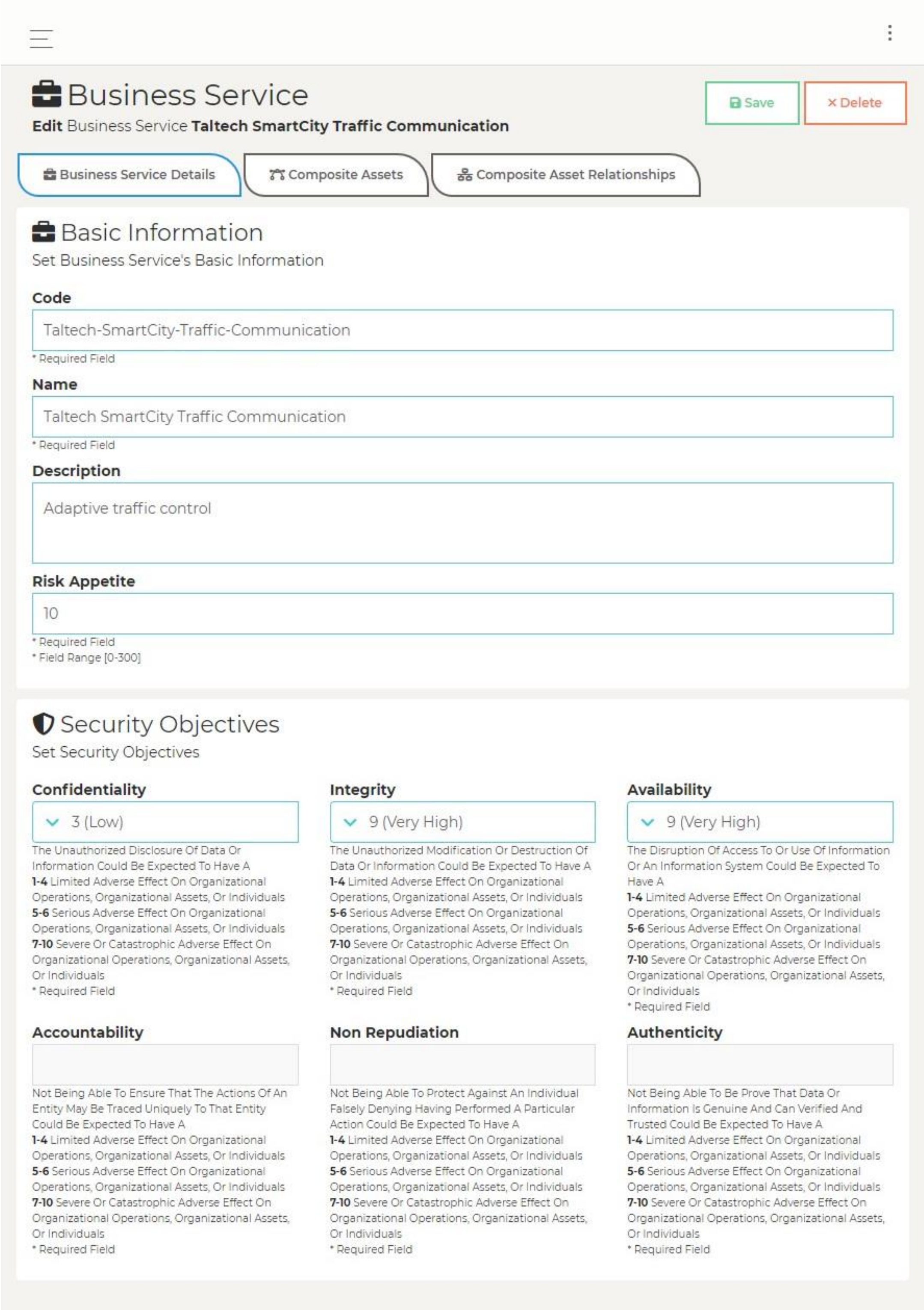


Figure 42. AV Shuttle Network Communication Business Service (Basic Information)

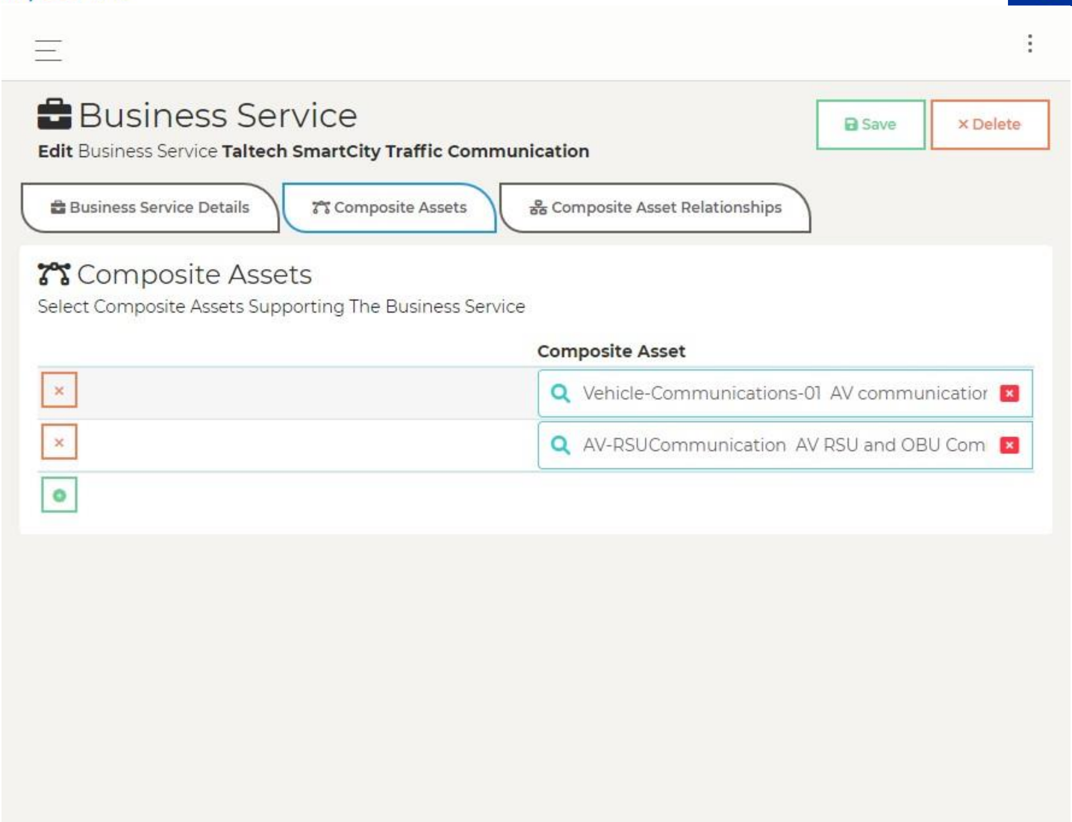


Figure 43. AV Shuttle Network Communication Business Service (Composite Assets)

Following that, the risk assessor decomposed each composite asset to its basic assets, extracting the identified threats, their likelihood and any applicable counter-measures.

During the Pilot Demonstration, as soon as the CSIRP operator finished their incident analysis, the identified threats and vulnerabilities (included in the IRIS incident reports) were sent to RITA. As a result, the risk assessor had to re-evaluate the security posture and impact of the business service by reviewing and updating the threat probabilities and any available countermeasure.

Additional figures depicting the RITA functionality during the Pilot Demonstration can be found in Annex III.

- For AV communications (Vehicle-Communications-01) this is shown in Annex II Figure 7, Figure 8, Figure 9 and Figure 10, including the assets relationships shown in Figure 11.
- For AV RSU and OBU Communications, this is shown in Annex III **Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.** and **Error! Reference source not found.**, including the assets relationships shown in **Error! Reference source not found.**.

4.3.2.3.4 XSOAR

XSOAR was not active in this test-case.

4.3.2.3.5 CTIP

CTIP was not active in this test-case. In the background, Graylog periodically launches requests to the CTIP to gather relevant IOCs. Since the attacker in the use-case 1 was a new, unknown actor, no data was available to enrich the alert generated.

4.3.2.3.6 CSIRP

CSIRP was not active in this test-case.

4.3.2.4 Future activities

Tallinn Pilot permitted identifying that more data was needed inside the SIEM to perform effective detection.
In the following month, log collection from shuttle internal server into Graylog will be implemented, and specific parsers and detection rules will be added to ensure those logs will be correctly exploited. A playbook to handle this incident will also be implemented into the SOAR.

4.3.3 Test Case 3: Fraudulent manipulation of the Payment Validation System

4.3.3.1 Test-case scope

In this scenario, a passenger wants to validate her ticket/card for the transportation journey. The passenger will be on-board the means of transportation. The passenger has multiple methods for ticket validation for her user journey:

- The passenger taps their Tallinn Transport smart card on the Validator.

The desired behaviour of the system is as below:

- The payment validator service/app checks the passenger data against a database. If the smart card, ticket, or credit card are fraudulent/expired/not valid, the validation will be rejected. If the validation is genuine, then a sound from the validator will acknowledge the successful validation.

The following table describes the assets involved in the scenario and the scope of each of them:

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Payment service system	Hardware, Middleware, Software, Data, Redundancies	TalTech	Physical or virtual computing units, Operating System, Application Server, Web services,	Network interfaces (Ethernet, Wifi, 4G, Bluetooth) OS interfaces (SSH, Telnet, RDP, etc.) Docker Flask Web Server Application interfaces (APIs, REST, etc.)	System that manages ticketing service, holds the information on the active subscriptions, allows new registrations and manages payments.

			Databases and DBMS, Log files, configuration data	Database connectors File Transfer Services (e.g., SFTP) NFC interface/RFID interface	
Payment Validation System					
HMI Machine Validator	Hardware, Middleware, Software	TalTech	Hardware (network interfaces, sensors, credit card, micro-computer, touch display), Firmware, OS, Log and configuration files	Network interfaces - RFID, Ethernet, NFC, QR Code, Credit Card, User Interface	Selling/Ticket Validator.
Gateway	Hardware, Middleware, Software	TalTech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Standard computer hw interfaces Network interfaces (Ethernet) OS interfaces (SSH, Telnet, RDP, etc.) Application interfaces (APIs, REST, JSON etc.) Web services Database connectors Interfaces for ISO8583 (financial transactions)	Gateway between ticketing system and the acquiring bank.
Communication Module	Hardware, Middleware	TalTech	Modem, Firmware, Log and configuration files	CAN bus, 3G/4G	Used for communication of the Payment services with internal network and external network.

Table 7. Assets involved in the scenario 3

4.3.3.2 Attack scenarios

The aim of this Test-Case is to test the ability of the CitySCAPE toolkit to detect fraud attacks on the ticket validation system. The integrity of the ticket validation system is of paramount importance for enabling authentication of users and tickets on public transport journeys. This Test-Case focuses on a cyber-attack which consists of a fraudulent user, who has cloned a transportation card to obtain free transport journeys.

The attack was carried out as follows:

1. Ticket validator has a hidden configuration window for connections it makes, that can be found by clicking on the screen. Validator is also not locked in kiosk mode.

2. Knowing IP scan website through the dirb scanner, as follows.
dirb http://193.40.245.62/validator

---- Scanning URL: http://193.40.245.62/validator/ ----
+ http://193.40.245.62/validator/add (CODE:405|SIZE:178)

+ http://193.40.245.62/validator/delete (CODE:401|SIZE:19)
+ http://193.40.245.62/validator/logs (CODE:401|SIZE:19)
+ http://193.40.245.62/validator/manage (CODE:401|SIZE:19)
+ http://193.40.245.62/validator/sync (CODE:200|SIZE:63)

3. Finding validator/sync/ endpoint, which would provide to the attacker valid UID-s.

4. Cloning the card with the UID found in the database, example: DEADBEEF, using mifare card tool on android and magic mifare 1k card.

5. Getting successful validation on the bus using the cloned card.

Other possible attacks include brute force incremental and random sampling.

4.3.3.2.1 Outcome of the vulnerable PoC study

The attack shown during the Pilot could have been detected at the following stages:

- When the attacker scan the server for accessible folders using dirbuster;
- When the attacker accesses the confidential endpoint /sync containing the cards' UIDs.

Those two detections possibilities can only be carried on if the access logs generated by the apache server are sent to Graylog SIEM for analysis, which was not available in the time required for analysis and customisation. The fraudulent manipulation of the payment validation system cannot be detected, since the fraudulent card generated is a perfect clone of the original one; thus, to the system, it appears legitimate. The detection solution presented above can only detect the fact that the information necessary to fraud has been stolen, but not that it has been exploited.

4.3.3.2.2 Future activities

Tallinn Pilot permitted to identify that more data was needed inside the SIEM to perform effective detection. In the following month, log collection from the apache server into Graylog will be implemented, and specific parsers and detection rules will be added to ensure those logs will be correctly exploited. A playbook to handle this incident will also be implemented into the SOAR. Nonetheless, as stated previously, the solution will detect that information necessary to fraud has been stolen, but not that it has been exploited.

4.3.4 Test Case 4: Integrity of GNSS System

4.3.4.1 Test-case scope

This Test-Case has a similar scope with Test-Case 1, i.e. the AV Shuttle provides last-mile transportation for Tallinn Passengers. The difference is in the target system, which, for this Test-Case, focuses on the Global Positioning System (GPS) which localises the transportation mode.

In this scenario, the passenger is able to move from the city transportation mode to the last-mile services (AV Shuttle) seamlessly. The passenger interactions to achieve this are presented below.

1. Passenger departs from the city-transport mode and reaches the AV Shuttle.
2. The AV Shuttle carries the passenger to the end destination.

The following table describes the assets involved in the scenario and the scope of each of them.

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Mobile Network (4G/5G/)	Network	TalTech	4G and 5G Router	Via network (DSRC, UDP, TLS1.3) to anyone having a valid subscription to the network (Access via 2F Authentication using FIDO tokens and VPN)	Communication between Remote Operations Center and AV Shuttle.
Adhoc vehicular network	Network	Taltech	-	Via ITS messages to anyone part of the ITS-V2X network OBU (CohDA Mk5) RSU (CohDA MKx) CAMS Messages (CohDA proprietary protocol (MAP, SPAT etc.), ITS-G5 Application Compliant)	Direct adhoc communication between vehicles and roadside units.
Autonomous Self-Driving Shuttle					
Vehicle on-board Computer	Hardware	Taltech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Middleware (ROS Kinetic Kame) Applications (Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.
Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is stored in the ROSBag logging system.	The video files from on-board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo-location/ SLAM.
IMU	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files,	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.

			configuration data		
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communication modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on-board unit and sensors and router. Manages access to the network and segments network in VLANs).
AV Shuttle Operating System	Middleware/Firmware OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self-driving application	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services Database connectors	Autoware.ai Application framework for self-driving vehicles.
Teleoperation services	Hardware, Middleware, Software, Data, Redundancies	Teleoperation Services Provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperation Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
Actuators	Hardware, Firmware, Software	Taltech		Network interface (Ethernet, CAN)	Actuators

Table 8. Assets involved in the scenario 4

4.3.4.2 Attack scenarios

The aim of this Test-Case is to test the ability of the CitySCAPE toolkit to detect cyber-attacks, which impact the integrity of the GNSS used in the transportation system. Integrity of GNSS is crucial for accurate positioning. The scope of the attack is limited to the GNSS telemetry data received by the AV Shuttle system.

Following the same process as for Test Cases 1 and 2. The attacker performs the following steps:
- **Fingerprinting** - Trying to identify targets and potential vulnerabilities
- **Getting in** - Trying to exploit vulnerabilities to break in;
- **Modification of data** provided by GNSS.

The same tools as for test case 2 were used:

- Nmap
- Web browser
- Postgres command lines,
- Hydra / crunch

Here again, the implied elements were the control server (see Figure 1) as depicted in Figure 44 for test case 4.1 and the GNSS unit located in the vehicle, as depicted in Figure 44. In the first case, the final target was to modify the server PostgreSQL to change the stored GNSS data and in the second case to modify the GNSS service configuration itself to affect the GNSS behaviour.

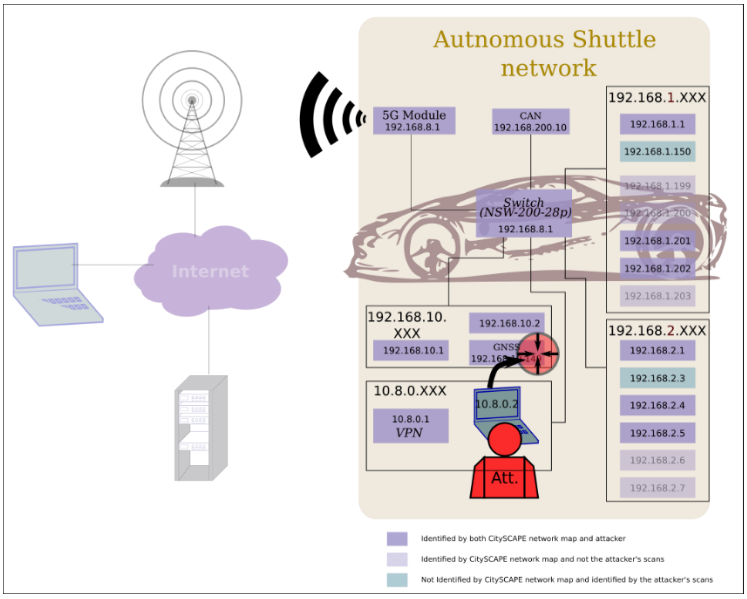


Figure 44. Test case 4.2 involved elements

4.3.4.3 Outcomes

Since this attack involves more complex interactions inside the vehicle data ecosystem than others (the attack was a manipulation of data and did not involve malicious network packet injection or other visible markers), additional time was required to understand which CitySCAPE tools could detect the attack, how and when in the attack kill chain. The attack was workshopped at the TALLINN Pilot and it was conclusion is that the SIEM platform offered the most appropriate tool to detect this attack. The attack couldn't be conducted during the 24th and 25th as additional time is needed to tune and train the SIEM for this attack.

4.3.4.4 Future activities

During the operational data collection (beginning of July) it was found that the shuttle server log generation was not compatible with Graylog log collection interface. Therefore, the data analysis by the SIEM operators could not be conducted in time for the TALLINN Pilot on the 24th and 25th of August. Further developments are needed to create a compatible interface and ensure data necessary for detection is available to the SIEM. This is being progressed in September.

4.3.5 Test Case 5: Transport Data Integration with Mobile Application (SIGLA Move)

4.3.5.1 Test-case scope

As described in the work proposed initially within the DoA, the project would also consider cyber-security aspects related to mobile technology-based services for passengers using multimodal transportations systems.
In particular, the project wants to address matters of relevance related to the management of the citizens' access to a broad set of city-level multimodal transport organizations services. On one side, the secure access management for citizens to all types of vehicles (thanks to mobile based services) is considered, as well as the assurance and protection of citizens and services against specific cyber-attacks in the multimodal transport domain, addressing interconnected threats and propagated vulnerabilities.
The project planned to consider smartphones as the nowadays prominent way to access the multiple means (and the services to use them). As described in deliverable D3.3, the solution implemented integrates in a brand-new development (CitySCAPE Mobile Security Toolkit – also referred as "Mob-Sec"), a commercial product (Kaspersky KMS) to safeguard the passenger's access and data to multimodal transport services.
This Mob-Sec has been integrated into SIGLAMoving, a mobile based solution for the provision of Infomobility services related to multimodal transport systems, that the colleagues from SIGLA designed and developed for CitySCAPE.
This let the consortium to enrich the Tallinn pilot activities (and the project) with activities related to mobile security investigations and experimentation.
Having as objective to validate Mob-Sec - through SIGLAMoving - the efficiency in detecting vulnerabilities and attacks against mobile-based technological solutions and services, four attack scenarios (described within the next section) has been designed, implemented and executed during the Tallinn pilot activities.

As described in CitySCAPE deliverables (e.g., D7.1 "Pilot scenarios, validation plan, and Pre-piloting preparation"), a number of elements are necessary to be available to perform the piloting activities. It needs to consider that the pilot activity - focusing on SIGLAMoving and, consequently, on CitySCAPE Mob-Sec - adopts Kaspersky Mobile Security SDK by KSP on mobile application and integrates with SIEM by ACS and RITA by ED and UPRC.

The elements are reported in the following table.

Name	Type	Managed by / Owned by	Basic Asset Breakdown	Interfaces	Role
Mobile device	*Hardware*	*Tallinn*	*A mobile device where SIGLAMoving (and*	-	*Hosting installation of mobile apps*

			consequently the CitySCAPE Mobile Security Toolkit) can be installed		
Mobile Network (4G/5G)	*Network*	*Tallinn*	*The Mobile device should have access / is endowed of a mobile network access*	*Via SIM card and WiFi*	*Supporting communication features*
SIGLAMoving Mobile App	*Software*	*SIGLA*	*The mobile app delivering both info-mobility services and CitySCAPE Mobile Security Toolkit cyber-security features*	*Via dedicated registration to "beta tester" channel on PlayStore*	*Detecting threat and vulnerabilities on mobile services (as infomobility ones)*
SIGLAMoving back-end API	*Software*	*SIGLA*	*The back-end API of SIGLAMoving solution*	*Via HTTP Restful based API and json*	*Provides services on infomobility to access local transports*
CitySCAPE Mobile Security Toolkit API	*Software*	*SIGLA & KSP*	*The back-end API element of the CitySCAPE Mobile Security Toolkit*	*Via HTTP Restful based API and json*	*Collects cyber-security information from mobile and forwards them to SIEM and RITA*
SIEM	*Software*	*ACS*	*The SIEM of the CitySCAPE toolkit (see D3.3)*	*- Via HTTP Restful based API and json - User Interface dedicated dashboards*	*Supports analysis and monitoring activities of LTP cyber-security management team*

RITA	Software	ED	*Element of CitySCAPE toolkit called RITA (see D3.3)*	*- Via HTTP Restful based API and json - User Interface dedicated dashboards*	*Supports analysis and monitoring activities of LTP cyber-security management team*

Table 9. Elements of Transport Data Integration with SIGLA App

Besides these elements, Android mobile phone accounts are also needed to be registered for installation of SIGLAMoving solution from the Android PlayStore "alpha channel".
They were communicated via email to SIGLA contact persons to be enrolled into the "alpha channel" programme.
The piloting activity lasted for 5 days, repeating the same tests for two people each day.
The attack scenarios were designed considering the guideline of test cases stories described in deliverable D3.3 "CitySCAPE architecture: modules and interfaces" for the Mob-Sec validation execution, whose relationship with the technical test procedures have been already described in WP7 pilot's documentation (D7.1).

	User Story
User story A	Anna [U1] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of hers, staying in the surroundings of the city she lives in. In line with her will to embrace a sustainable lifestyle, Anna wants to use the services provided by the Public Transport System to reach Elena. This implies using a set of multimodal transport services, namely: a bus, a metro, another bus and an urban (small) train. She has already done this trip numerous times and since she already knows what lines and transport services to use, she starts planning her travel. For this reason, she collects information via the transport company's mobile application. The application is linked with the Mob-Sec features. Hence, when she opens the transport company's mobile application, a full antivirus check is performed, and a couple of threats are identified and registered locally in the form of logs transparently to Anna's usage of the mobile application. Those collected data are sent to the Mob-Sec back-end, SIEM and RITA in near real time.
User story B	Anna [U1] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of her, staying in the surroundings of the city she lives in. In line with her will to embrace a sustainable lifestyle, Anna wants to use the services provided by the Public Transport System to reach Elena. However, Anna lives close to 2 bus stops, both at walking distance: one closer, one further. Consequently, she needs to check where the closest bus stop is and when the first bus arrives. For this reason, she checks for

	relevant information via the transport company's mobile application. The application is linked with the Mob-Sec features. Hence, when she accesses the transport company's mobile application to query for bus stops and arrival times, Mob-Sec verifies whether the API URLs used by the transport company mobile application are safe. Any identified security issues, such as threats and vulnerabilities, are registered locally and sent to the Mob-Sec backend, SIEM and RITA in near real time. The transport company mobile application indicates to Anna that bus line 3 is coming in 12 minutes, so she walks to the further bus stop to do a bit of exercise.
User story C	Anna [U1] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of her, staying in the surroundings of the city she lives in. In line with her will to embrace a sustainable lifestyle, Anna wants to use the services provided by the Public Transport System to reach Elena. After checking for the closest bus stop and arrival times, via the transport company mobile application, she selects the bus stop of preference. When she arrives at the bus stop, she checks on the transport company mobile application that the bus is arriving in 1 minute. She makes use of the transport company mobile application to buy her a ticket. Since the application is linked with the Mob-Sec features, Mob-Sec verifies whether the API URLs used for the payment service are secure. Any identified security issues, such as threats and vulnerabilities are registered locally and sent to the Mob-Sec back-end, SIEM and RITA in near real time.
User story D	Anna [U1] a citizen of a European city (e.g., Genova or Tallinn), needs to go visit Elena, a friend of her, staying in the surroundings of the city she lives in. In line with her will to embrace sustainable lifestyle, Anna uses the services provided by the Public Transport System to reach Elena. Using the transport company mobile application, she selects bus line 3 towards the metro station 'A'. While sat on the bus, she uses her mobile phone and from time to time she checks line 3 stops to understand exactly where to disempark. When she reaches the Metro 'A' station bus stop, she checks on the transport company mobile application the arrival time of the next metro: it arrives in 5 minutes. Since the application is linked with the Mob-Sec features, Mob-Sec verifies that the API URLs used for accessing the arrival times are safe. However, to obtain arrival time information the mobile phone connects to a local Wi-Fi. Since the application is linked with the Mob-Sec features, Mob-Sec verifies whether the connection is secure and unfortunately it is not. Mob-Sec registers locally all identified security issues, such as threats and vulnerabilities and sends them to the Mob-Sec back-end, SIEM and RITA in near real time. Later, Anna reaches the train station after having travelled a few minutes on metro and then on bus 22. Her phone connects to a local Wi-Fi, provided by a bar where she sat to have a coffee while waiting for her train. Mob-Sec verifies whether the connection is secure and unfortunately it is not. Mob-Sec registers locally all identified security issues, such as threats

	and vulnerabilities and sends them to the Mob-Sec backend, SIEM and RITA in near real time
User story E	Fabio [U2] a registered CitySCAPE security officer (SOC) working at the Local Transport Company, is using the CitySCAPE toolkit to receive and manage all information produced by Mob-Sec and the rest of CitySCAPE components. Any identified security issues, including threats and vulnerabilities that are sent to the Mob-Sec backend is visualised through the SIEM user interface, allowing Fabio to implement policies to face those vulnerabilities identified. Furthermore, once per day the Mob-Sec backend sends the identified security issues to RITA, allowing Fabio to calculate what is the risk and impact to the transport services as a result of the identified security issues, allowing him to plan and implement appropriate countermeasures

The execution of scenarios was performed with two different smartphones, one per person: one rooted and one not. This is not compulsory, but it was necessary to test “root detection” security feature.
Data produced by Mobile Security Toolkit through SIGLA Moving are regularly sent to SIEM and RITA. In case, connection issue happens between

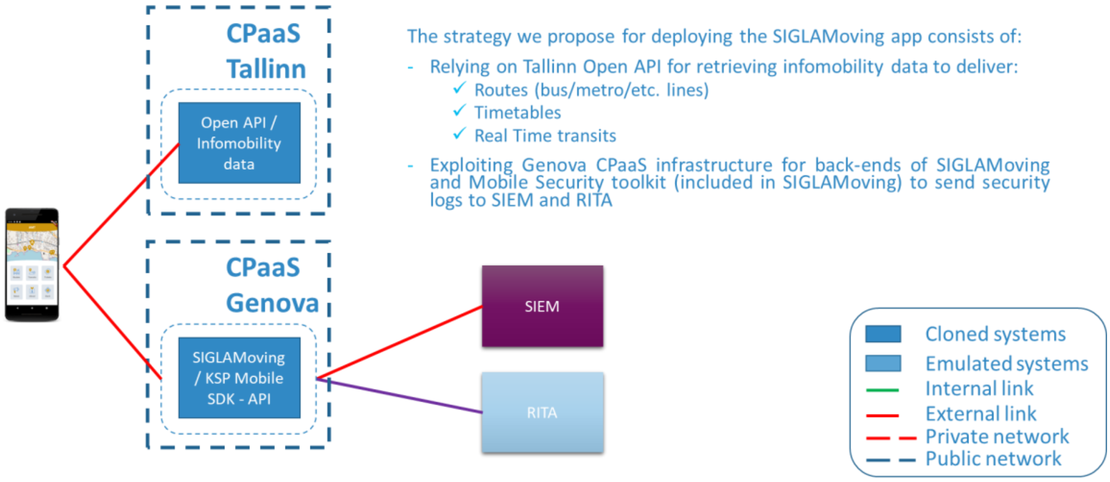


Figure 45. Mob-Sec CitySCAPE deployment architecture

Mobile Security Toolkit and SIEM/RITA, the server elements of Mobile Security Toolkit logs locally the sent data (to avoid permanent data loss).
As described in the previous figure, the deployment of Mob-Sec solution and its integration into Tallin CPaaS involved a mobile application (i.e., SIGLAMoving integrating KMS and Mob-Sec front-end modules), server-side API elements - hosted on Amazon AWS for both pilot sites by AMT and managed by SIGLA (i.e., the Mob-Sec backend), SIEM and RITA.
Within this infrastructure, the vulnerabilities and attacks detected by KSP KMS are logged by Mob-Sec front-end module. This latter sends them (tagged meaningfully according to the detected attack category) to Mob-Sec back-end module that forwards them to SIEM and RITA.

4.3.5.2 Attack scenarios

This section describes the attack scenarios referring to the 4 user stories associated to Mob-Sec validation (see previous chapter user stories).

The considered individual attacks and vulnerabilities and the association to each of these four scenarios are described in detail within deliverable D7.1 "Pilot scenarios, validation plan, and Pre-piloting preparation" at section *3.4.6 Test procedures, 3.4.7 Test Cases description and 3.4.8 CitySCAPE User stories.*

To support the performance of attack tests and validation, a test configuration manual dedicated to pilot partners was prepared by SIGLA. This action was meant to describe in detail how to produce each attack and vulnerability conditions independently.

4.3.5.2.1 Scenario A

[A]: The first scenery is very easy to be replicated. In fact, Anna has to open the SiglaMoving App, the backend will work in background, and will detect smartphone's vulnerabilities. At the end of the detection process, the main page of the app will display (see Figure 46).

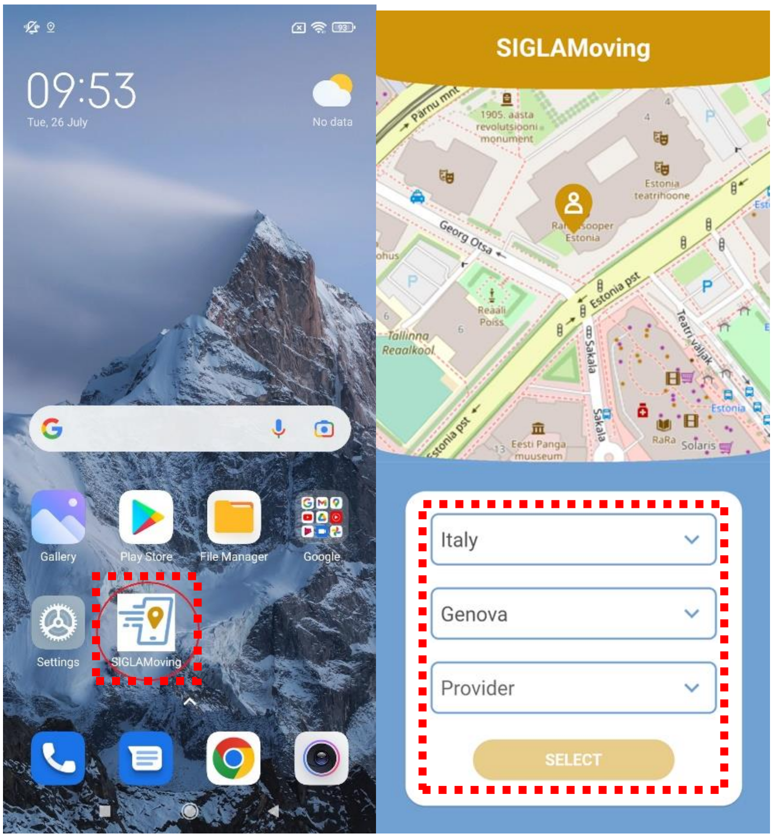


Figure 46. SiglaMoving App

4.3.5.2.2 Scenario B

[B]: To replicate this scenario, first we have to select a provider in the SiglaMoving main page, in that way we unlock the "Select" button. Once we are inside the App, we can click on the routes section.

Figure 47. Selected provider

On the page that will be loaded, all the data on the available routes of the public transport provider (in that case we use the route 3 for example) can be found, then we need to move from the timetable to the maps tab.

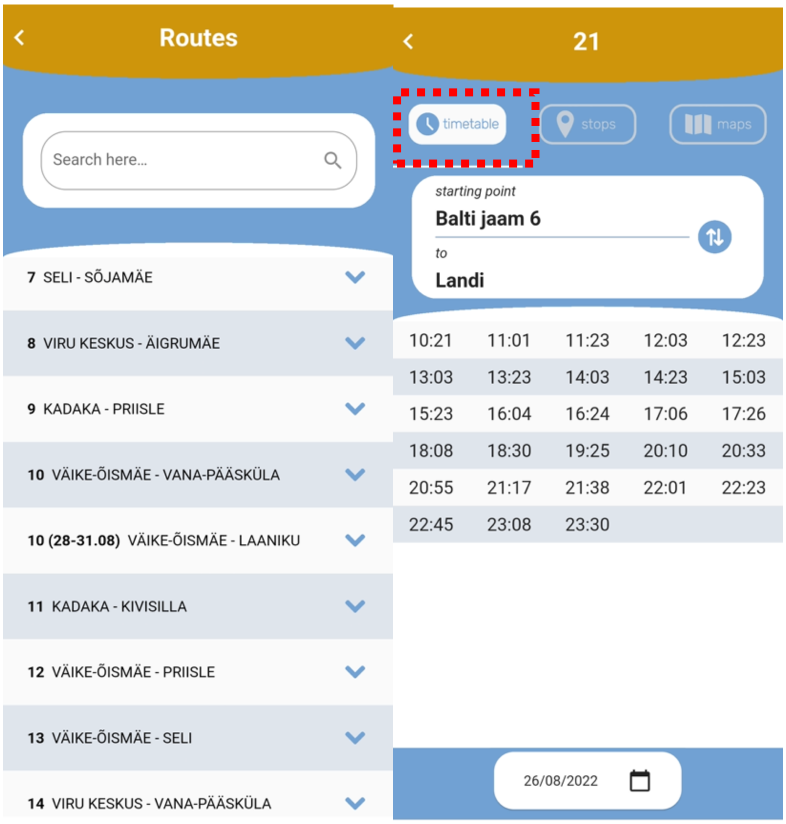


Figure 48. Routes and timetables

From here we can see all the bus stops along the 3 bus route. By enlarging the section of the map, we can see more specifically which bus stop is closer or farther away and decide accordingly which one to reach.

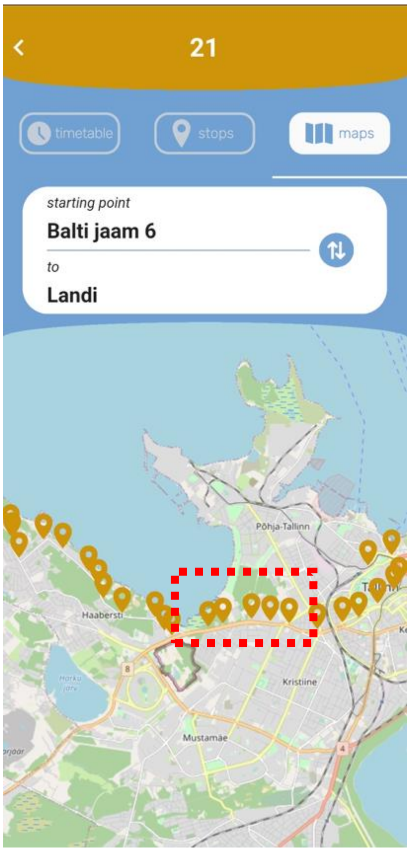


Figure 49. Bus line and stops

4.3.5.2.3 Scenario C

[C] : For this scenario we need, to open SiglaMoving app, and this time, in the main page, we have first to check the arrivals time of the bus, in the "Transits" section .

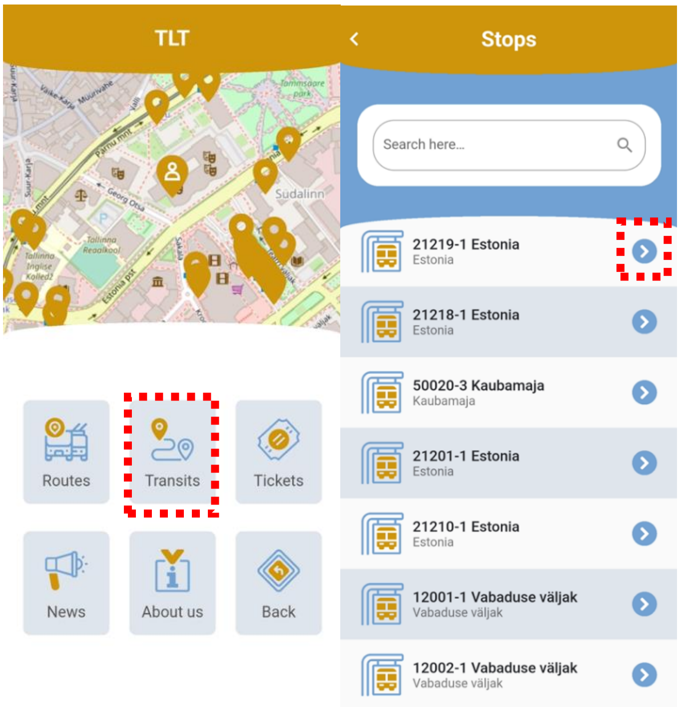


Figure 50. Selected bus lines

Clicking on transits, the bus stops information will display, and opening one of this, we are able to see the Bus Line number, and the time we must wait.

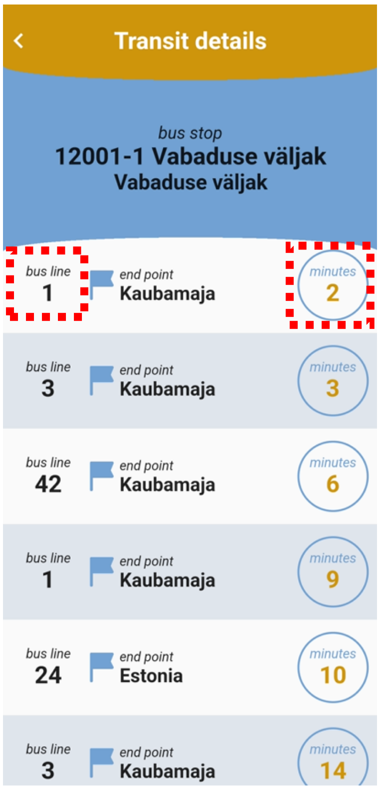


Figure 51. Bus line information and arrival time

4.3.5.2.4 Scenario D

[D]: Anna, in this scenario, could easily check the arrivals time of the bus, with the procedure that we have described in the scenario [C]

4.3.5.3 Outcomes

The results of the pilot campaigns confirmed the correct identification of vulnerabilities by Mob-Sec and the completed integration with SIEM and RITA.
The execution of the pilot testing actions, even though successful under the functional point of view, was of crucial importance in producing reflections on how to configure the second pilot activity related to Mob-Sec and that will be executed during the Genova pilot campaign.

In particular, it underlined the necessity of producing attack conditions to fully test Mob-Sec capabilities given the fact that in a short time frame (e.g., 5 days of piloting) and minimal users sample (e.g., 2 users per day) not all the features may be tested under normal conditions.

Moreover, it stressed the necessity of furtherly tuning the execution of some detection procedures, making coherent waiting time for application's users in order to avoid eventual reduction of usability (due to excessive loading times).
For the Tallinn pilot, every test has been performed successfully as expected, thanks to the limited number of users involved and due to the fact that all the attacks were performed manually.

The integration among all the CitySCAPE elements worked as expected.

4.3.5.4 Future activities

Log collection from Sigla Server to Graylog has already been validated with dummy alerts. To be able to implement a realistic detection scenario, further development is needed to integrate detection rules inside the Graylog SIEM and playbooks inside XSOAR using scenarios that remain to be defined.

CONCLUSIONS

This document has detailed the results of the CitySCAPE TALLINN Pilot that was conducted throughout the months of July and August (Piloting August 24th and 25th). The Pilot conducted a number of cyber test cases. For Test Cases 1, 2 and 3, the cyber-attacks were conducted on the Tallinn Pilot infrastructure and utilised the CPaaS data environment. Test-Case 1 demonstrated that the CitySCAPE toolkit could detect a DDoS attack on the AV Shuttle network and initiate a cyber incident response workflow. Test-Case 2 exhibited that the cyber-attack can be partially detected, and a cyber incident workflow can be initiated. Some information necessary for detection was not collected yet; the SIEM package required more log source to detect effectively attack and not just artefacts of it, as well the integration between the RITA and FIMCA, and the RITA and FIMCA calculation of risk and impacts. These issues and the remaining test cases were workshopped during the Pilot and a plan to remediate the issues and conduct the remaining test cases have been identified and actions to achieve completion of the Tallinn pilot activities will be enacted in September and October.

The pilot successfully demonstrated the Availability of AV Shuttle network test case and partially implemented the test-case on Adaptive Traffic Management. In these demonstrated test case the CitySCAPE toolkit functioned to enable effective detection of the cyber-attack and cyber incident response involving collaboration with the CERT partner (DNSC). For the remaining test cases issues were identified with the integration of CitySCAPE modules, specifically the integration within the SIEM tools (SIEM-CTIP) on the security orchestration and the RITA-FIMCA integration. Furthermore, it was identified that the SIEM needed customisation to the TALLINN pilot environment for creation of detection rules and playbooks for orchestration. During the Pilot, these gaps were identified and there is a plan for remediation and completion of the remaining in September and October.

In conclusion, the demo test cases conducted during the Tallinn Pilot showed that the CitySCAPE toolkit can produce the expected results for detection of cyber-attacks and enhanced incident response in the multi-modal transportation environment. Whilst the Tallinn Pilot was unable to complete all the test cases on the 24th and the 25th of August, many valuable lessons were learnt for the coming Genoa Pilot. These included that the cybersecurity attack test cases need to contain granularity of detail which enable the SIEM operator to customise it to the pilot environment. Furthermore, the integration of the CitySCAPE toolkit needs to be fully validated before piloting, this includes, specifically, the integration between IDS and SIEM, SIEM toolkit and the RITA and FIMCA.

The completed pilot evaluation for Tallinn and Genoa will be contained in D7.5 “Pilot Evaluation and Knowledge capitalisation”.

ANNEX I - IDS/IPS ENGINE USER GUIDE

CitySCAPE – USER GUIDE

T5.4 – IDS/IPS ENGINE

Francesca Costantino, Rosella O. Mancilla
Engineering Ingegneria Informatica SpA

August 24, 2022

INDEX

- Task Objectives – Contributors
- State of the art
- Our approach
- USER GUIDE for Cyber-security services operator or CitySCAPE admin (5’)
  - Anomaly Detection Procedure (ADP) API user guide (5’)
- USER GUIDE for Cyber-security services operator or CitySCAPE admin and CPaaS admin (3’)

26/8/2022 2

WP5 – Task 5.4- IDS/IPS ENGINE

- Objective:
  - ✓ This task focuses on the development of the IDS/IPS engine.
  - ✓ The IDS/IPS module is able to monitor constantly the IT and OT infrastructure and the information gathered will be sent to the higher-level components.
  - ✓ This module is be based on an existing tool (e.g. SNORT) but it is customized according to the needs of the project.
- Leadership: ENG leads; contributors: ED, UPRC, ACS, STAM
- Deliverable: D5.4 IDS/IPS final prototype [ENG, Other, **M30**]

WP5 – Task 5.4- IDS/IPS ENGINE

- Objective:
  - ✓ This task focuses on the development of the IDS/IPS engine.
  - ✓ The IDS/IPS module is able to monitor constantly the IT and OT infrastructure and the information gathered will be sent to the higher-level components.
  - ✓ This module is be based on an existing tool (e.g. SNORT) but it is customized according to the needs of the project.
- Leadership: ENG leads; contributors: ED, UPRC, ACS, STAM
- Deliverable: D5.4 IDS/IPS final prototype [ENG, Other, **M30**]

State of the art IDS/IPS

- **IDS/IPS:** software and/or hardware devices that detect intrusions into a system or a network.
  - **IDS (Intrusion Detection System)** is a passive protection system.
  - **IPS (Intrusion Prevention System)** is an active protection system.

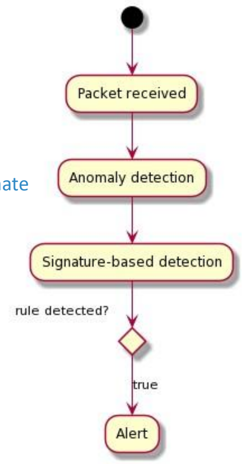
- The **IDSs/IPSs** are installed in critical points of the network (e.g. next to router, gateway, server web ..)

- **Type of detection techniques in real time are**:
  - **Anomaly - based IDS/IPS**
  - **Signature - based IDS/IPS**

26/8/2022 4

OUR APPROACH

- Identify anomalous traffic from legitimate
- Identify malicious traffic



26/8/2022 5

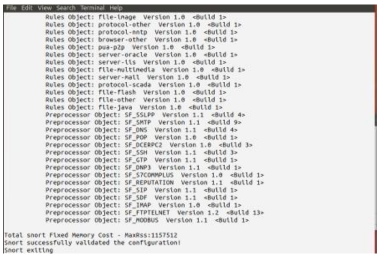
CitySCAPE

USER GUIDE for Cyber-security services operator or CitySCAPE admin

CitySCAPE

- **Run the IDS/IPS engine to TEST the configuration**:
  - *sudo snort -T -i <interface name> -c /etc/snort/snort.conf*

✓ Where:
- -T flag indicates to run a test for the SNORT configuration
- -c flag indicates which file to use
- -i flag specifies the name of the network interface.



26/8/2022 6

USER GUIDE for Cyber-security services operator or CitySCAPE admin

CitySCAPE

- **Run the IDS/IPS offline, with PCAP file** :
  - *sudo snort -c /etc/snort/snort.conf -l /var/log/snort -r <path pcap file> -u snort – g snort*
- **Run the IDS/IPS online:**
  - *sudo snort -c /etc/snort/snort.conf -l /var/log/snort -u snort –g snort –i <interface>*

✓ Where:
- -c flag indicates which config file to use
- -l flag indicates log directory
- -r flag indicates the pcap to be analysed and processed
- -u flag specifies to run as a specific user
- -g flag specifies to run as a specific group

- **View IDS/IPS logs files:**
  - *sudo snort -c /etc/snort/snort.conf –r /var/log/snort/snort.log.1659706028*

26/8/2022 7

CitySCAPE

USER GUIDE for Cyber-security services operator or CitySCAPE admin

- IDS/IPS output

```
        Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
        Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
Commencing packet processing (pid=3985)
===============================================================================
Run time for packet processing was 1.213 seconds
Snort processed 201 packets.
Snort ran for 0 days 0 hours 0 minutes 1 seconds
   Pkts/sec:          201
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       1033269248
  Bytes in mapped regions (hblkhd):      24555520
  Total allocated space (uordblks):      549637344
  Total free space (fordblks):           483631904
  Topmost releasable block (keepcost):   62256
===============================================================================
Packet I/O Totals:
   Received:          201
   Analyzed:          201 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          214 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          214 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:           50 ( 23.364%)
        UDP:            0 (  0.000%)
        TCP:          164 ( 76.636%)
```

```
===============================================================================
Action Stats:
     Alerts:          164 ( 76.636%)
     Logged:          164 ( 76.636%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            2
      Alert:            0
Verdicts:
      Allow:          195 ( 97.015%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  AllowFlow:            6 (  2.985%)
  BlockFlow:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)
===============================================================================
Frag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
               Discards: 0
          Memory Faults: 0
               Timeouts: 0
               Overlaps: 0
              Anomalies: 0
                 Alerts: 0
                  Drops: 0
     FragTrackers Added: 0
    FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
    Frag Nodes Inserted: 0
     Frag Nodes Deleted: 0
===============================================================================
===============================================================================
Stream statistics:
```

26/8/2022 8

USER GUIDE for Cyber-security services operator or CitySCAPE admin

CitySCAPE

Barnyard2 is the submodule that stores and processes the SNORT binary output into a MySQL database.

- **Continuous processing mode** – real-time events' storing (online)
  - sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo -g snort -u snort

Where:

- -c flag specifies the config file
- -d flag is the snort output directory
- -f flag specifies the file to look for
- -w flag specifies the bookmark file
- -u flag tells Barnyard to run as a specific user
- -g flag tells Barnyard to run as a specific group

```
Running in Continuous mode

        --== Initializing Barnyard2 ==--
Initializing Input Plugins!
Initializing Output Plugins!
Parsing config file "/etc/snort/barnyard2.conf"


+[ Signature Suppress list ]+
----------------------------
+[No entry in Signature Suppress List]+
----------------------------
+[ Signature Suppress list ]+
        --== Initialization Complete ==--

  ______   -*> Barnyard2 <*-
 / ,,_  \  Version 2.1.14 (Build 337)
 |o"  )~|  By Ian Firns (SecurixLive): http://www.securixlive.com/
 + '''' +  (C) Copyright 2008-2013 Ian Firns <firnsy@securixlive.com>

Using waldo file '/var/log/snort/barnyard2.waldo':
    spool directory = /var/log/snort
    spool filebase  = snort.u2
    time_stamp      = 1653376944
    record_idx      = 1384
Opened spool file '/var/log/snort/snort.u2.1653376944'
Waiting for new data
```

26/8/2022 9

USER GUIDE for Cyber-security services operator or CitySCAPE admin

- **File processing mode:** processing a single log file (offline).
  - sudo barnyard2 -c /etc/snort/barnyard2.conf -o /var/log/snort/snort.u2.1653376944

    ✓ Where:
    - -c flag specifies the configuration file
    - -o flag enables the file processing mode
    - The file snort.u2.***** is the specific file that you want process.

```
alert.csv              snort.log.1652344315  snort.u2.1652085271  snort.u2.1652358307
barnyard2.waldo        snort.log.1652344609  snort.u2.1652085294  snort.u2.1652358435
snort.log.1652084790   snort.log.1652358307  snort.u2.1652091045  snort.u2.1652957259
snort.log.1652085294   snort.log.1652358435  snort.u2.1652164843  snort.u2.1653301703
snort.log.1652091045   snort.log.1652957259  snort.u2.1652343423  snort.u2.1653376944
snort.log.1652164843   snort.log.1653301703  snort.u2.1652343610
snort.log.1652343423   snort.log.1653304192  snort.u2.1652344315
snort.log.1652343610   snort.log.1653376944  snort.u2.1652344609
```

26/8/2022 10

USER GUIDE for Cyber-security services operator or CitySCAPE admin

To check if new events are stored in the MySQL database launch the following command:

- *mysql -u snort -p snort -e "select count(*) from event"*

✓ Where:
- -u flag specifies the MySQL user
- -p flag specifies that a password is required
- -e flag indicate what to show.

```
Enter password:
+----------+
| count(*) |
+----------+
|     2730 |
+----------+
```

26/8/2022 11

CitySCAPE Anomaly Detection Procedure API

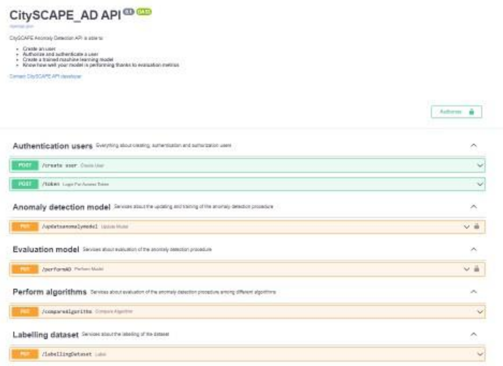
The API include the APD and several endpoints to test the procedure.

To start the API, lauch:

- *python –m uvicorn main:app --reload*

An interactive documentation, is also available at:

- *http://IP_ADDRESS:8000/docs*



26/8/2022 12

CitySCAPE ADP API - authentication

AUTHENTICATION:

This service is about creating, authentication and authorization users.

Here we can find two endpoints:

- ✓ **Create user:** it is possible to create a user
- ✓ **Token:** after login, you will be obtained a token for authentication.

26/8/2022 13

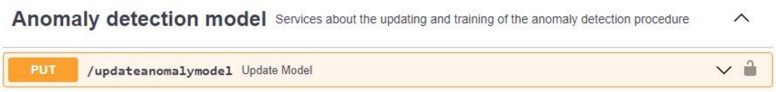
CitySCAPE ADP API – update model

UPDATE MODEL:

The ADP model can be updated by importing a new training dataset (.csv). Also, the following metrics are returned

- accuracy (total number of correctly predicted records over the total number of records)
- confusion matrix (TP, FN, FP, TN)

It returns accuracy value and the number of True Positive, True Negative, False Negative and False Positive



26/8/2022 14

CitySCAPE API – SERVICES

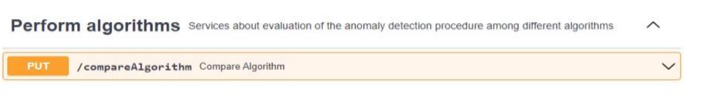
COMPARE ALGORITHMS:

This service compare the results of the anomaly detection procedure using different algorithms:

Resulting metrics are:

- accuracy (total number of correctly predicted records over the total number of records)
- confusion matrix (TP, FN, FP, TN)
- required extension is .csv

This service returns the algorithm's name, the accuracy value, the number of True Positive, True Negative, False Negative and False Positive and the time taken for the procedure.



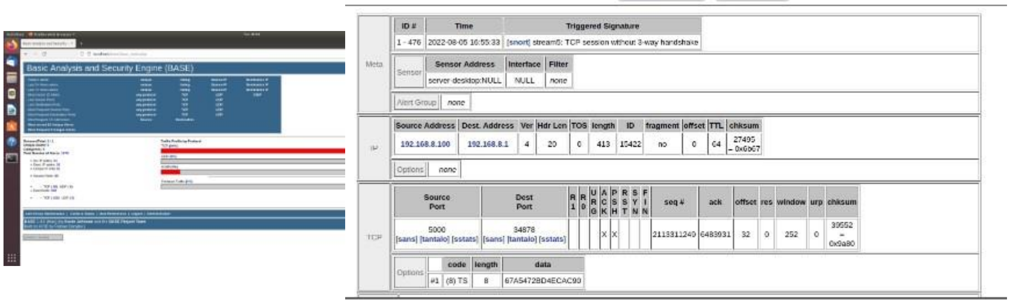
26/8/2022 15

USER GUIDE for Cybersecurity services operator or CitySCAPE admin and CPaaS admin

The GUI to view alerts stored in the database is also available to CPaaS admin.

Following the link ***http://IP/base/index.php***

The authentication page appears. After authentication you can access the main page.



26/8/2022 16

Any questions?

Thank you!

ENGINEERING

Francesca Costantino, Rosella Omana Mancilla

Engineering Ingegneria Informatica S.p.A

Francesca.costantino@eng.it, rosellaomana.mancilla@eng.it

This project has received funding from the EU's Research and Innovation programme Horizon 2020 under grant agreement No 883321 Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

ANNEX II - RITA TEST-CASE 1 DEMO FUNCTIONALITY

- Test-Case 1 Asset Cost Evaluation

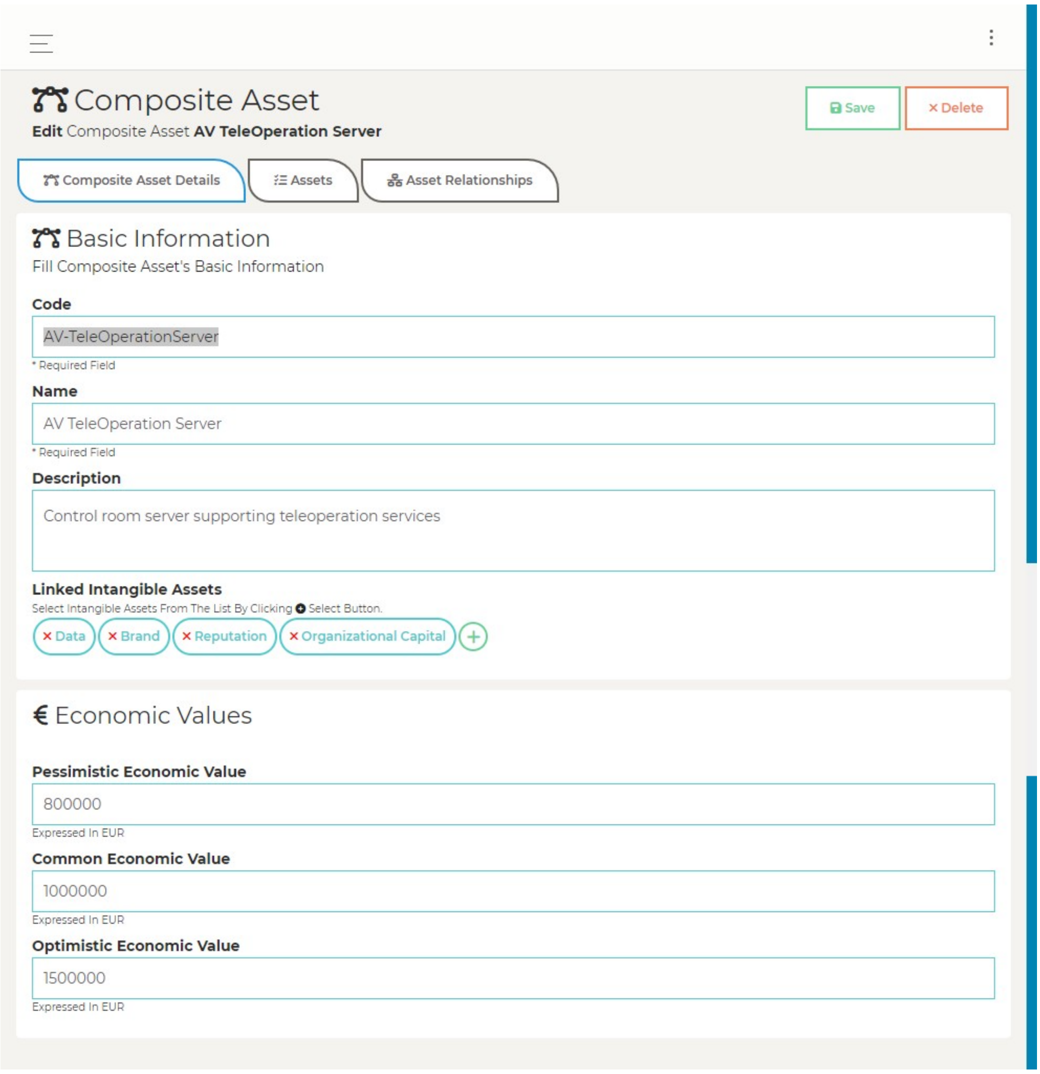


Figure 1. AV TeleOperation Server (Basic Information)

- RITA Threat Mapping Test-Case 1

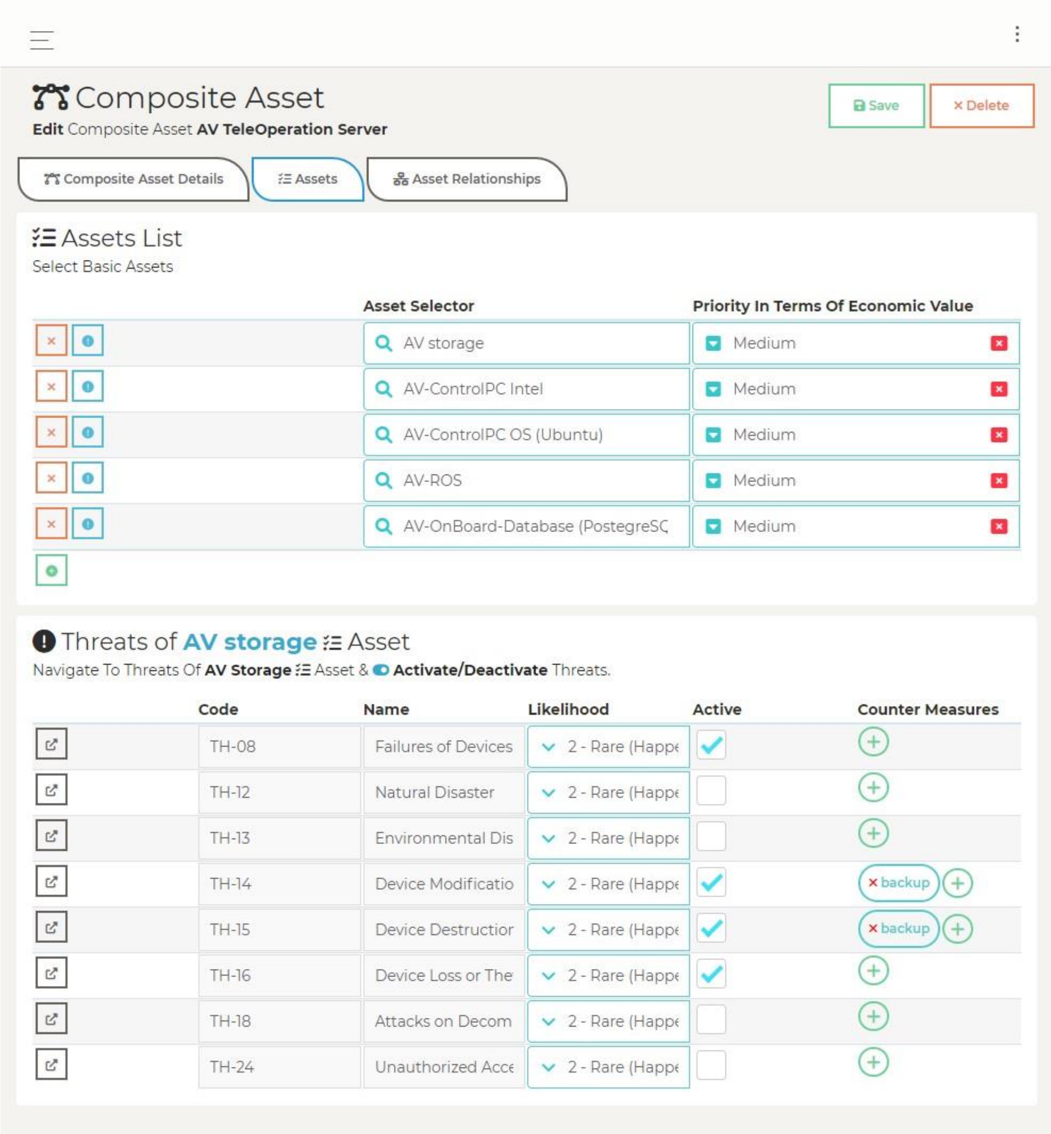


Figure 2. AV TeleOperation Server (AV Storage Threats and Likehoods)

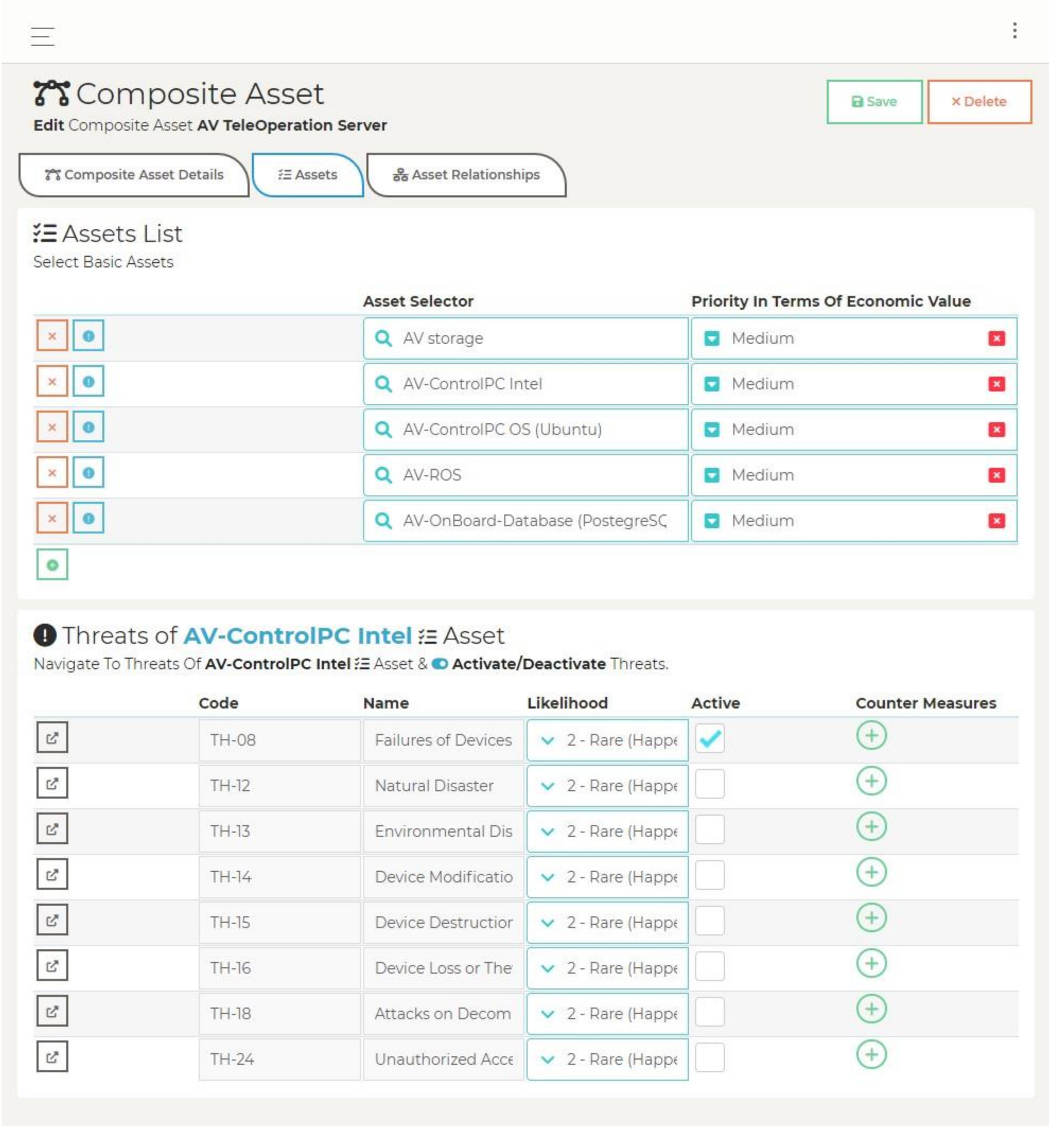


Figure 3. AV TeleOperation Server (AV Control PC Intel Threats and Likehoods)

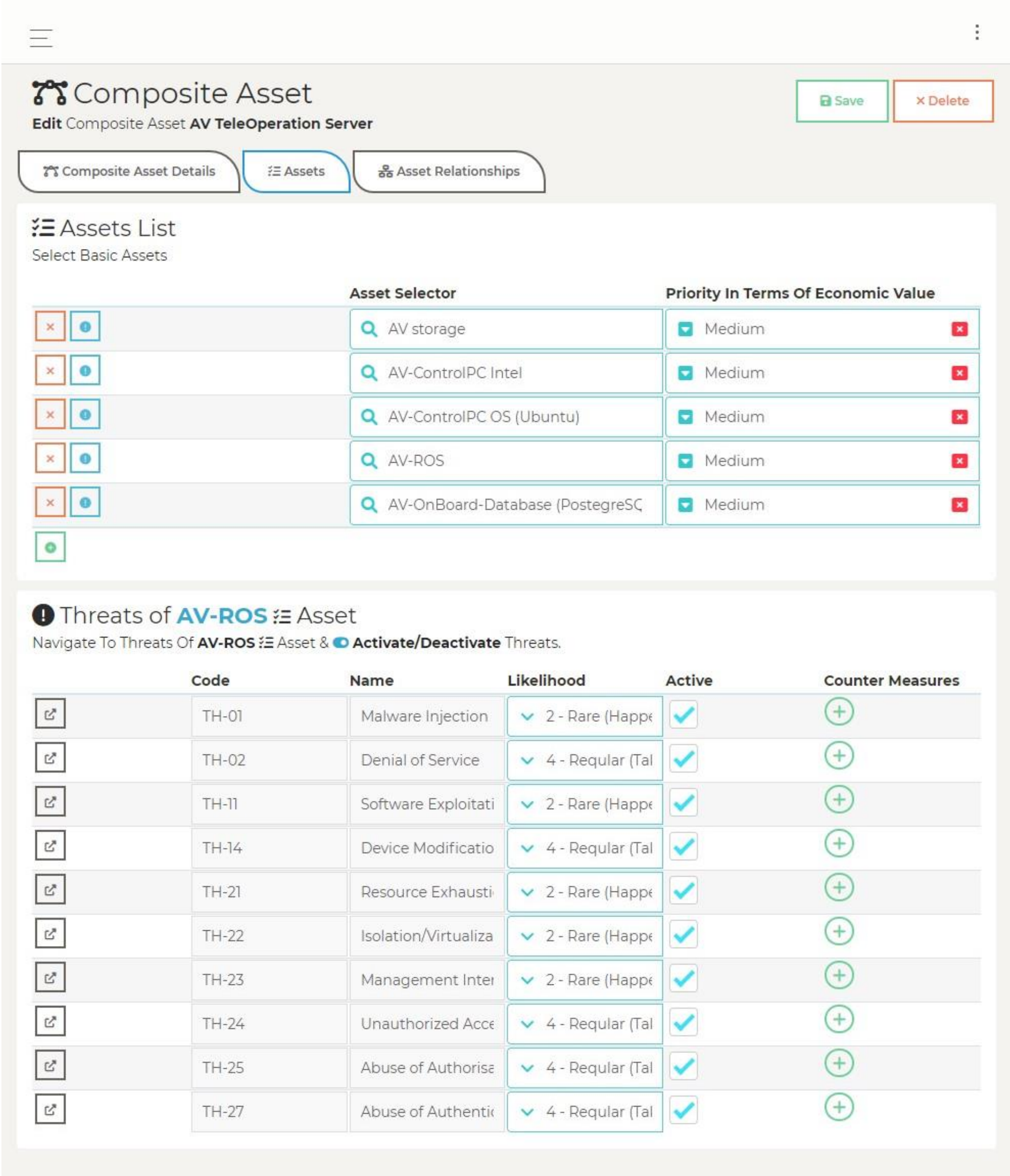


Figure 4. AV TeleOperation Server (AV ROS Threats and Likehoods)

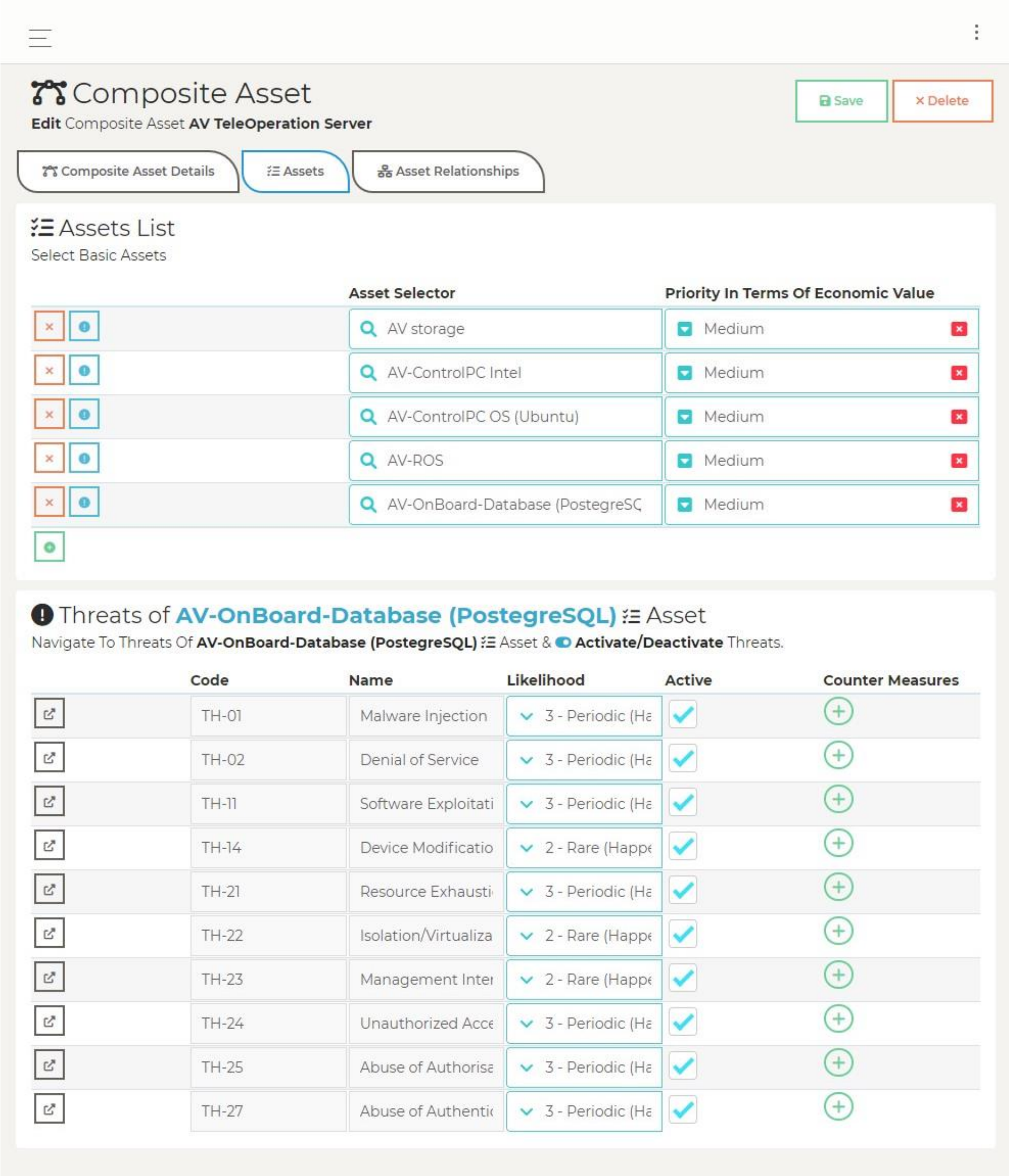


Figure 5. AV TeleOperation Server (AV On Board PostgreSQL Database Threats and Likehoods)

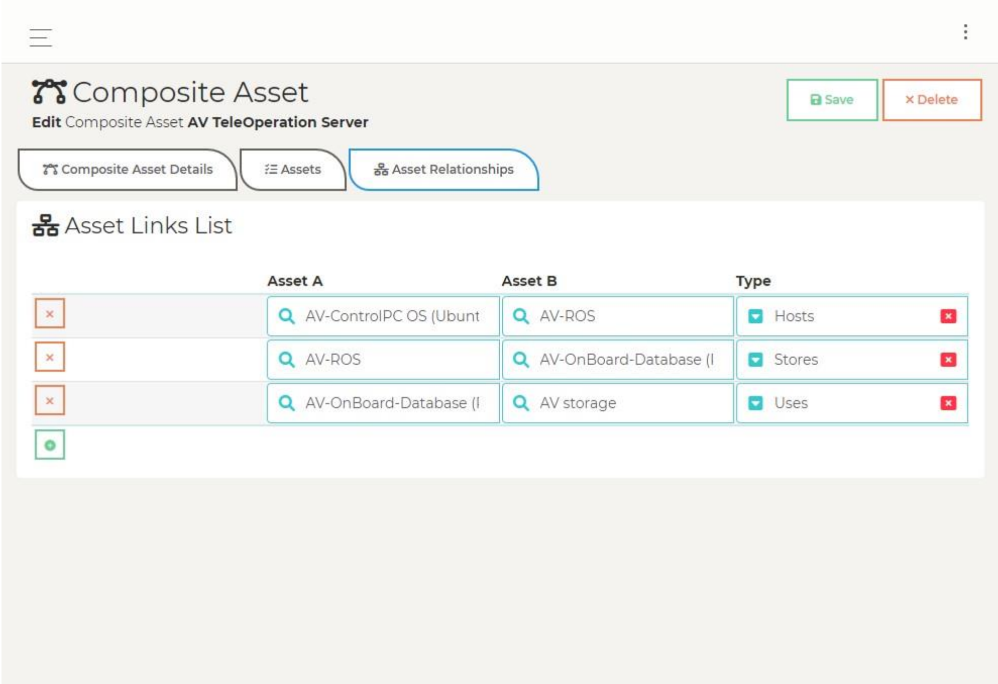


Figure 6. AV TeleOperation Server (Asset Relationships)

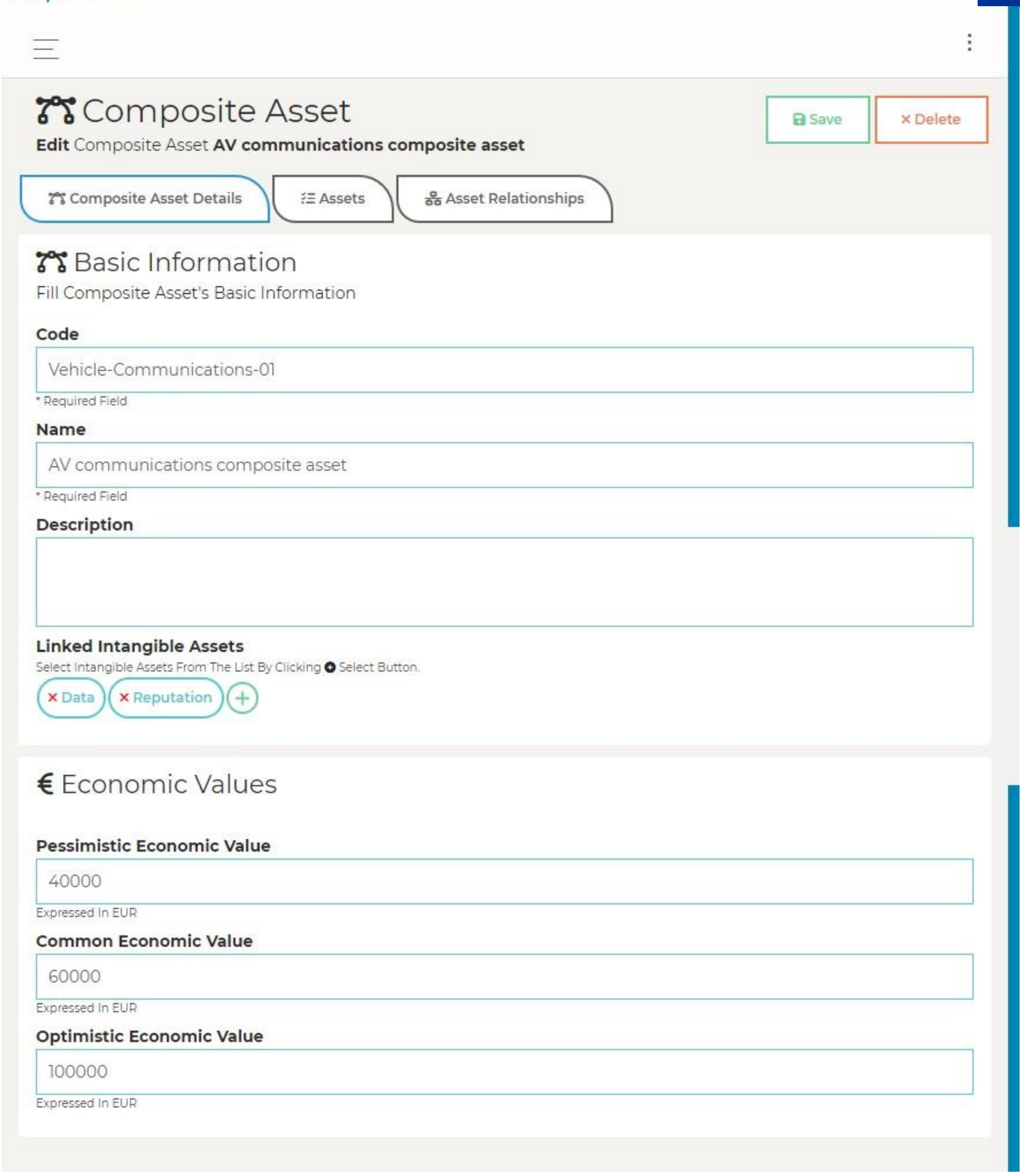


Figure 7. AV communications (Basic Information)

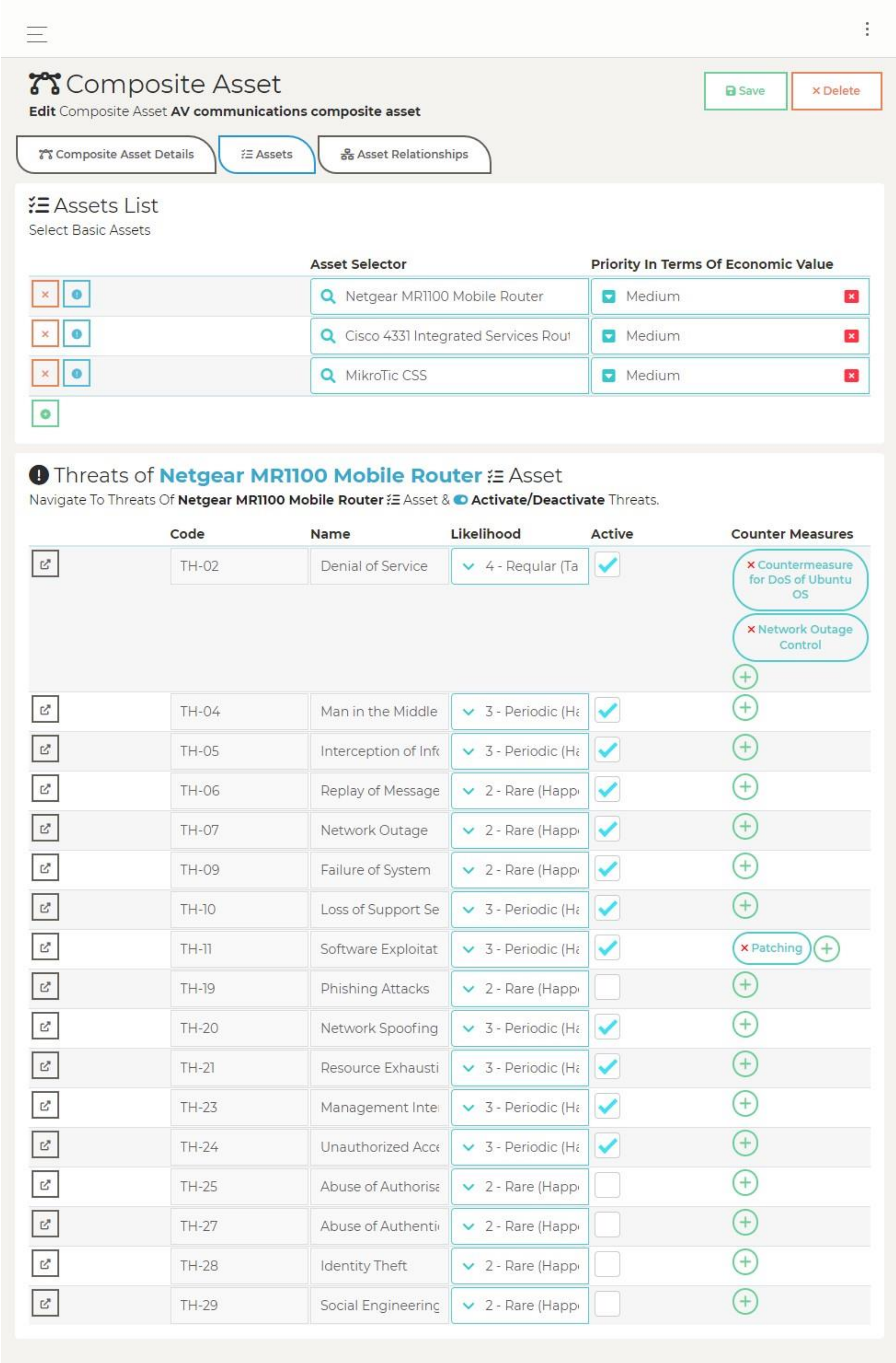


Figure 8. AV communications (Netgear MR1100 Mobile Router Threats and Likelihoods)

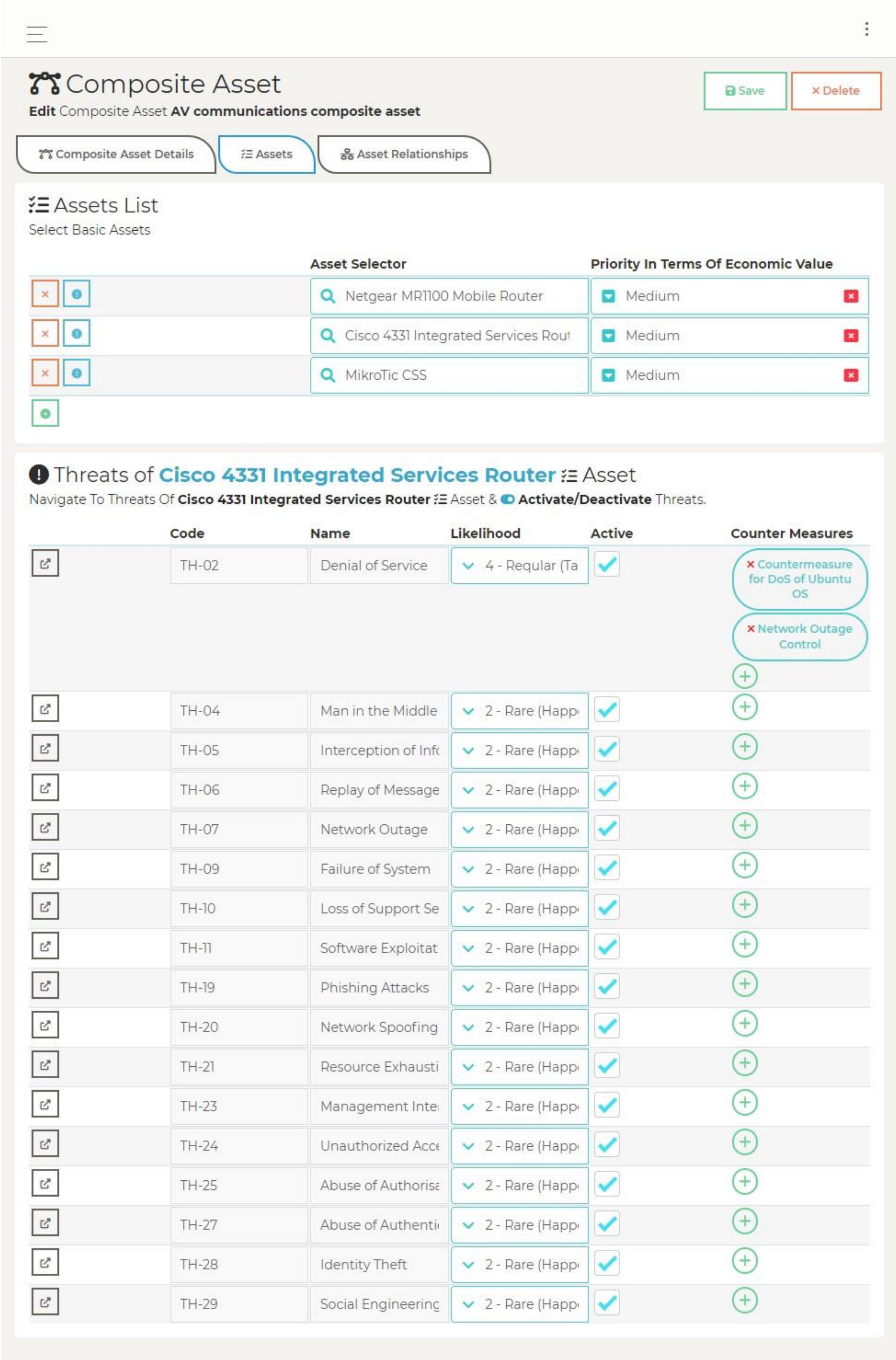


Figure 9. AV communications (Cisco 4331 Integrated Services Router Threats and Likelihoods)

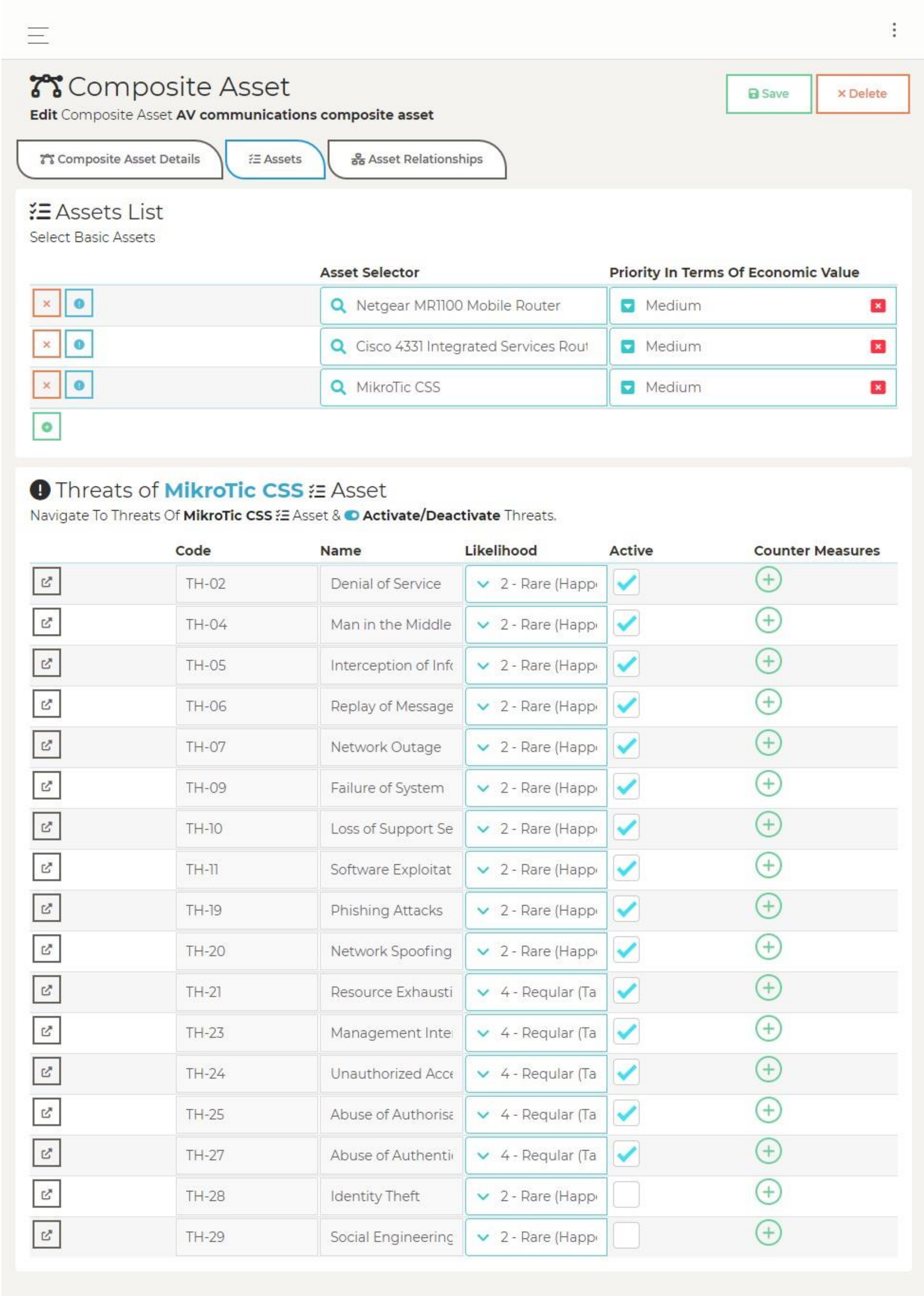


Figure 10. AV communications (MikroTic CSS Threats and Likelihoods)

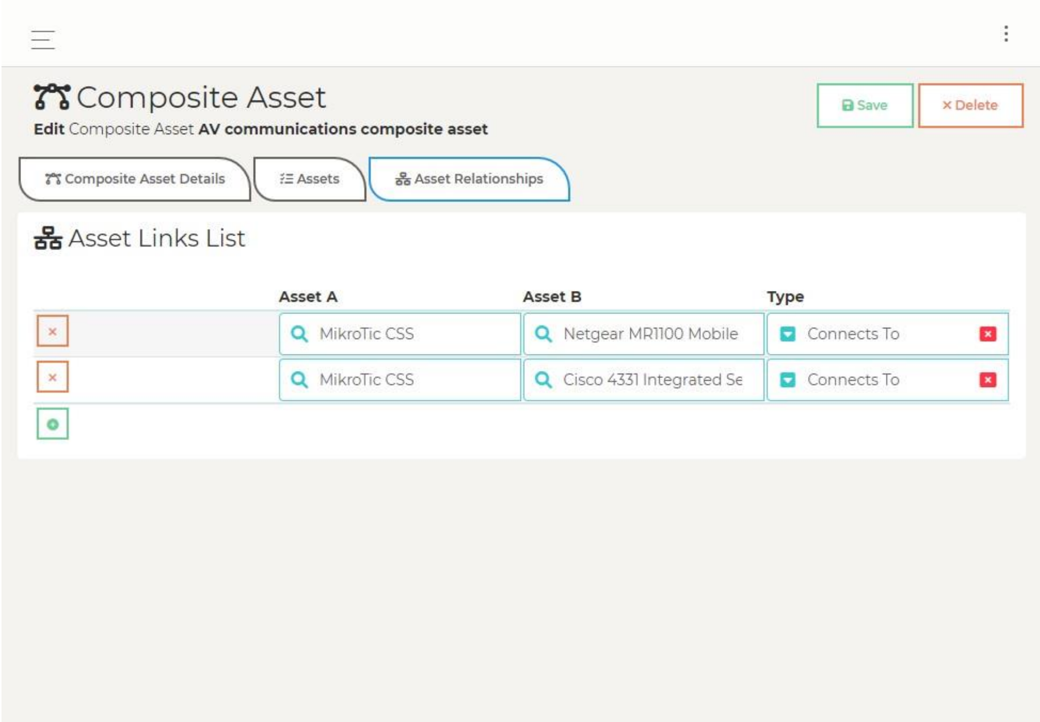


Figure 11. AV communications (Asset Relationships)

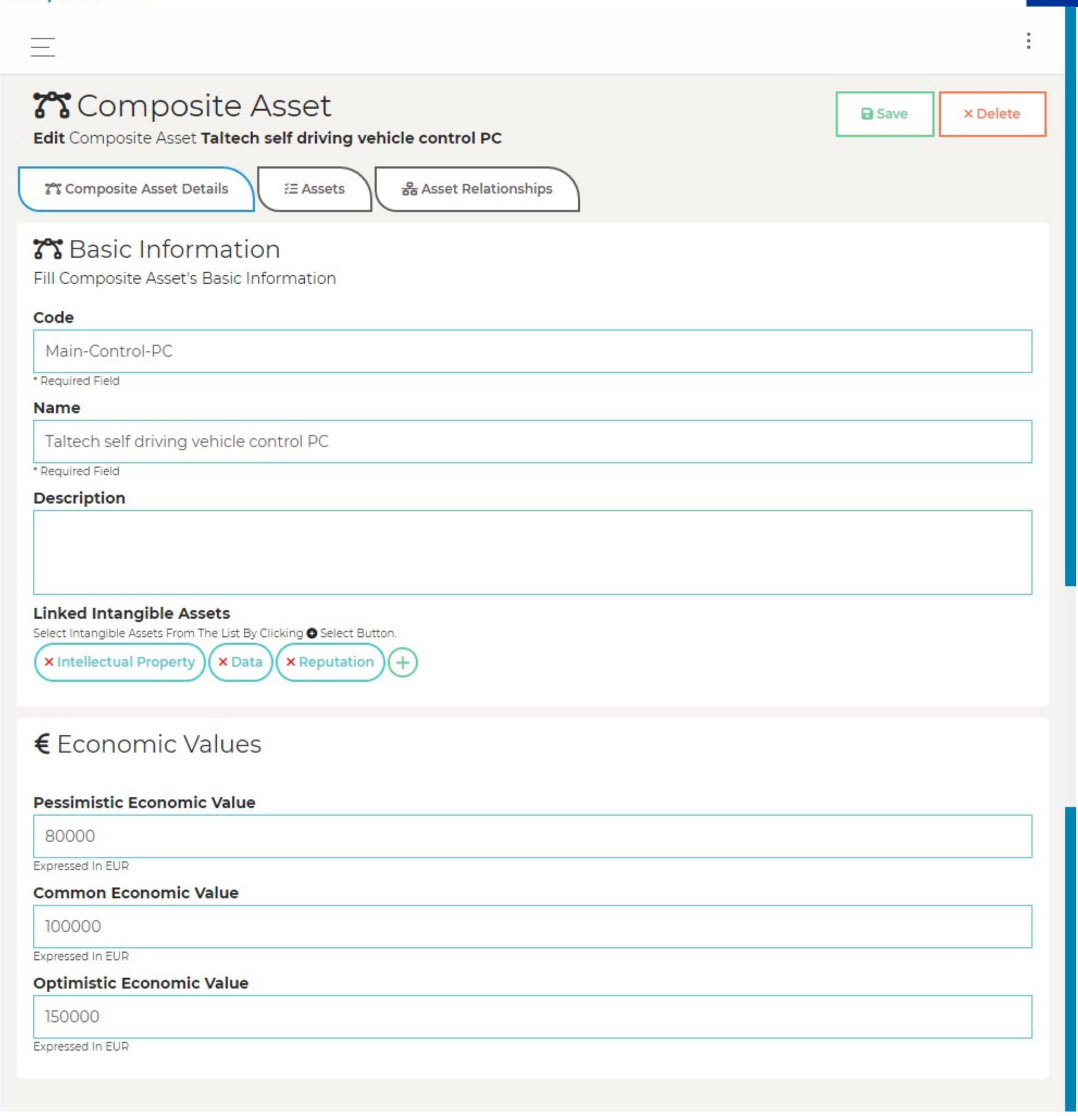


Figure 12. Main-Control-PC (Basic Information)

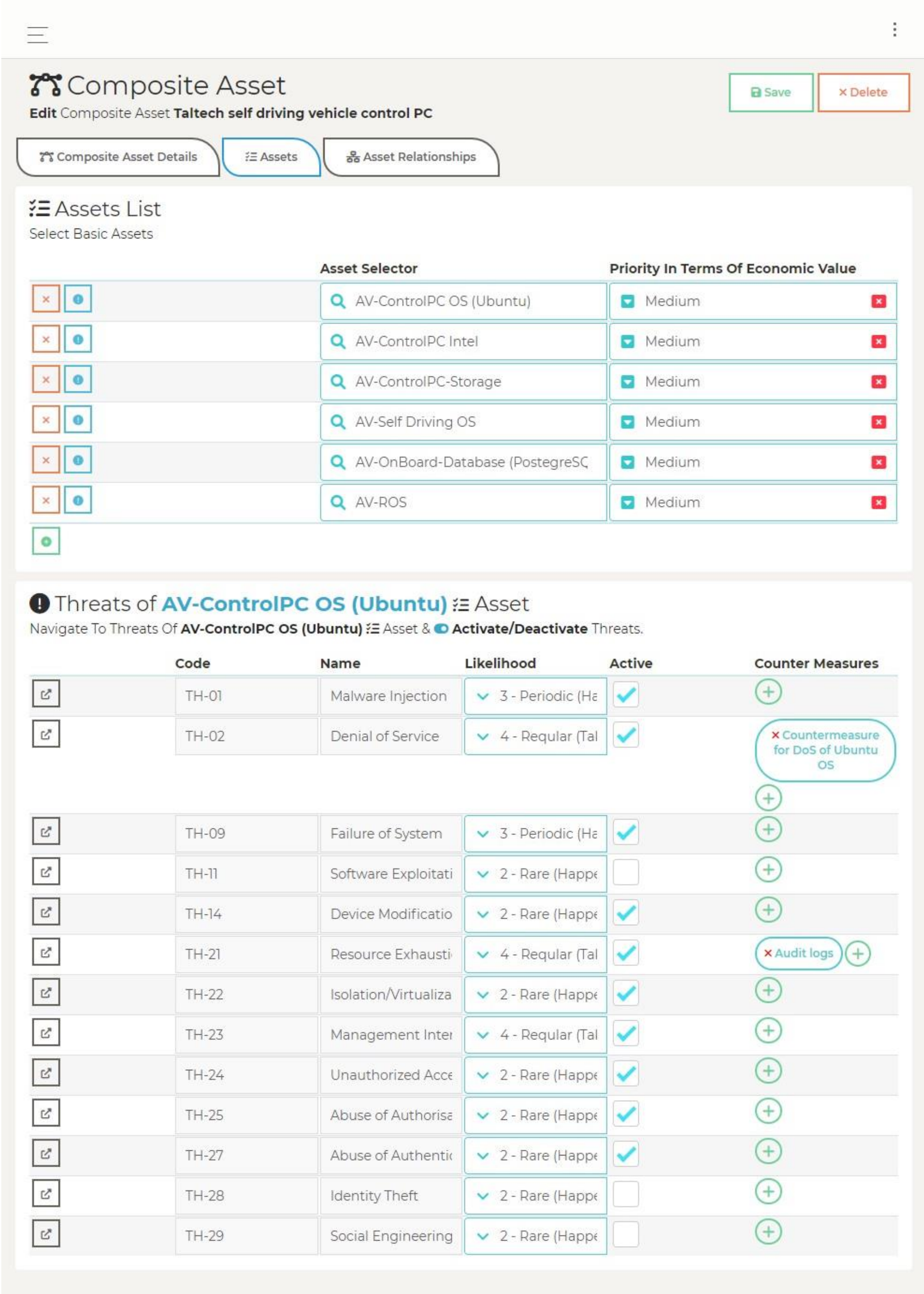


Figure 13. Main-Control-PC (AV Control PC OS Ubuntu Threats and Likehoods)

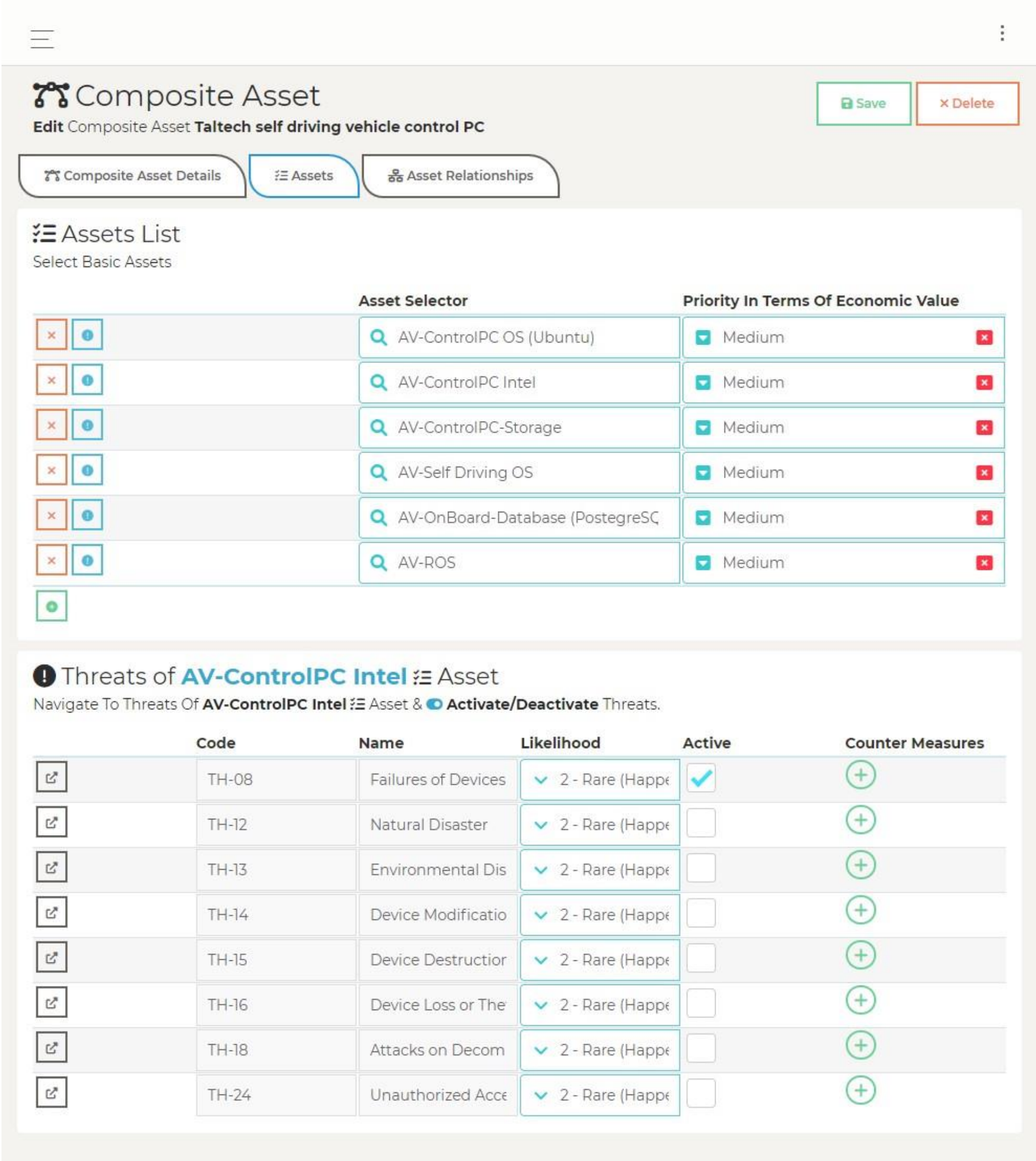


Figure 14. Main-Control-PC (AV Control PC Intel Threats and Likehoods)

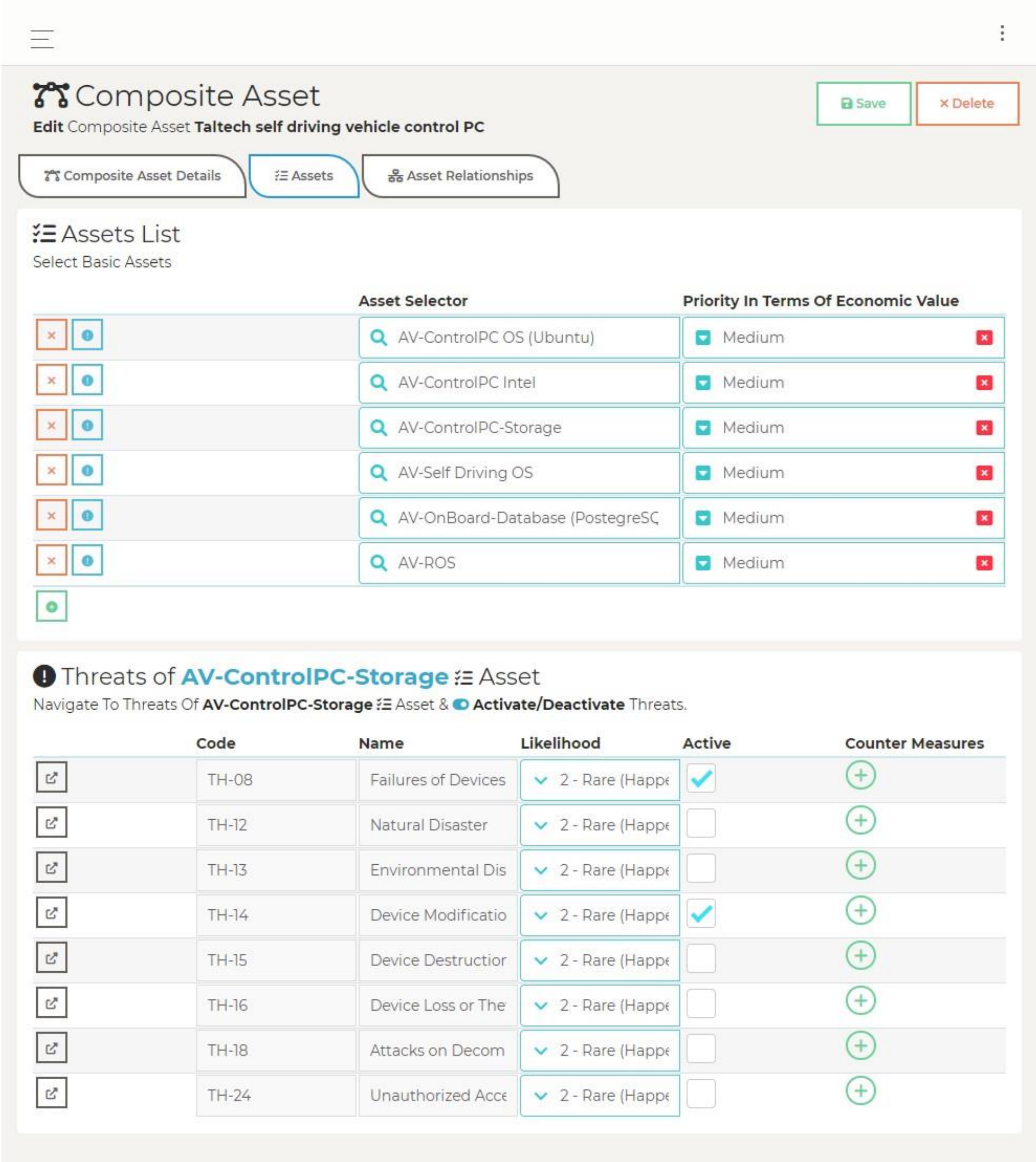


Figure 15. Main-Control-PC (AV Control PC Storage Threats and Likehoods)

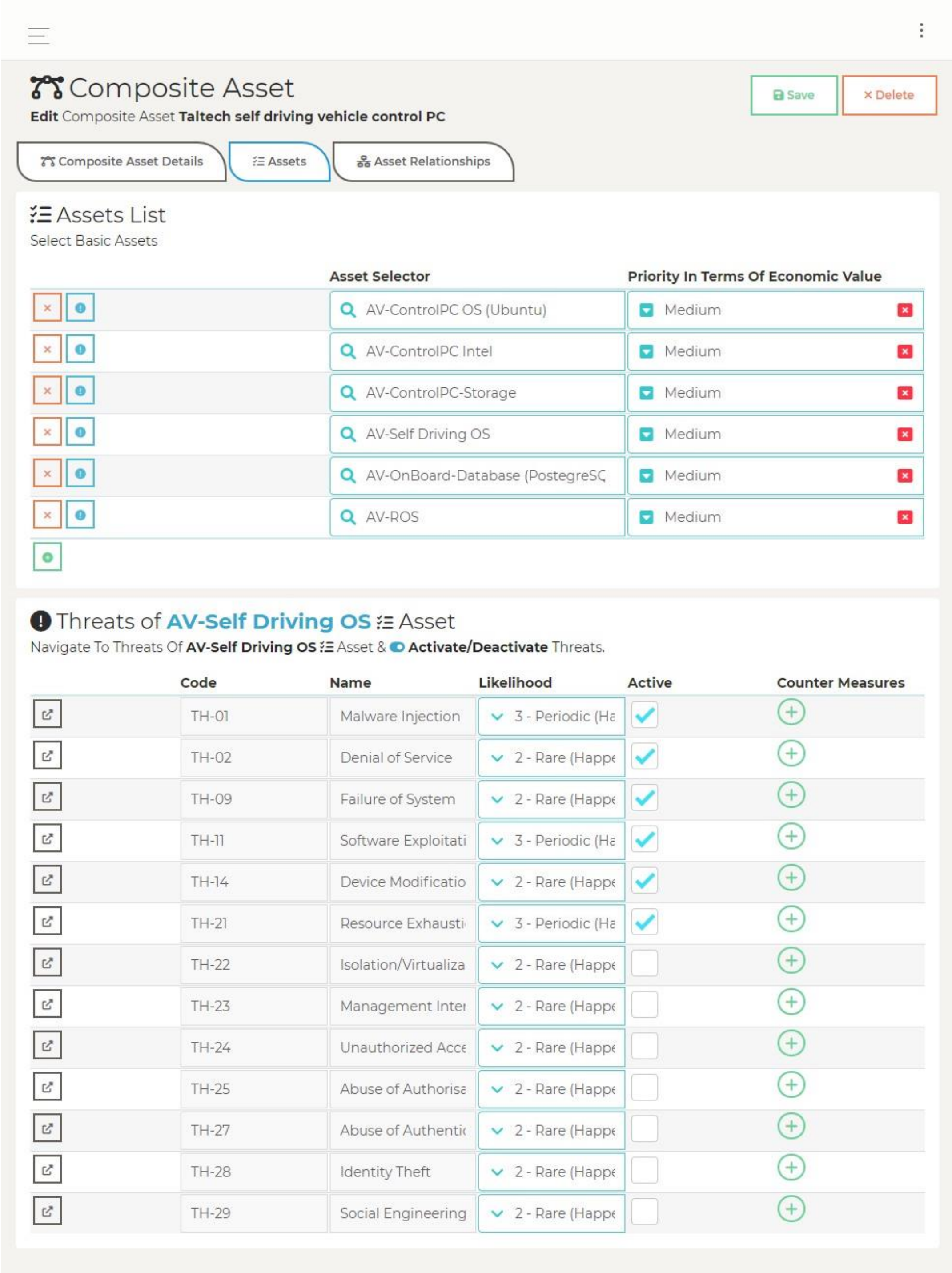


Figure 16. Main-Control-PC (AV Self-Driving OS Threats and Likehoods)

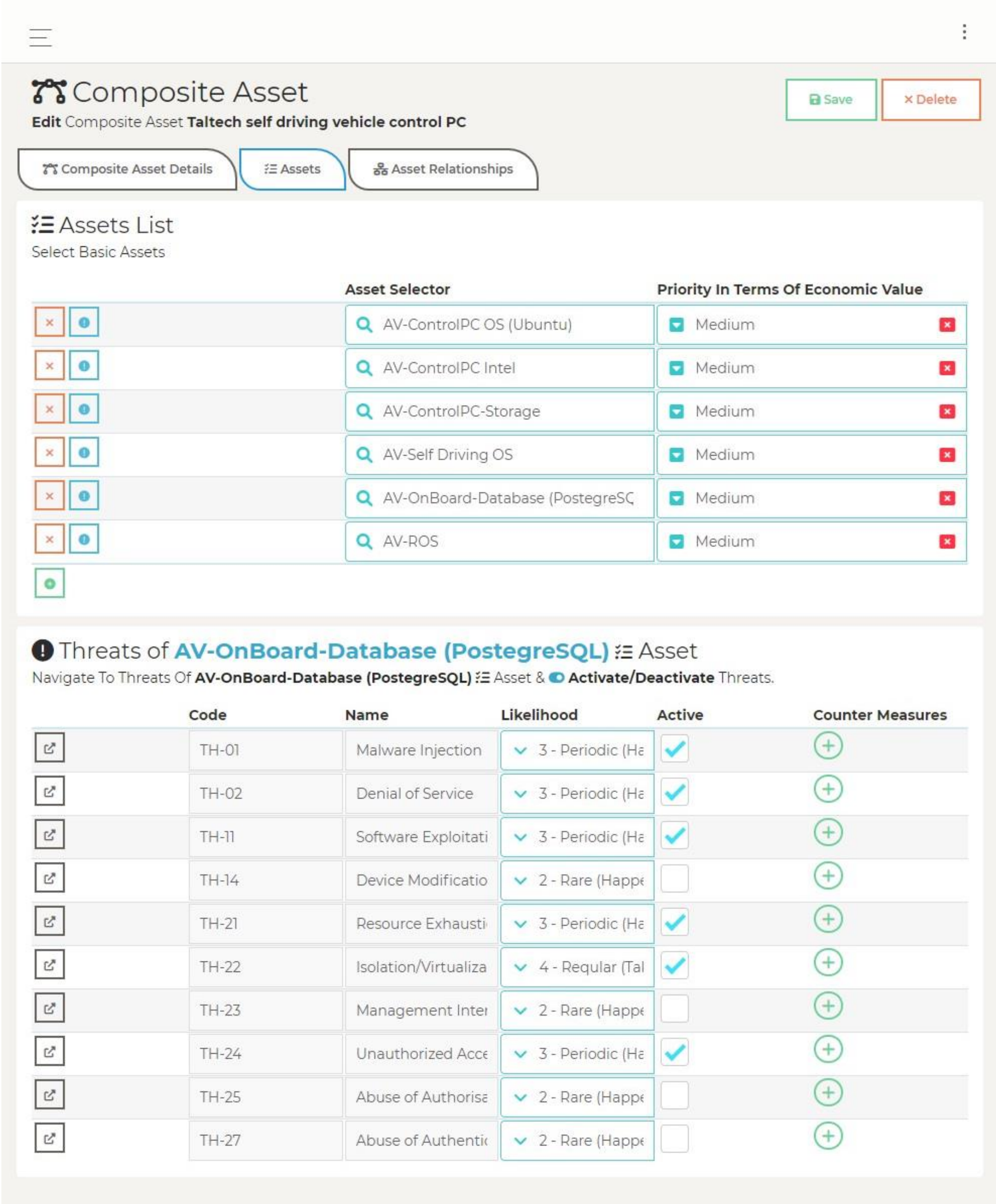


Figure 17. Main-Control-PC (AV On-board PostgreSQL Database Threats and Likelihoods)

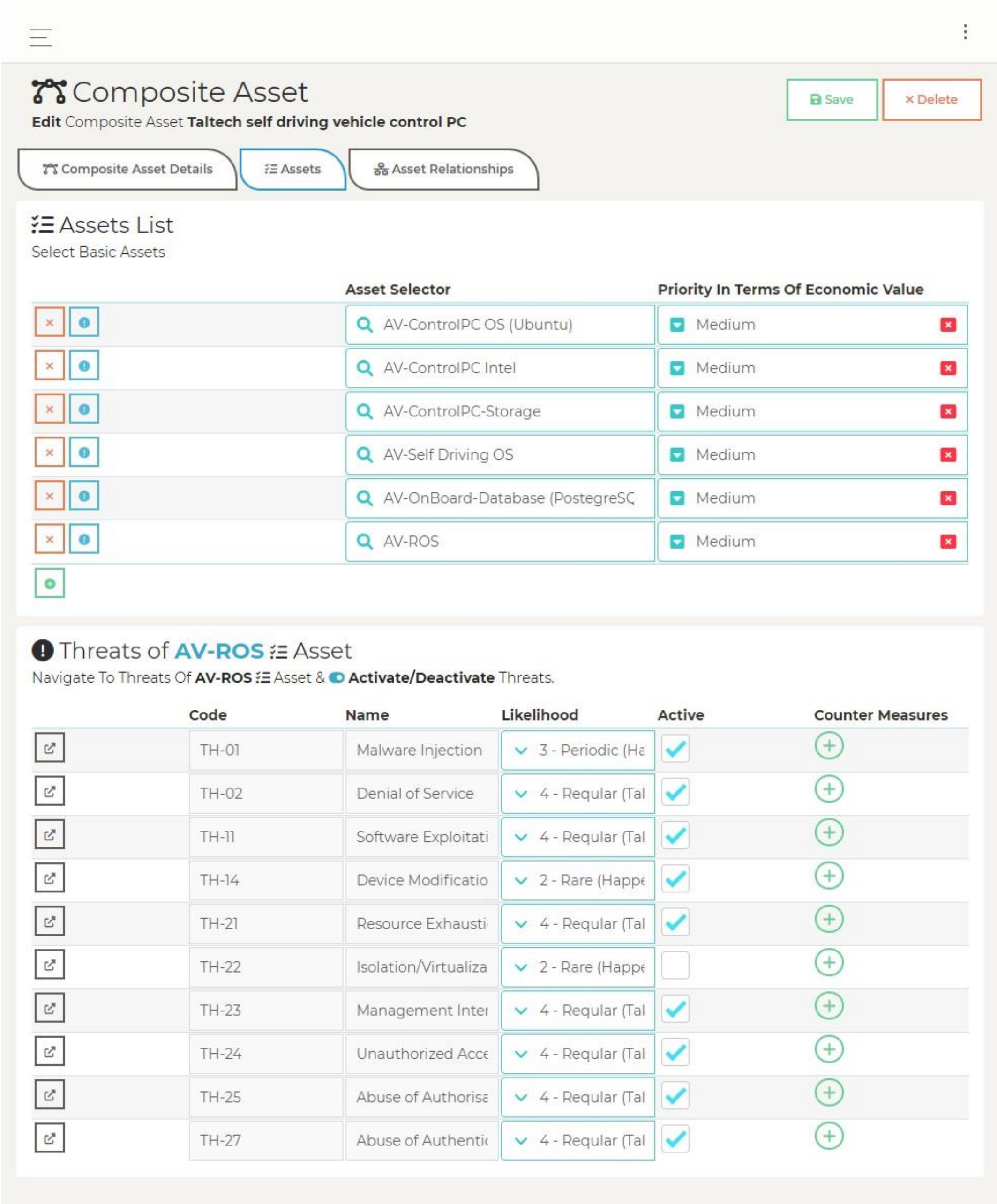


Figure 18. Main-Control-PC (AV-ROS Threats and Likelihoods)

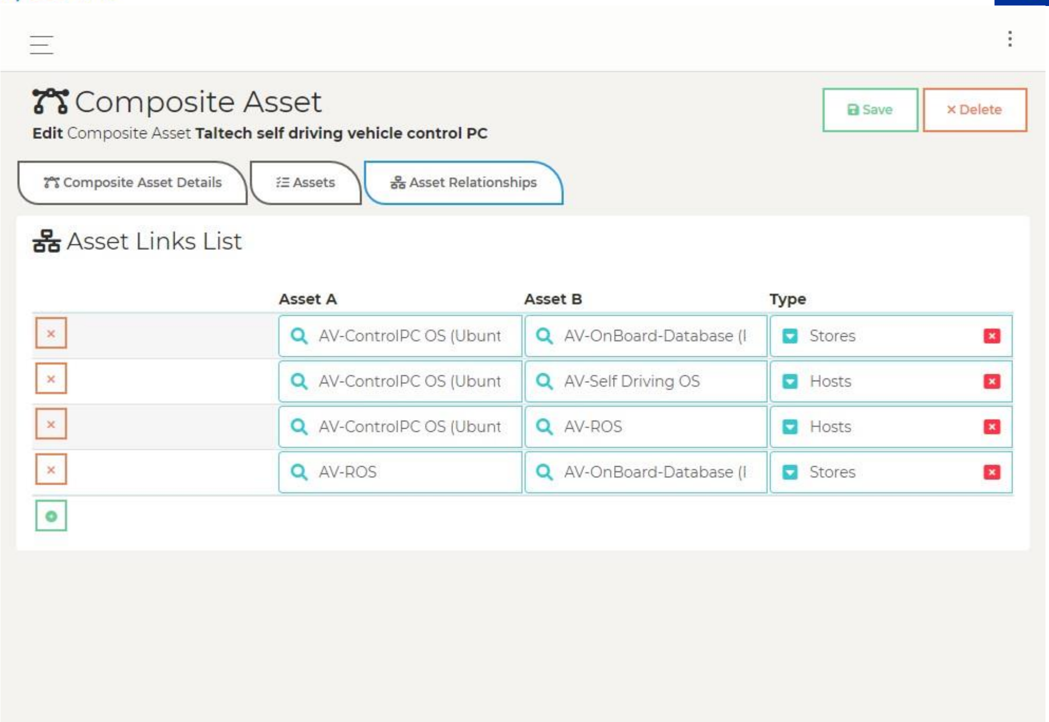


Figure 19. Main-Control-PC (Asset Relationships)

ANNEX III - RITA TEST-CASE 2 DEMO FUNCTIONALITY

- Test-Case 2 Asset Cost Evaluation

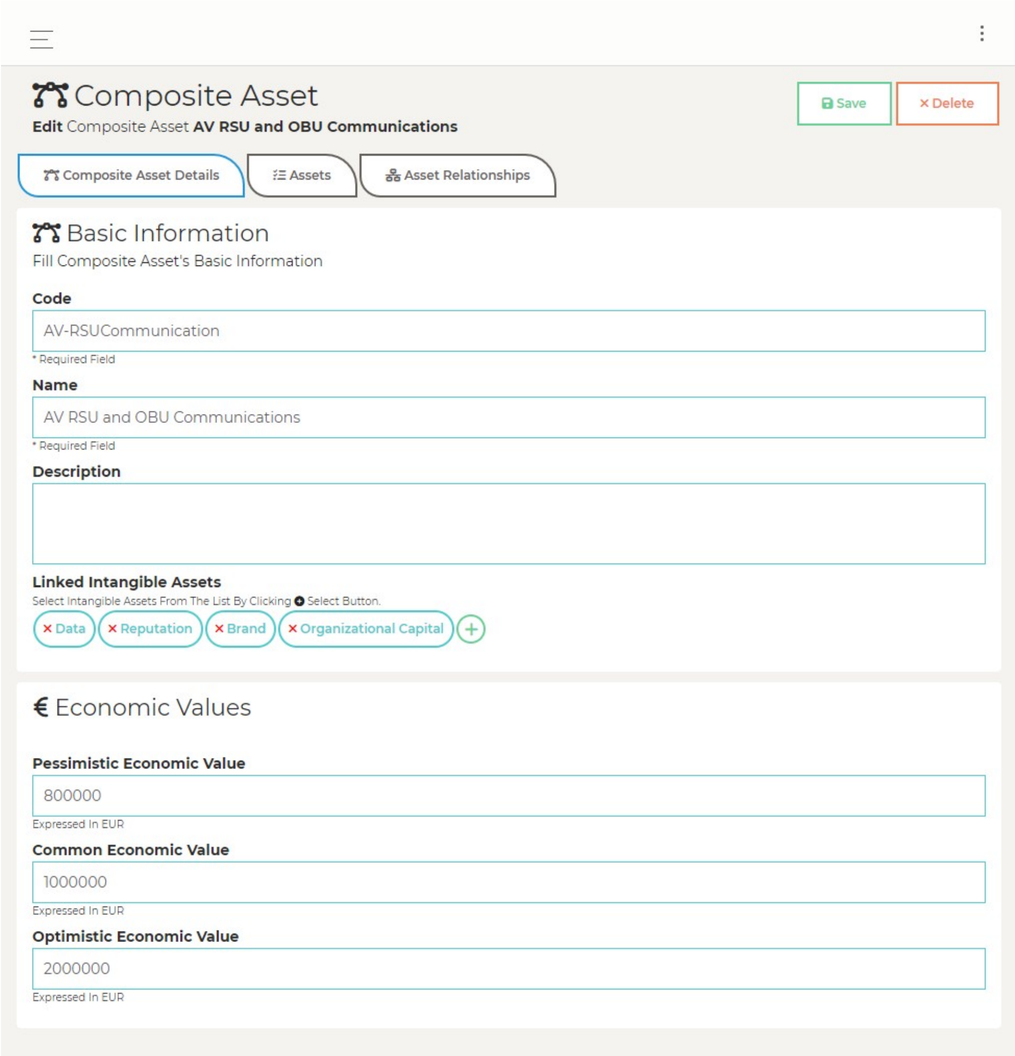


Figure 20. AV RSU and OBU Communications (Basic Information)

- RITA Threat Mapping Test-Case 2

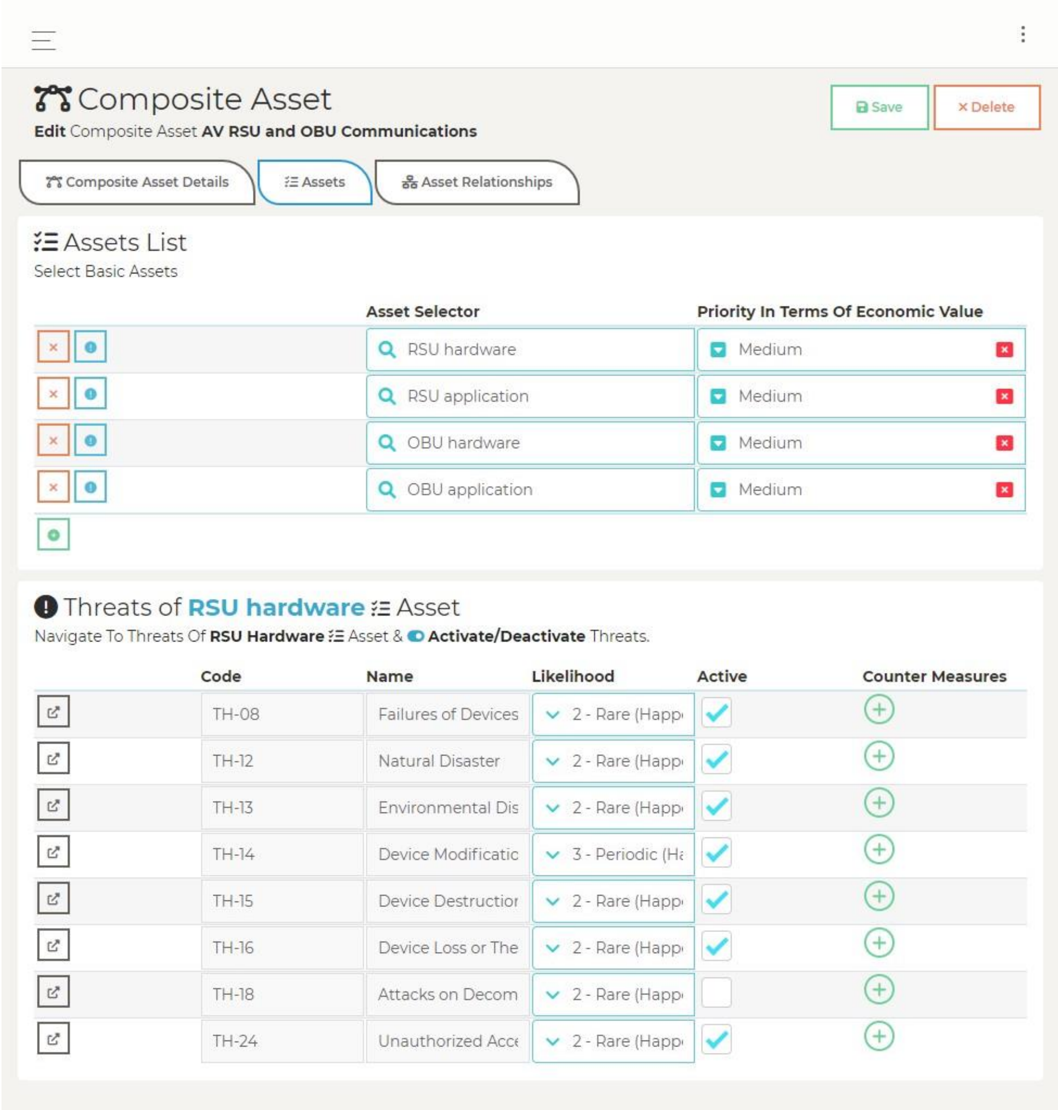


Figure 21. AV RSU and OBU Communications (RSU hardware and Likehoods)

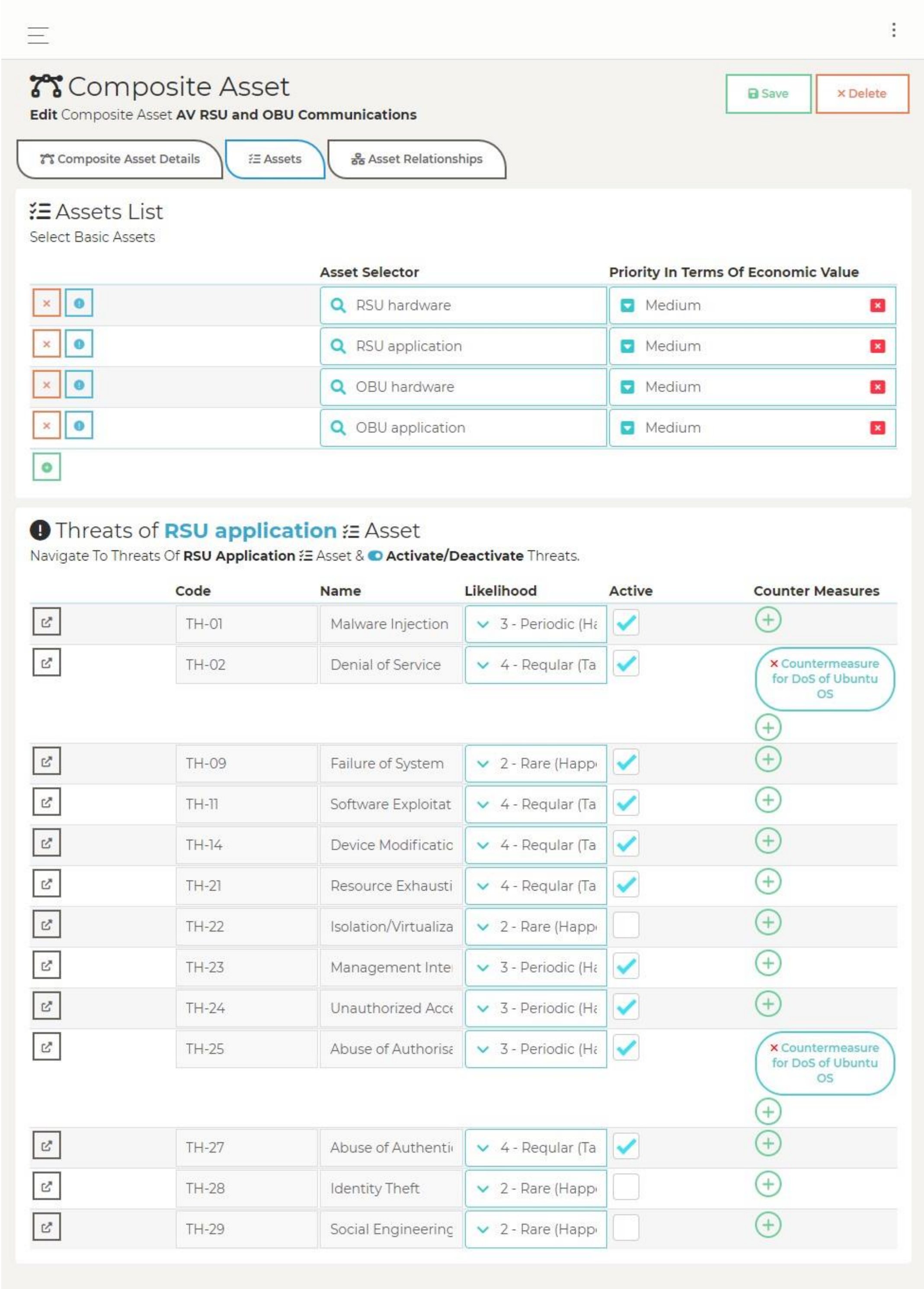


Figure 22. AV RSU and OBU Communications (RSU application Threats and Likehoods)

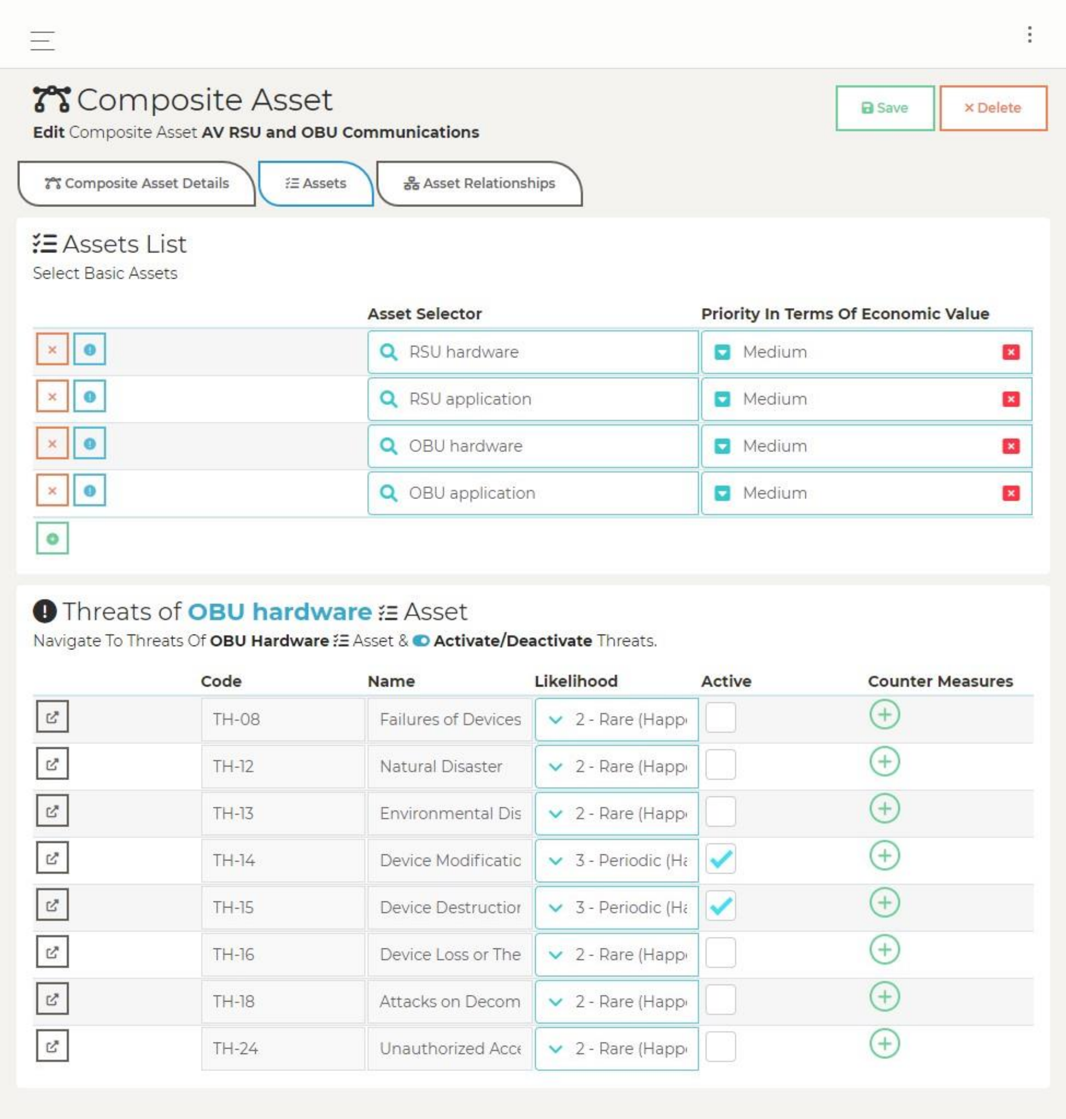


Figure 23. AV RSU and OBU Communications (OBU hardware Threats and Likehoods)

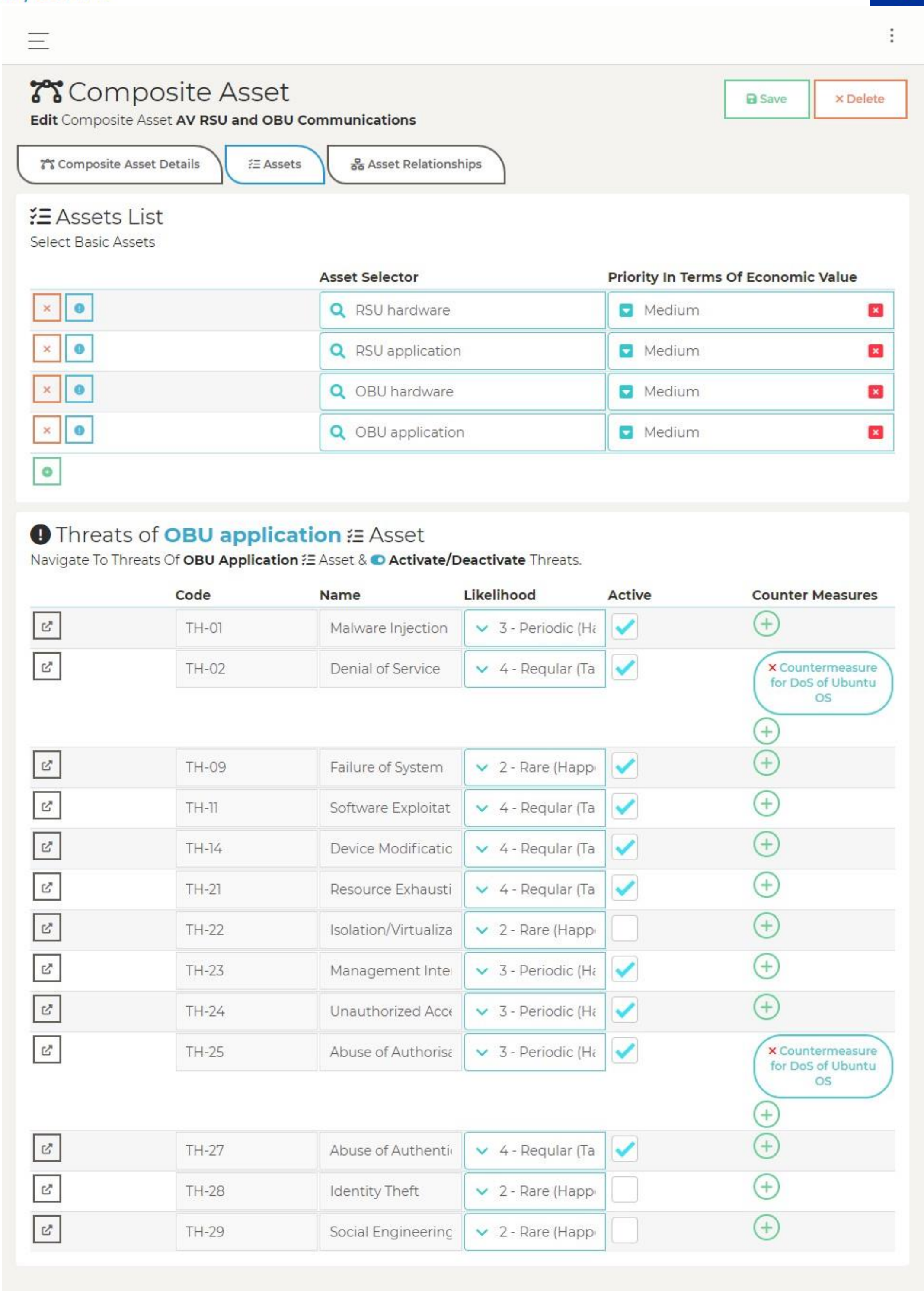


Figure 24. AV RSU and OBU Communications (OBU application Threats and Likehoods)

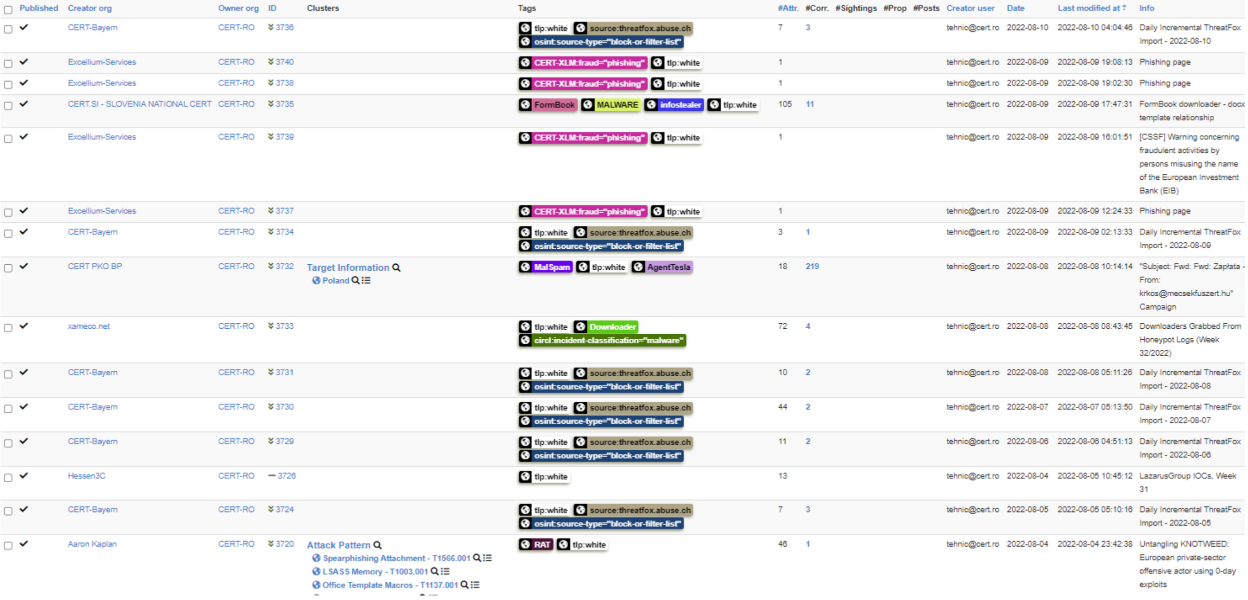
ANNEX IV - CTI EXCHANGE WITH DNSC

It is essential that the cybersecurity tests do not impact operational systems of Tallinn University of Technology. The cybersecurity tests need to be performed on a network which is isolated from the university and will not have the potentiality to have cascading impacts on real-world/live services. The weeks of August 8th to 18th will be used to prepare the Tallinn Pilot Demonstration.

Any cybersecurity solution needs to be updated based on changes in the cyber threat landscape, which is where shared CTI enters the picture. Threat sharing platforms such as MISP ensure that new threats can be identified more quickly such that response can be adequately coordinated.

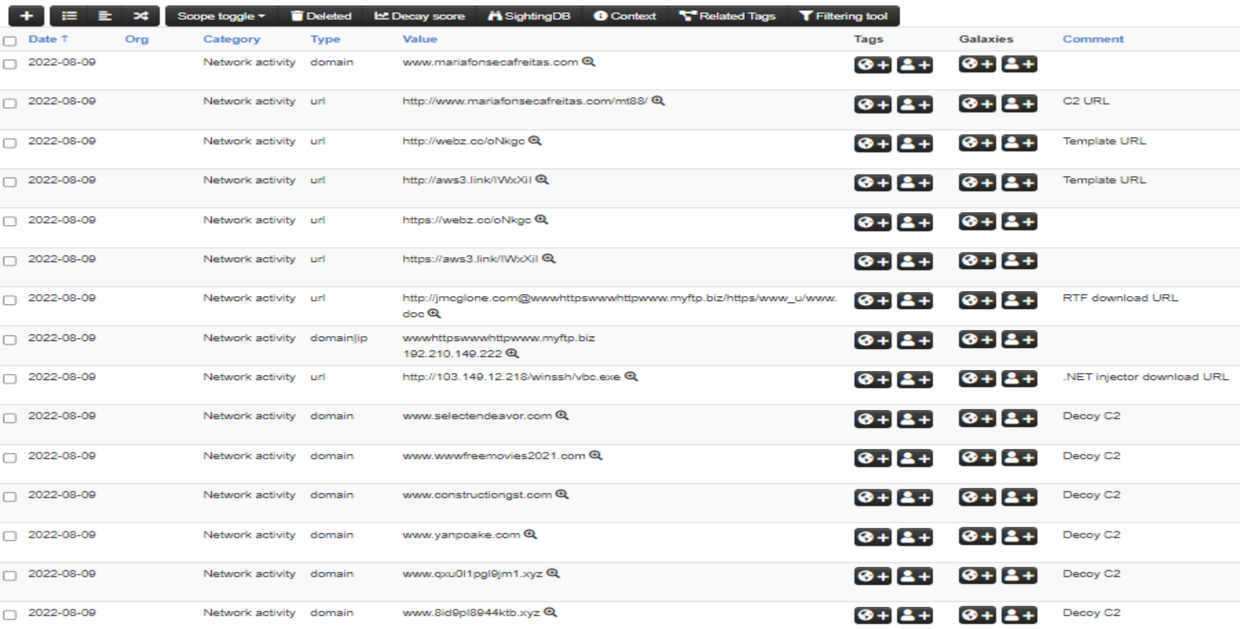
DNSC, the Romanian CERT that is a partner in the CitySCAPE project, uses MISP for the collection of cybersecurity alerts from different stakeholders. The platform is used for the collection, processing, and dissemination of data related to cybersecurity incidents, vulnerabilities, threats, events, and artefacts, including incident notifications received by DNSC. Information such as malicious URLs, IPs, and file signatures are usually distributed through this module.

During pilot execution in Tallinn DNSC presented how it exchanges IOCs with other entities. DNSC's MISP data tagged with 'TLP:WHITE' can be made available to CitySCAPE in a feed that can be imported in the CitySCAPE platform. TLP stands for Traffic Light Protocol; a protocol created to promote the sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four main tags to indicate expected sharing boundaries to be applied by the recipient(s). The four tags are red (named recipients only), amber (limited distribution), green (community-wide distribution), and clear/white (unlimited distribution). CitySCAPE will receive only TLP:CLEAR/TLP:WHITE data for now. DNSC usually shares IOCs from last 7 days. To facilitate sharing, DNSC IOCs are also available via SFTP. The print-screens below show examples of TLP:WHITE type events that can be exported from the DNSC MISP, examples of attributes (IOCs) attached to an event and also examples of IOCs exported to the SFTP server.



Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	#Sightings	#Prop	#Posts	Creator user	Date	Last modified at	Info
✔	CERT-Bayern	CERT-RO	3736		tlp:white source:threatfox.abuse.ch osint:source-type="block-or-filter-list"	7	3				tehnic@cert.ro	2022-08-10	2022-08-10 04:04:46	Daily Incremental ThreatFox Import - 2022-08-10
✔	Excellium-Services	CERT-RO	3740		CERT-XLM:fraud="phishing" tlp:white	1					tehnic@cert.ro	2022-08-09	2022-08-09 19:08:13	Phishing page
✔	Excellium-Services	CERT-RO	3738		CERT-XLM:fraud="phishing" tlp:white	1					tehnic@cert.ro	2022-08-09	2022-08-09 19:02:30	Phishing page
✔	CERT.SI - SLOVENIA NATIONAL CERT	CERT-RO	3735		FormBook MALWARE infostealer tlp:white	105	11				tehnic@cert.ro	2022-08-09	2022-08-09 17:47:31	FormBook downloader - docx template relationship
✔	Excellium-Services	CERT-RO	3739		CERT-XLM:fraud="phishing" tlp:white	1					tehnic@cert.ro	2022-08-09	2022-08-09 16:01:51	[CSSF] Warning concerning fraudulent activities by persons misusing the name of the European Investment Bank (EIB)
✔	Excellium-Services	CERT-RO	3737		CERT-XLM:fraud="phishing" tlp:white	1					tehnic@cert.ro	2022-08-09	2022-08-09 12:24:33	Phishing page
✔	CERT-Bayern	CERT-RO	3734		tlp:white source:threatfox.abuse.ch osint:source-type="block-or-filter-list"	3	1				tehnic@cert.ro	2022-08-09	2022-08-09 02:13:33	Daily Incremental ThreatFox Import - 2022-08-09
✔	CERT PKO BP	CERT-RO	3732	Target Information Poland	MalSpam tlp:white AgentTesla	18	219				tehnic@cert.ro	2022-08-08	2022-08-08 10:14:14	"Subject: Fwd: Fwd: Zapłata - From: krkos@mecsekfuszert.hu" Campaign
✔	xameco.net	CERT-RO	3733		tlp:white Downloader circl:incident-classification="malware"	72	4				tehnic@cert.ro	2022-08-08	2022-08-08 08:43:45	Downloaders Grabbed From Honeypot Logs (Week 32/2022)
✔	CERT-Bayern	CERT-RO	3731		tlp:white source:threatfox.abuse.ch osint:source-type="block-or-filter-list"	10	2				tehnic@cert.ro	2022-08-08	2022-08-08 05:11:26	Daily Incremental ThreatFox Import - 2022-08-08
✔	CERT-Bayern	CERT-RO	3730		tlp:white source:threatfox.abuse.ch osint:source-type="block-or-filter-list"	44	2				tehnic@cert.ro	2022-08-07	2022-08-07 05:13:50	Daily Incremental ThreatFox Import - 2022-08-07
✔	CERT-Bayern	CERT-RO	3729		tlp:white source:threatfox.abuse.ch osint:source-type="block-or-filter-list"	11	2				tehnic@cert.ro	2022-08-06	2022-08-06 04:51:13	Daily Incremental ThreatFox Import - 2022-08-06
✔	Hessen3C	CERT-RO	— 3726		tlp:white	13					tehnic@cert.ro	2022-08-04	2022-08-05 10:45:12	LazarusGroup IOCs, Week 31
✔	CERT-Bayern	CERT-RO	3724		tlp:white source:threatfox.abuse.ch osint:source-type="block-or-filter-list"	7	3				tehnic@cert.ro	2022-08-05	2022-08-05 05:10:16	Daily Incremental ThreatFox Import - 2022-08-05
✔	Aaron Kaplan	CERT-RO	3720	Attack Pattern Spearphishing Attachment - T1566.001 LSASS Memory - T1003.001 Office Template Macros - T1137.001	RAT tlp:white	46	1				tehnic@cert.ro	2022-08-04	2022-08-04 23:42:38	Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits

Figure 26. TLP: WHITE MISP events



Scope toggle | Deleted | Decay score | SightingDB | Context | Related Tags | Filtering tool

Date	Org	Category	Type	Value	Tags	Galaxies	Comment
2022-08-09		Network activity	domain	www.mariafonsecafreitas.com			
2022-08-09		Network activity	url	http://www.mariafonsecafreitas.com/mt88/			C2 URL
2022-08-09		Network activity	url	http://webz.cc/oNkgc			Template URL
2022-08-09		Network activity	url	http://aws3.link/lWxXil			Template URL
2022-08-09		Network activity	url	https://webz.cc/oNkgc			
2022-08-09		Network activity	url	https://aws3.link/lWxXil			
2022-08-09		Network activity	url	http://jmoglone.com@wwwhttpswwwhttpwww.myftp.biz/https/www_u/www.doc			RTF download URL
2022-08-09		Network activity	domain|ip	wwwhttpswwwhttpwww.myftp.biz 192.210.149.222			
2022-08-09		Network activity	url	http://103.149.12.218/winssh/vbc.exe			.NET injector download URL
2022-08-09		Network activity	domain	www.selectendeavor.com			Decoy C2
2022-08-09		Network activity	domain	www.wwwfreemovies2021.com			Decoy C2
2022-08-09		Network activity	domain	www.constructiongst.com			Decoy C2
2022-08-09		Network activity	domain	www.yanpoake.com			Decoy C2
2022-08-09		Network activity	domain	www.qxu0l1pgl9jm1.xyz			Decoy C2
2022-08-09		Network activity	domain	www.8id9pl8944ktb.xyz			Decoy C2

Figure 27. MISP event attributes

feed_tlp-white_domain.txt

```
amakpost.com
alicehui.com
amasides.my.id
alinac.ca
alsanjari.co.uk
alinatourbg.com
alsancaklimanemlak.com
```

feed_tlp-white_ip-dst.txt

```
95.142.46.35
80.233.134.147
95.141.37.3
93.190.137.212
109.192.30.125
80.153.75.103
93.51.177.66
```

feed_tlp-white_ip-dst-port.txt

```
160.176.72.124|443
120.61.3.72|443
129.208.171.212|995
79.141.164.139|80
201.22.52.216|443
197.89.109.218|443
39.52.13.165|995
```

feed_tlp-white_md5.txt

```
6c10466ad7c153e7f949fa3c6600b6ac
ffb1e8babaecc4a8cb3d763412294469
b75c869561e014f4d384773427c879a6
0fce93cd9beeea30a7f0e2a819d2b968
75ee947e31a40ab4b5cde9f4a767310b
24313581bbbffa9a784b48075b525810
```

feed_tlp-white_sha256.txt

```
5c7286df292fbb73f350828f6c46f2e80964fa22566388186950e04858feff1e
979f9d1e019d9172af73428a1b3cbdff8aec8fdbe0f67cba48971a36f5001da9
8f2ea18ed82085574888a03547a020b7009e05ae0ecbf4e9e0b8fe8502059aae
696b6b9f43e53387f7cef14c5da9b6c02b6bf4095849885d36479f8996e7e473
610ec163e7b34abd5587616db8dac7e34b1aef68d0260510854d6b3912fb0008
107da216ad99b7c0171745fe7f826e51b27b1812d435b55c3ddb801e23137d8f
1f36898228197ee30c7b0ec0e48e804caa6edec33e3a91eeaf7aa2c5bbb9c6e0
```

feed_tlp-white_url.txt

```
http://171.81.64.182:40182/Mozi.m
http://27.202.44.93:55209/Mozi.m
https://ejeana.co.ug/index.php
http://ejeana.co.ug/index.php
http://yadrochy.ru.com/ImageGamebigloadGeneratorTemp.php
http://51.15.62.59/AED77D05-A028-477C-B013-04F33F1385C3/index.php
https://cdn.discordapp.com/attachments/953078028693553272/953079659447332884/botnet
https://cdn.discordapp.com/attachments/953078028693553272/953079659208269864/botnet
https://cdn.discordapp.com/attachments/953078028693553272/953079658633654323/botnet
https://cdn.discordapp.com/attachments/953078028693553272/953079658813993020/botnet
https://cdn.discordapp.com/attachments/953078028693553272/953079658998530049/botnet
http://142.11.213.113/EkSgbins.sh
https://onedrive.live.com/download?cid=D31E0CBB0FDCD228&resid=D31E0CBB0FDCD228%21222
&authkey=AFH3-1bOqXg0i-U
https://focused-raman.62-4-21-193.plesk.page/o
http://www.infiniteinvesting.net/rzwo/
http://103.156.91.63/cloud__to_drive/vbc.exe
```

Fig 28. IOCs from SFTP files exported from MISP

Considering that the exchange of IOCs is bidirectional, it was also discussed how DNSC can receive CTI from CitySCAPE (either through the MISP platform installed in CitySCAPE, or through the SFTP server installed at DNSC level).