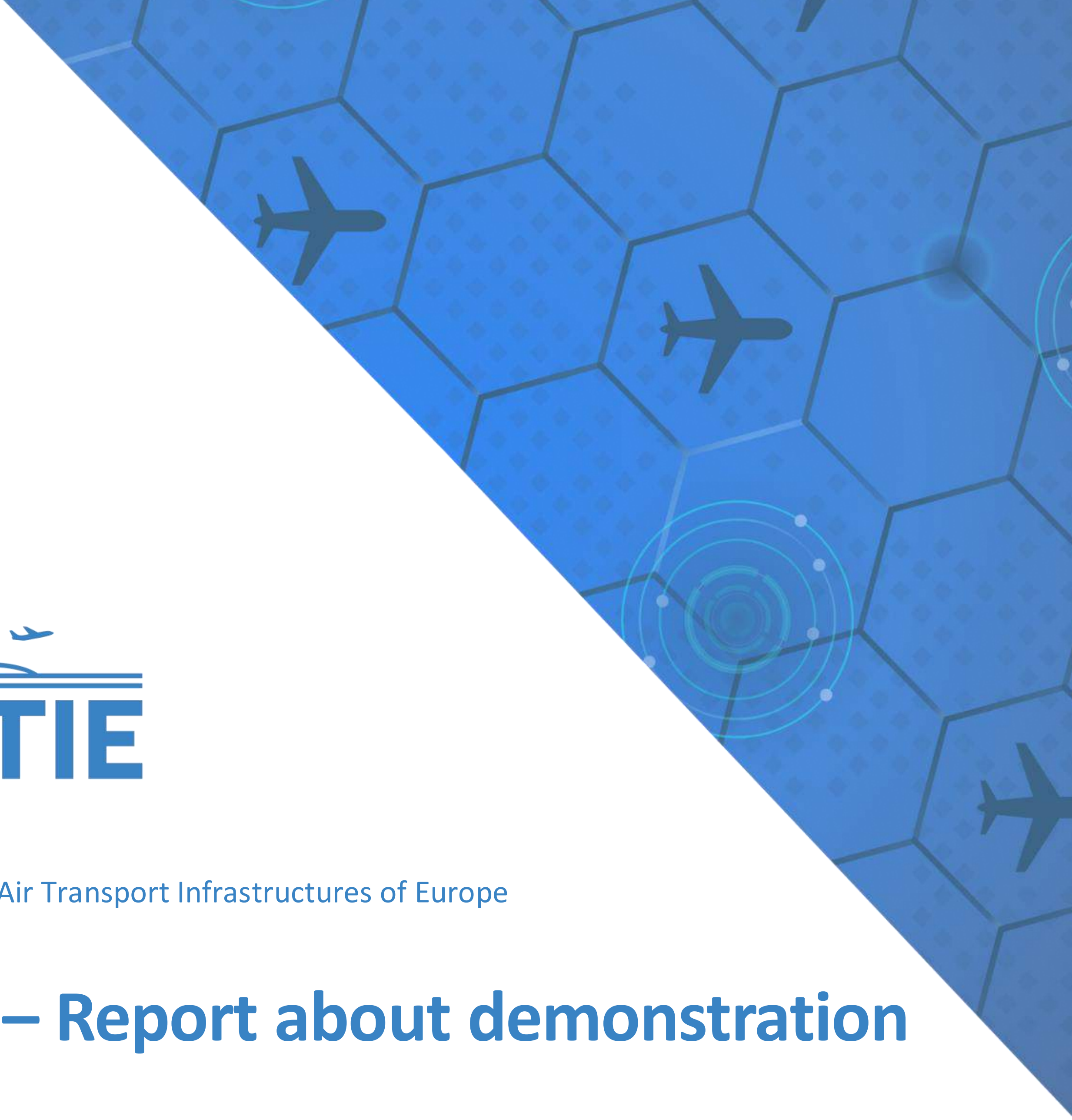


SATIE

Security of Air Transport Infrastructures of Europe

D6.6 – Report about demonstration and results in Milan Airport

Deliverable Number	D6.6
Author(s)	SEA, DLR, DGS, ACS, FHG, ITTI, ISEP, SAT, IDE
Due/delivered Date	M30/2021-11-05
Reviewed by	ACS, KEMEA, DLR
Dissemination Level	PU
Version of template	1.083

Start Date of Project: 2019-05-01

Duration: 30 months

Grant agreement: 832969

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969

DISCLAIMER

Although the SATIE consortium members endeavour to deliver appropriate quality to the work in question, no guarantee can be given on the correctness or completeness of the content of this document and neither the European Commission, nor the SATIE consortium members are responsible or may be held accountable for inaccuracies or omissions or any direct, indirect, special, consequential or other losses or damages of any kind arising out of the reliance upon the content of this work.

The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. All intellectual property rights are owned by the SATIE consortium members and are protected by the applicable laws. Except where otherwise specified, all document contents are: "©SATIE Project – All rights reserved". Reproduction is not authorised without prior written agreement.

Document contributors

No.	Name	Role (content contributor / reviewer / other)
1	Elena Branchini (SEA)	Content contributor
2	Andrei-Vlad Predescu (DLR)	Content contributor
3	Tim Stelkens-Kobsch (DLR)	Content contributor
4	Marco Albertario (SEA)	Content contributor
5	Thomas Oudin (ACS)	Content Contributor
6	Kelly Burke (DGS)	Content contributor
7	Eva Catarina Gomes Maia (ISEP)	Content contributor
8	Corinna Köpke (FHG)	Content contributor
9	Thomas Mauger (IDE)	Content Contributor
10	Nils Carstengerdes (DLR)	Content contributor
11	David Lancelin (ACS)	Technical Review
12	Vasileios Kazoukas (KEMEA)	Security Review
13	Meilin Schaper (DLR)	Quality Review

Document revisions

Revision	Date	Comment	Author
V0.1	2021-10-05	Initial draft	Elena Branchini
V0.2	2021-10-05	Sections 2.1 and 2.2	Elena Branchini
V0.3	2021-10-06	Sections 3.1, 3.2 and 3.3	Thomas Oudin
V0.3	2021-10-07	Section 3.9	Kelly Burke
V0.4	2021-10-11	Sections 2.3.1 – 2.4	Elena Branchini
V0.4	2021.10.11	Section 3.8	Eva Catarina Gomes Maia
V0.5	2021.10.21	Intermediate review	Andrei-Vlad Predescu Tim Stelkens-Kobsch
V0.5	2021.10.21	Sections 2.3.2 – 2.3.2.2 – 2.3.2.3 – 2.3.2.4 – 2.3.2.5	Marco Albertario
V0.6	2021.10.21	Sections 2.3.2.1 – 2.5 – 2.5.1, section 2.4 review	Elena Branchini
V0.6	2021-10-22	Section 3.7	Corinna Köpke
V0.6	2021-10-26	Section 3.5	Thomas Mauger
V0.6	2021-10-26	Section 2.3.2.2 integration, section 2.3.2 harmonization	Marco Albertario
V0.7	2021-10-26	Merge contents – check contents – new version	Elena Branchini
V0.8	2021-10-27	Executive summary – Introduction – Chapter 2 revision – Chapter 5 revision	Elena Branchini
V0.9	2021-10-28	Revisions of the Executive summary – Introduction – Chapter 2 revision – Chapter 5 revision	Andrei-Vlad Predescu Marco Albertario Elena Branchini
V0.9	2021-11-03	Final technical check and approval for submission	David Lancelin, Technical Manager
V0.9	2021-11-04	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V0.10	2021-11-04	Minor update in conclusions	Elena Branchini
V1.0	2021-11-05	Final quality check and approval for submission	Meilin Schaper, Quality Manager

Executive summary

This deliverable is a report about the demonstration event held in Milan Malpensa Airport at 8th September 2021, corresponding to SATIE Task 6.5 (Integration and demonstration in Milan airport). The objective of D6.6 is to provide the results of SATIE applied to a real airport environment scenario where, in normal operating conditions, the solution turns out to be a vital decision support tool to prevent or mitigate the cyber and physical attacks. This clearly emerges during the execution of the various phases of the scenario, when the Milan Malpensa Airport systems are attacked, putting at risk the passengers in land side, as well as passengers and aircraft in the air side. Also, a physical unauthorized access attempt is carried out through the scenario.

Table of Content

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
ABM	Agent-Based Model
ACS	Airbus Cyber Security
AI	Artificial Intelligence
ALCAD	Application Layer Cyber Attack Detection
AOC	Airport Operations Centre
AOCC	Airport Operations Control Centre
AODB	Airport Operations Data Base
ATM	Air Traffic Management
BHS	Baggage Handling System
BIA	Business Impact Assessment
BP-IDS	Business Process-based Intrusion Detection System
CAS	Crisis Alerting System
CCTV	Closed-Circuit Television
CE	Correlation Engine
CERT	Computer Emergency Response Team
CEST	Central European Summer Time
CI	Critical Infrastructure
COVID-19	Coronavirus Disease 2019
DLR	Deutsche Zentrum für Luft- und Raumfahrt e. V.
DNS	Domain Name System
EU	European Union
FIDS	Flight Information Display System
GLPI	Gestionnaire Libre de Parc Informatique
ICT	Information and Communications Technology
ID	Identification number
IE	Innovation Element
IMP	Incident Management Portal
IP	Internet Protocol

Acronym	Definition
IPS	Impact Propagation Simulation
IPT	Impact Propagation Tools
ISEP	Instituto Superior de Engenharia do Porto
IT	Information Technology
KPI	Key Performance Indicator
MA	Malware Analyser
M-AIS	Milan Airport Information System
ML	Machine Learning
MXP	Milan Malpensa International Airport
NAT	Network Address Translation
PAD	Passenger Anomaly Detection
PC	Personal Computer
RDP	Remote Desktop Protocol
RIS	Risk Integrated Service
RMS	Resource Management System
SATIE	Security of Air Transport Infrastructures of Europe
SEA	Società per Azioni Esercizi Aeroportuali
SMS	Short Message Service
SMS-I	Investigation Tool
SOC	Security Operations Centre
SSH	Secure Shell
TAP	Test Access Point
UAC	Unified Access Control
UI	User Interface
USB	Universal Serial Bus
VIP	Vulnerability Intelligence Platform
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VuMS	Vulnerability Management System

1 Introduction

The present document ends the series of deliverables from the Work Package 6 (WP6), work package which was responsible for the activities related to the "Integration, test, validation and demonstration" of the SATIE Solution. This work package represents a big effort in terms of persons/months in SATIE, accounting for more than one fifth of the total project's effort.

The work package started with Task 6.1, which was the preparation and integration on the simulation platform. The objective of the task was to provide a simulation environment which allows partners to integrate, interconnect and test their solutions in near real conditions. In this fundamental task, the SATIE Tools for threat prevention, threat detection, incident response and impact mitigation were deployed and integrated together on the CyberRange platform to implement the SATIE Solution.

The next task, Task 6.2 "Test, verification and validation", represented the link between Task 6.1 and the final tasks referred to the demonstrations in the three Airports. The task outlined (in D6.2 "Test, validation and demonstration scenarios" (1)) the specific scenarios which were conducted and tested during the first step of the SATIE Solution's validation in a simulation environment (in D6.3 "Test and validation results on the simulation platform" (2)). Some of the issues identified during the first part of the validation conducted in the simulation scenarios were addressed before the second part of the validation (i.e.: the final demonstrations) begun. As a consequence, also the SATIE Solution received some improvements according to the results of the first validation step (i.e.: the simulations).

The final three tasks of WP6 (T6.3 "Integration and demonstration in Zagreb airport" – T6.4 "Integration and demonstration in Athens airport" – T6.5 "Integration and demonstration in Milan airport") represent the second, and final, step of the SATIE Solution's validation. The respective results are reported in the deliverables D6.4 (Zagreb demonstration) (3), D6.5 (Athens demonstration) (4) and this one, D6.6 (Milan demonstration). The demonstrations highlight that the SATIE Solution potentially corresponds to a holistic, interoperable and modular security toolkit to be exploited by the next generation of Airport Operations Centre (AOC) and Security Operations Centre (SOC).

The purpose of the Milan Malpensa demonstration is to confirm in a real operational scenario the benefits of the SATIE Solution. Actually, the demonstration showed that SATIE can potentially protect land side, air side, as well as restricted areas from cyber, physical and cyber-physical attacks. The SATIE Solution has been tailored specifically for the needs of the airport, therefore, once deployed, it successfully helped in mitigating the risks associated with the threats derived from the attacks.

The present D6.6 reflects the results of the Milan Malpensa demonstration including the preparation, the conduction of the actual event and feedback gained from the demonstration's aftermath. The deliverable is divided in the following five chapters:

- Chapter 1 of this document explains WP6 and its related tasks and deliverables, besides recalling the description of the dynamics between the main actors involved: AOC operators and SOC operators;
- Chapter 2 explains in detail the Milan Airport demonstration. It contains a thorough explanation of the activities carried out in preparation of the demonstration and an overview of the demonstration event. Also, a detailed focus is made on the locations used and on the integration of the cyber and physical infrastructure on SEA and ACS side, including the steps towards this integration. The description of the operations during the event is followed by the details of demonstration Scenario #3 that include the SAIE Tools involved in the scenario and the storyboard behind it. The chapter 2 ends with Table 2.1 which explains all the steps of the demonstration set-up and their related tools;
- Chapter 3 presents how the SATIE Solution and the accompanying components have been used to detect the cyber and physical threats of the attack scenarios described in section 2.5;

- Chapter 4 presents the evaluation results of the Milan Malpensa Airport demonstration. These provide a tangible assessment of the success factors, including information gained from questionnaires and evaluation participants' (positive) feedback. The chapter opens with the presentation of the KPIs related to the Milan Malpensa Airport demonstration, together with a brief description about their assessment, and followed by the questionnaire results analysis. It is useful here to highlight that the initial target of the KPIS is prevailingly reached or overcome;
- Lastly, chapter 5 is the "Conclusions" chapter, containing the lessons learned.

2 Milan International Airport demonstration

The demonstration event in Italy was organized by SEA, Società per Azioni Esercizi Aeroportuali, the company managing the Milan Linate and Milan Malpensa Airports, with the technical support of all the partners.

The SATIE Milan Malpensa demonstration event was carried out on the 8th of September, 2021 at the Milan Malpensa International Airport (MXP) premises in Somma Lombardo, Lombardy region, Italy (Figure 2.1). Due to the COVID-19 health and safety protocols and travelling restrictions, it was a hybrid – i.e. both virtual and physical – event, consisting of a combination of pre-recorded video materials, real-time live streaming and live-performance scenario demonstrations.

Figure 2.1: The Milan Malpensa Airport premises

The present chapter describes in detail all the demonstration-specific operations performed in Milan Malpensa. Section 2.1 describes SEA's activities towards the demonstration, while Section 2.2 presents an overview of the Milan Malpensa demonstration event. Section 2.3 describes the airport sites used during the live demonstration, including event localization and logistics information (section 2.3.1), and explains the MXP cyber and physical infrastructure used for the execution of the demonstration scenarios, as well as the airport's infrastructure and systems integration with the SATIE Solution (section 2.3.2). Section 2.4 describes the coordinated activities undertaken by SEA and the SATIE technical partners that took place, live, during the Milan Malpensa demonstration event. Section 2.5 gives a quick overview of the SATIE Tools that were used to address the cyber and physical attacks. It also describes and explains in detail the steps and all the actions carried out during the execution of the threat scenarios by the SOC, AOC operators and by the moderator to carry out this second and final part of the validation (after the simulation, as said in chapter 1).

2.1 Activities towards the demonstration

In preparation of the Milan Malpensa demonstration event, three among SEA's ICT Dept employees and two among SEA's Operations Dept employees voluntarily joined the project with the role of SOC operators, AOC operators and a hacker (Figure 2.2). As to SOC operators, the role was played by two

ICT Help Desk Specialists, and one ICT Security Manager, as to AOC operators, the role was played by one Deputy AOCC Manager and one Airport Duty Manager, the role of the hacker was played by the Airport Operations Applications Manager (actually the father of the Airport Operations Data Base and its "*shadow*" replica used to test SATIE, i.e. M-AIS, the Milan Airport Information System).

Figure 2.2: Presentation of SEA's hacker, SOC and AOC operators during the Milan Malpensa demonstration event

SEA's Team, supported by SEA's SATIE project coordinator, had been trained in using the SATIE Tools during the SATIE training days dedicated to SEA that took place remotely in two half days on the 9th and on the 11th of March 2021. The scope of the training workshop was to get the SOC and AOC operators of the Milan Malpensa Airport familiarized with the SATIE Tools, in order to use them in the two most important steps of the Project: I) the simulation/validation first and II) the demonstration event later.

The simulation/validation event took place remotely in one and a half day on the 27th and on the 28th of April 2021. The results of the simulation/validation event are reported in D6.3: "Test and validation results on the simulation platform" (2). The simulation/validation of the SATIE Solution in the simulation environment was performed by four of the five participants from the Milan Malpensa Airport and included three SOC operators and one AOC operator. The Milan Malpensa SATIE Team faced five complex cyber-physical threat scenarios, that means fifteen run-throughs in total. The Team was satisfied, except for some specific terms in use in Zagreb as to BHS and in Athens as to passport control, that required some explanation from the other airport scenario owners.

Both the training and the simulation/validation event were supported by a comprehensive training handbook (5).

To prepare themselves at their best for the demonstration, whose initial date was June 2021, SEA's SATIE Team required that the platform remained open in order for them to keep "*hands on*" it and get more familiar with its main functionalities. Being SATIE a research project, the tool has not been adopted, therefore it is not used every day as a cyber security tool. This is why, responsibly, SEA explained this issue to the platform owner (ACS) and to all the tools owners and required to be able to carry out some extra internal sessions called "*SEA's self-training sessions*". These were carried jointly by the whole team on:

- 17th March 2021;
- 25th March 2021;

- 31st March 2021;
- 22nd April 2021 (in preparation of the simulation/validation);
- 17th May 2021;
- 14th, 15th and 16th June 2021 (during the registration of the Scenario#3 video);
- 22nd July 2021;
- 27th August 2021 (RIS and SMS-I specific training for demonstration);
- 1st, 3rd, 6th and 7th September 2021(in preparation of the demonstration).

Each session until the one in July lasted more or less 3,5 hours and was followed by a debriefing session where the impressions of the participants were gathered and translated into suggestions for the technical partners. The August and September sessions were completely demonstration oriented and were fully supported by the technical partners, especially ISEP and DGS for the ones held 27th August and ACS for the ones immediately before the demonstration in September.

The functioning of SATIE became clearer when it became fully ready for use and SEA started using it. SEA had the opportunity to analyse the various SATIE components in order to establish which ones could be most useful in the Malpensa scenario, and decided to include:

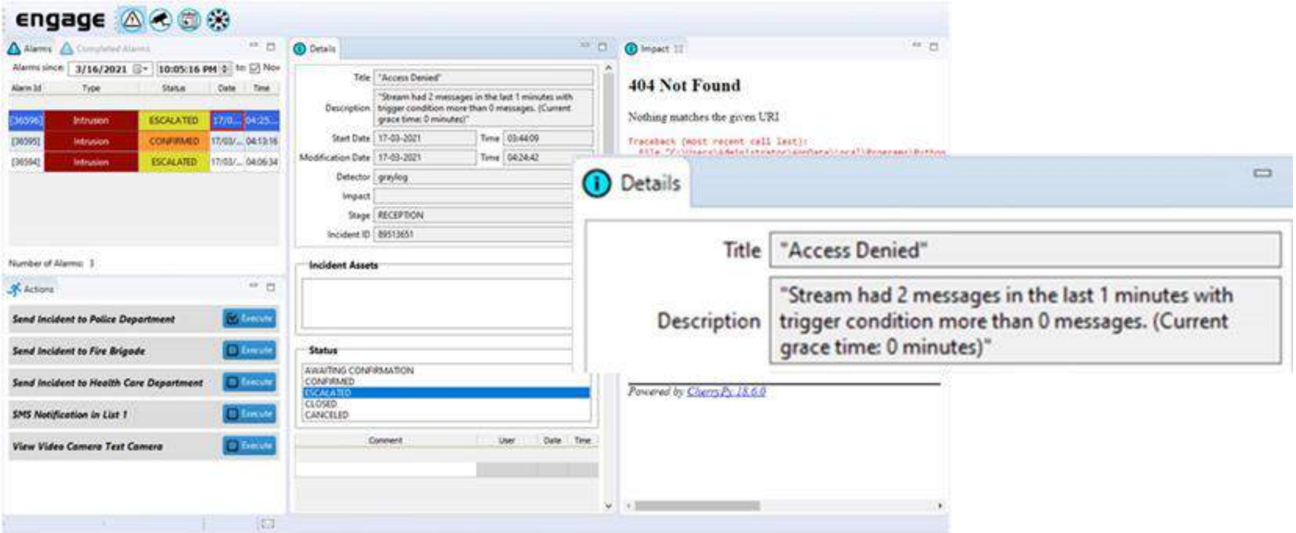
- the Crisis Alerting System,
- the Impact Propagation Simulation – particularly the Agent Based Model.

None of the two was included in the SEA scenario according to the Description of the Action.

To help customize SATIE for the market, SEA transferred the outputs of the initial sessions to the technical partners, especially ACS and Satways, according to its idea of a possible usage at the airport. Below, some examples to improve specific fields can be found:

- Operational – Communication between SOC and AOC

  Initially the Alert[1] message sent from the SOC to the AOC was computer-generated and thus not understandable for the AOC operators (Figure 2.3). SEA requested that the information sent from the SOC to the AOC be written in a free text form, clearly reporting in the "Description" field of the Crisis Alerting System (CAS) the details of the alarms described in the Correlation Engine (CE). As a result, ACS modified the Incident Management Portal software accordingly and Satways modified the "Description" field in the " Details" box section of the main page of the CAS.



Alarms since: 3/16/2021 10:05:16 PM to: ☑ Now

Alarm Id	Type	Status	Date	Time
[36596]	Intrusion	ESCALATED	17/0...	04:25...
[36595]	Intrusion	CONFIRMED	17/03/...	04:13:16
[36594]	Intrusion	ESCALATED	17/03/...	04:06:34

Number of Alarms: 3

Send Incident to Police Department
Send Incident to Fire Brigade
Send Incident to Health Care Department
SMS Notification in List 1
View Video Camera Test Camera

Title: "Access Denied"
Description: "Stream had 2 messages in the last 1 minutes with trigger condition more than 0 messages. (Current grace time: 0 minutes)"
Start Date: 17-03-2021 Time: 03:44:09
Modification Date: 17-03-2021 Time: 04:24:42
Detector: graylog
Impact:
Stage: RECEPTION
Incident ID: 89513651

Status: AWAITING CONFIRMATION / CONFIRMED / ESCALATED / CLOSED / CANCELED

Comment	User	Date	Time

404 Not Found

Nothing matches the given URI

```
Traceback (most recent call last):
```

Powered by CherryPy 18.6.0

Details

Title: "Access Denied"
Description: "Stream had 2 messages in the last 1 minutes with trigger condition more than 0 messages. (Current grace time: 0 minutes)"

Figure 2.3: Initial description of the Incident, computer generated

[1] Alerts and Incidents are defined according to the SATIE ontology (11)

- Operational – SOC

  i) SEA requested the possibility to change the status of an event in the Incident Management Portal (IMP), i.e.: if the event is transformed from Alert into Incident there might be the necessity to bring it back to Alert. ACS created the "Rollback to alert" procedure;

  ii) With respect to the analysis of the Alerts, SEA required a procedure to fix the parameters on the basis of which the Alert must be transformed into an Incident and must be escalated to CAS.
  DLR solved this issue with the creation of the "Alert-to-Incident decision making guidance table", available in the D7.2 "Training Handbook" (5);

  iii) In case of a network attack, SEA requested that the SOC operator should know the IP address of what the attack is targeting and where the attack comes from. ACS reconfigured the IMP to make the IP addresses visible.

Other Operational suggestions for the SOC were not realized due to budget restrictions, especially as to the modification of the Incident Management Portal main page graphical interface, but were noted by ACS, for possible future implementations:

- the SOC operator does not have to find everything (closed and open Incidents) in the same page;
- the SOC operator should know at first sight that the Incident was sent to the CAS;
- the SOC operator should have a record of the Incidents sent to the AOC operator.

2.2 Milan Malpensa demonstration overview

Demonstration set-up operations in Milan Malpensa were organized and coordinated by SEA, with the active involvement and technical support of all the partners, some of whom were physically present at the Malpensa premises to install some fundamental tools (Figure 2.4).

Figure 2.4: Installation of the Unified Access Control at the AOCC door at the Milan Malpensa Airport premises

SEA, in collaboration with the Project Coordinator and other SATIE Partners, announced the Milan Malpensa demonstration event to a considerable number of end-users (i.e. airport operators, stakeholders and individual experts) and motivated them to participate in the demonstration process of the SATIE Solution and its incorporated components, including the following:

- sending personal and public invitations (via personal e-mails);
- promoting the demonstration event to aviation communities and critical infrastructure protection networks;
- inviting airport and security stakeholders based on contact information that had been collected by networking in conferences and workshop events;
- engaging partners and stakeholders to communicate with their contact points, motivating potential end-users.

As a result of the dissemination efforts, seventy-one (71) people were attending the demonstration in total. The demonstration event took place in Malpensa's Crisis Room (Figure 2.5) and was attended by eleven (11) physically-present external participants and sixty (60) online participants in total, out of whom twenty-six (26) were externals. The external participants belonged to: Governmental Organizations, Regulatory Organizations, Research/Academic, Airline personnel, Airport personnel, Cyber Security Consultants and Transport Organizations. Due to the COVID-19 measures and travel restrictions, few people were allowed in the Crisis Room: most of the audience attended virtually, but SEA was lucky enough to have sufficient space to welcome 11 people to follow the event live. Thanks to the Project Coordinator, who managed the virtual conference, the audience following the demonstration remotely could take advantage of the online broadcasting and interactive process.

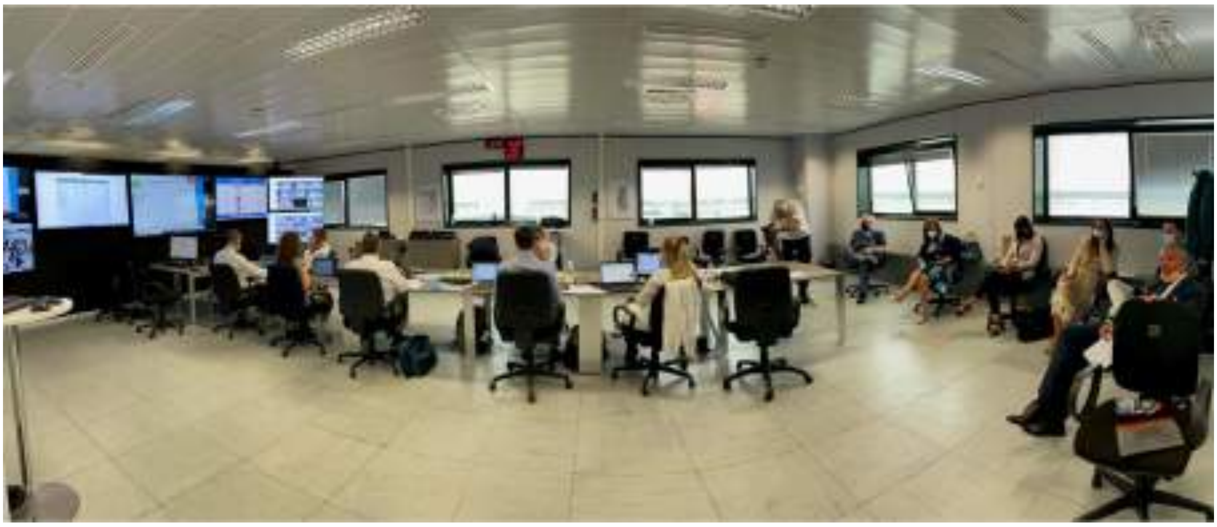


Figure 2.5: Milan Malpensa Airport demonstration event in the Crisis Room

For the purpose of the event, the SOC room was set up in the Crisis Room, while the AOC room was set up in the Airport Duty Manager backup room, to avoid compromising the AOCC operations running in parallel.

During the demonstration, the Security Operations Centre (SOC – Figure 2.6) and Airport Operations Centre (AOC – Figure 2.7) operators showed the performance of the SATIE Solution through the deployment of a realistic cyber and physical attack scenario - Scenario #3: Land side – air side and physical attack. The scenario consisted of three (3) sub-scenarios attacks, made realistic thanks to the simultaneous activities of a hacker, manipulating the RMS, the M-AIS and the FIDS to give origin to the cyber-attack (Figure 2.8) and of a terrorist trying to enter the AOCC room with a stolen badge, without the grants for the access.

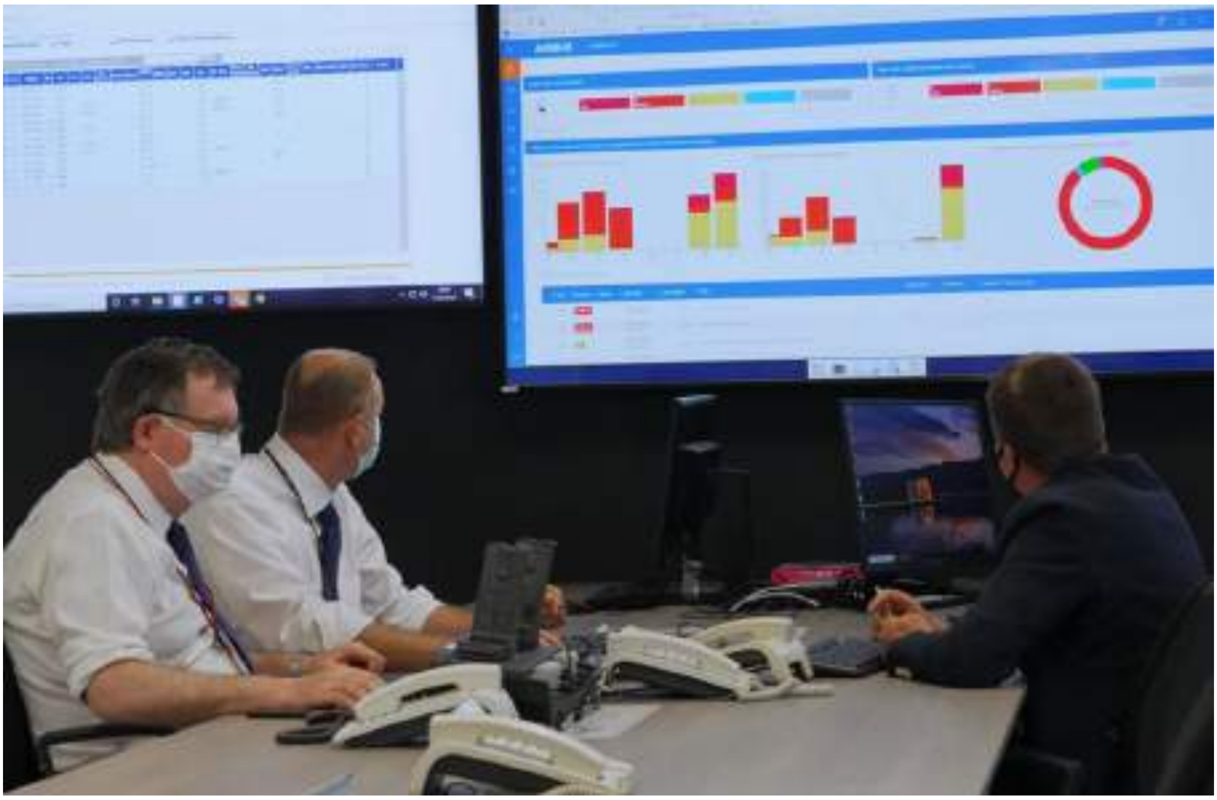


Figure 2.6: The Security Operations Centre (SOC) activities in the Crisis Room during the Milan Malpensa International Airport demonstration event

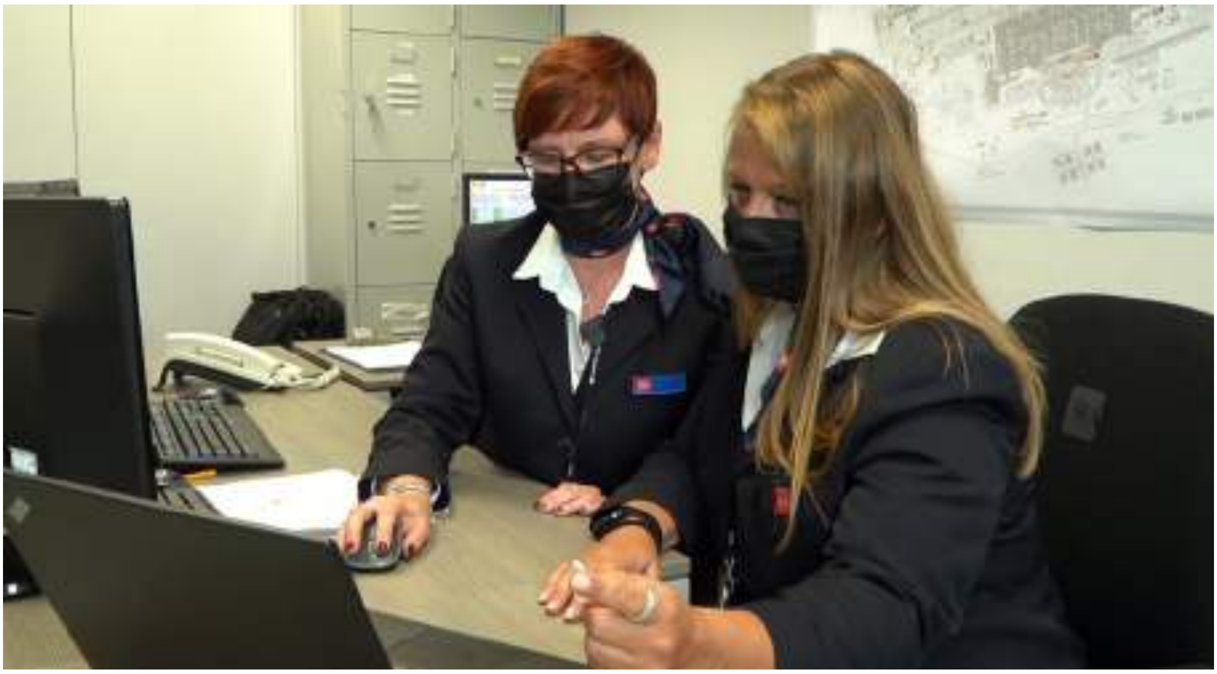


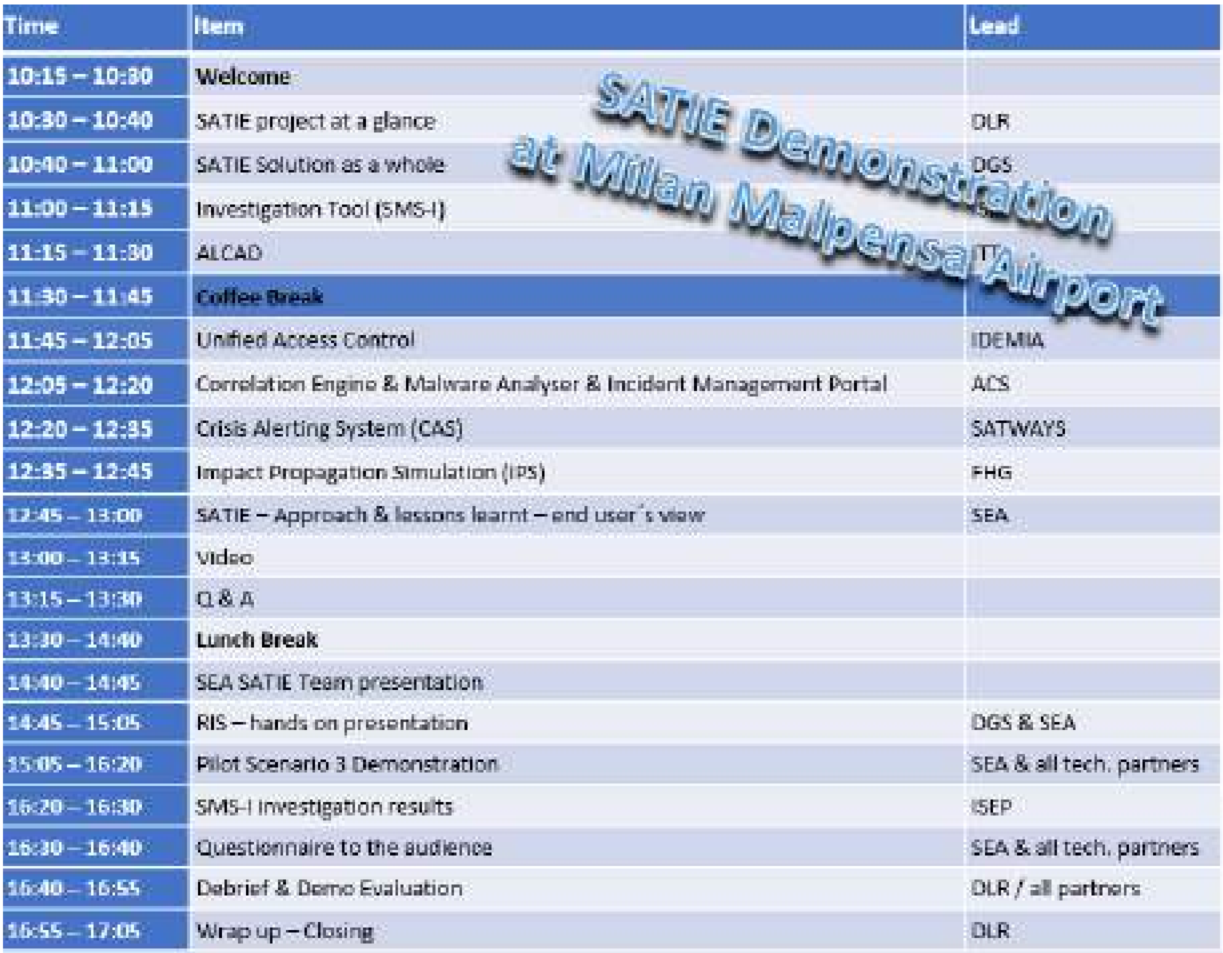
Figure 2.7: The Airport Operations Centre (AOC) activities in the Airport Duty Manager Backup Room during the Milan Malpensa International Airport demonstration event

Figure 2.8: The hacker in the dedicated room in Terminal 1 of Milan Malpensa International Airport, during the demonstration event

The SATIE Tools involved in the Milan Malpensa demonstration scenario included: Unified Access Control, Malware Analyser (MA), Application Layer Cyber Attack Detection (ALCAD), Impact Propagation Simulation (IPS), Correlation Engine, Incident Management Portal (IMP), Crisis Alerting System (CAS), Investigation Tool (SMS-I) and Risk Integrated Service (RIS). The last two were used to carry out an example of risk assessment before the start of the demonstration (RIS) and a multi-dimensional analysis over the cyber and physical Incidents reported during the demonstration by the SOC operators explaining how to read the results appearing on the dashboard (SMS-I), once the demonstration was finished.

The demonstration was structured with the clear idea of showing SATIE’s potential; thus, besides presenting the various tools and their functionalities, the scenario was designed with the purpose of testing the capacity of the SATIE Solution to reveal the threats in real time. The demonstration clearly showed the audience that SATIE is an example of holistic security, giving the assets and the people continuous protection across all attack surfaces: taking into consideration the totality of all physical, software, network and human exposure.

The SATIE demonstration at Milan Malpensa Airport was a full day event and lasted approximately seven hours. The agenda of the event is depicted in Figure 2.9.


SATIE Demonstration
at Milan Malpensa Airport

Time	Item	Lead
10:15 – 10:30	**Welcome**	
10:30 – 10:40	SATIE project at a glance	DLR
10:40 – 11:00	SATIE Solution as a whole	DGS
11:00 – 11:15	Investigation Tool (SMS-I)	[illegible]
11:15 – 11:30	ALCAD	ITT
11:30 – 11:45	**Coffee Break**	
11:45 – 12:05	Unified Access Control	IDEMIA
12:05 – 12:20	Correlation Engine & Malware Analyser & Incident Management Portal	ACS
12:20 – 12:35	Crisis Alerting System (CAS)	SATWAYS
12:35 – 12:45	Impact Propagation Simulation (IPS)	FHG
12:45 – 13:00	SATIE – Approach & lessons learnt – end user´s view	SEA
13:00 – 13:15	Video	
13:15 – 13:30	Q & A	
13:30 – 14:40	**Lunch Break**	
14:40 – 14:45	SEA SATIE Team presentation	
14:45 – 15:05	RIS – hands on presentation	DGS & SEA
15:05 – 16:20	Pilot Scenario 3 Demonstration	SEA & all tech. partners
16:20 – 16:30	SMS-I investigation results	ISEP
16:30 – 16:40	Questionnaire to the audience	SEA & all tech. partners
16:40 – 16:55	Debrief & Demo Evaluation	DLR / all partners
16:55 – 17:05	Wrap up – Closing	DLR

Figure 2.9: Agenda of the SATIE demonstration event at the Milan Malpensa International Airport

At the beginning of the demonstration event, SATIE project's idea was introduced, and the SATIE Solution as a whole was presented. Subsequently, SATIE project's technical partners gave overall presentations of the different SATIE Tools involved in the Milan Malpensa's demonstration scenario (see chapter 3), namely: Investigation Tool (SMS-I), ALCAD, Unified Access Control (UAC), Correlation Engine, Malware Analyser, Incident Management Portal (IMP), Crisis Alerting System (CAS), Impact Propagation Simulation (IPS). SEA presented the end user's point of view.

After the Scenario #3 video, SEA's personnel belonging to the SATIE Team was presented. The demonstration was preceded by a joint, SEA-DGS hands-on session to showcase the RIS and was followed by an analysis of the incidents reported during the demonstration using the SMS-I tool by ISEP.

The Milan Malpensa demonstration also included a Questions and Answers (Q&As) session, followed by a debrief and pilot evaluation session. During the Q&As session an online evaluation questionnaire was distributed to the audience for their feedback. To obtain exclusively unbiased opinions, only the participants external to the project (so called "independent external") were asked to answer the evaluation questionnaire. The SATIE Solution was considered a significant improvement compared to current security-monitoring systems, was rated as innovative and an excellent way to monitor and raise security alerts with good usability. It was agreed that the SATIE Solution provides all relevant information and enables faster detection of both cyber and physical threats. The biggest area for improvement expressed by all expert groups was the integration of the SATIE tools with the current airport systems.

Also, the feedback on the SATIE Tools contains adjectives such as: "fascinating", "robust" and "excellent" (this last one in more than one opinion!). One feedback was an explicit question on the commercialization of the tools within the next six months.

For the needs of the scenario’s deployment, the physical and cyber infrastructure of the Milan Malpensa International Airport was engaged, as further analysed in this deliverable within section 2.3.1 and section 2.3.2 respectively.

Figure 2.10 shows some preparatory work for the Milan Malpensa demonstration.

Figure 2.10: SEA and ACS works in preparation of the demonstration

2.3 Milan Malpensa cyber and physical infrastructure and systems integration with the SATIE Solution

The current section presents the cyber and physical infrastructure set up which was used for the SATIE Milan Malpensa demonstration.

2.3.1 Localisation and logistics

As described in section 2.2, the SATIE Milan Malpensa International Airport demonstration event was held at SEA premises in Italy on the 8th September 2021. For the demonstration live performance, the Crisis Room, the Airport Duty Manager Backup Room, a meeting “hacker” room and the Airport Operations Control Centre at Terminal 1 of the Milan Malpensa Airport were used (Figure 2.11 and Figure 2.12).

The Milan Malpensa Airport sites and equipment used to run the demonstration event were the following:

- **Terminal 1** of the Milan Malpensa International Airport was used for the performance of the combined physical and web demonstration event. Some of the rooms used, mentioned here below, are at different levels of Terminal 1;
- **The Security Operations Centre (SOC Room)** was set up in the **Crisis Room** of the airport, for the purpose of having at least a small live audience during the demonstration event. Here, three working positions for SEA's SATIE SOC operators were set up, together with a big monitor displaying the SATIE functionalities and graphical user interfaces. The other monitors displayed:
    - M-AIS – Milan Airport Information System;
    - RMS – Resource Management System;
    - FIDS – Flights Information Display System;
    - Live streaming from cameras in the Terminal, and on the Apron;
    - The ongoing demonstration Webex for the audience in the room.

  Thanks to the availability of space, the Crisis Room allowed for 11 people to attend as external audience.
- The **Airport Operations Centre** (**AOC) room** was set up in the Airport Duty Manager Backup Room of the Milan Malpensa Airport for the demonstration operations, allocating two working positions for the AOC operators trained users, giving access to the Crisis Alerting System (CAS) end users' environment of the SATIE Solution;
- The **Hacker working position** was set up in a meeting room at Terminal 1 of the Milan Malpensa Airport. All hacker's activities were performed in the specific area of the M-AIS and RMS "shadow systems" created for the SATIE Project (as explained in section 2.3.2) and were shown in real time: after a few seconds the Incident Management Portal recognized the unauthorized activities and raised alarms;
- An AOCC "**SATIE" Windows 10 workstation** was positioned inside the AOCC Room (see section 2.3.2.3);
- The **Unified Access Control** was positioned at the door outside the AOCC Room and connected to SEA's systems. The Unified Access Control – Control Unit was positioned in a cabinet inside the AOCC Room;
- **Networking and audio-visual equipment,** technical expertise support for the real-time video transmission to run the demonstration operations and perform the virtual event at Terminal 1 of the Milan Malpensa Airport.

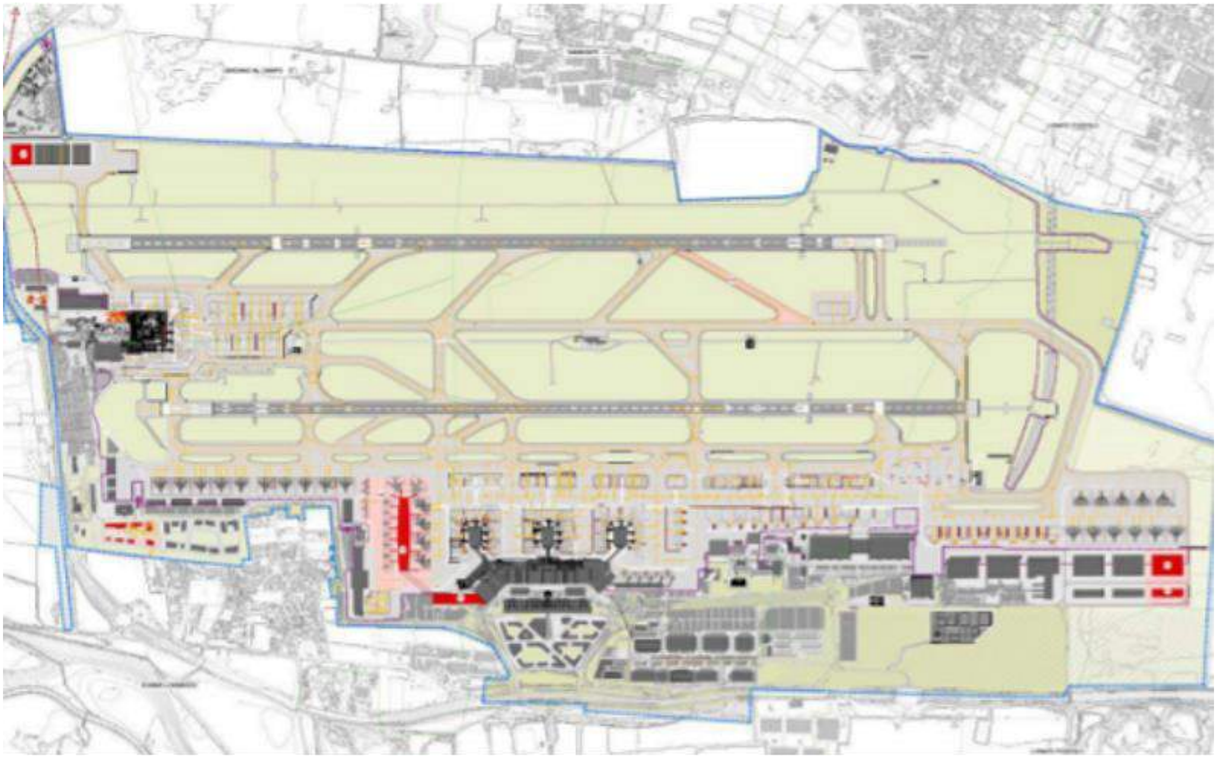


Figure 2.11: Milan Malpensa International Airport map

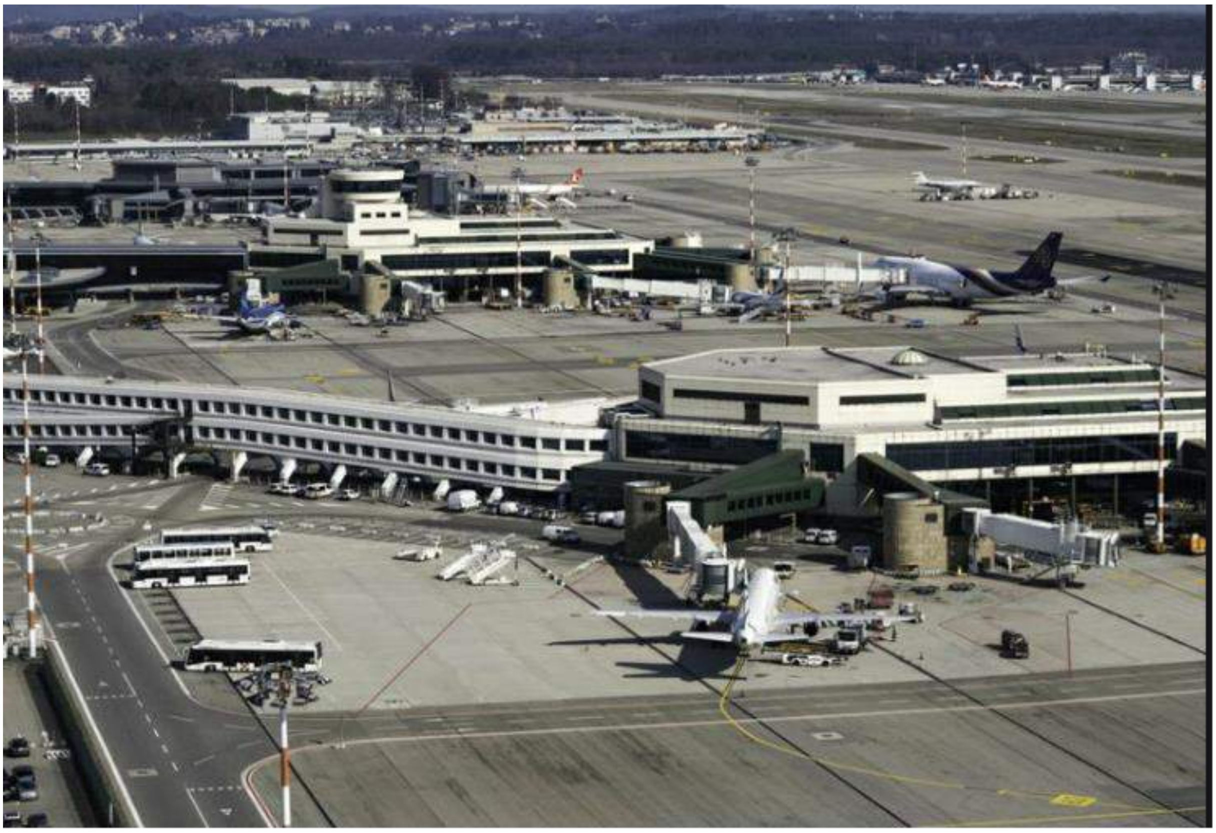


Figure 2.12: Milan Malpensa International Airport - Terminal 1 Apron

2.3.2 Cyber and physical infrastructure integration for the Milan Malpensa International Airport demonstration

The Milan Airport demonstration was devised in such a way as to involve both cyber and physical infrastructures in a coordinated operation. This structure made it possible to show the full range of capabilities of the SATIE Solution in response to attacks.

The structure included airport servers and workstations, connected to the airport network. A VPN connection allowed them to be reached from the main SATIE data centre.

2.3.2.1 Steps towards integration

Starting from the middle of January 2020, until the end of April 2020, SEA and ACS set up a series of "Clear the Sky" meetings during which, in parallel:

- the threats in Scenario #3 initially defined in the Grant Agreement were investigated in deep and fully re-assessed and revised according to their need of being simulated in a real scenario context, therefore identifying how to detect the cyber and physical threats;
- SEA networks and systems capabilities with reference to the needs of Scenario #3 were assessed;
- the perimeter of the architecture of the "SEA test system" was defined (Figure 2.15);
- the SEA systems to be included in the perimeter of the architecture of the "SEA test system" were defined;
- the cyber-attack steps (Figure 2.13) were defined;
- the physical attack steps were decided.

The "Clear the Sky" meetings with ACS were followed by SEA's internal update meetings, to check the progresses and update ACS accordingly.

As to the perimeter of the architecture of the "SEA test system", it was decided to keep the infrastructure at SEA premises, as shown in Figure 2.15, within section 2.3.2.2. The cyber-attack steps were defined accordingly (Figure 2.13):

- Step 1 – point of attack – Internet. Social engineering allows to identify possible point of attack within the AOCC;
- Step 2 – a spear phishing e-mail is sent to the e-mail address of an AOCC operator. The attachment containing the malware is opened and the virus spreads so that the hacker takes control of the workstation from which M-AIS and RMS are accessible;
- Step 3 – the malware performs a network scan to find an attack path to the M-AIS and RMS servers;
- Step 4 – through a brute-force attack against the RMS and M-AIS servers, the credentials for M-AIS and RMS are discovered;
- Step 5 – the hacker accesses the M-AIS web application and the RMS application with admin privileges, in order to alter data in both systems.

As a consequence of the "Clear the Sky" meetings, a "Letter of Understanding regarding SATIE activities" was finalized between SEA and ACS in May 2020 (Figure 2.14). Thanks to this Letter, the parties specified more in details the terms of their collaboration, including specific limitations for ACS regarding the accessible perimeter of the "SEA test system" and the waiver to use intrusive instruments such as injection and Bruteforce attacks.

ACS also has agreed to avoid those techniques whose primary purpose is to:

- permanently degrade the performance of the system or network (both local and distributed Denial of service);
- create permanent alterations or destruction of data;
- insert potentially harmful code permanently in the applications, in the network equipment and in the operating systems belonging to the "SEA test system";

- expose applications, the network and servers to attacks by external and unrelated subjects within the scope of the analysis (e.g.: backdoor, trojan horse, rootkit).

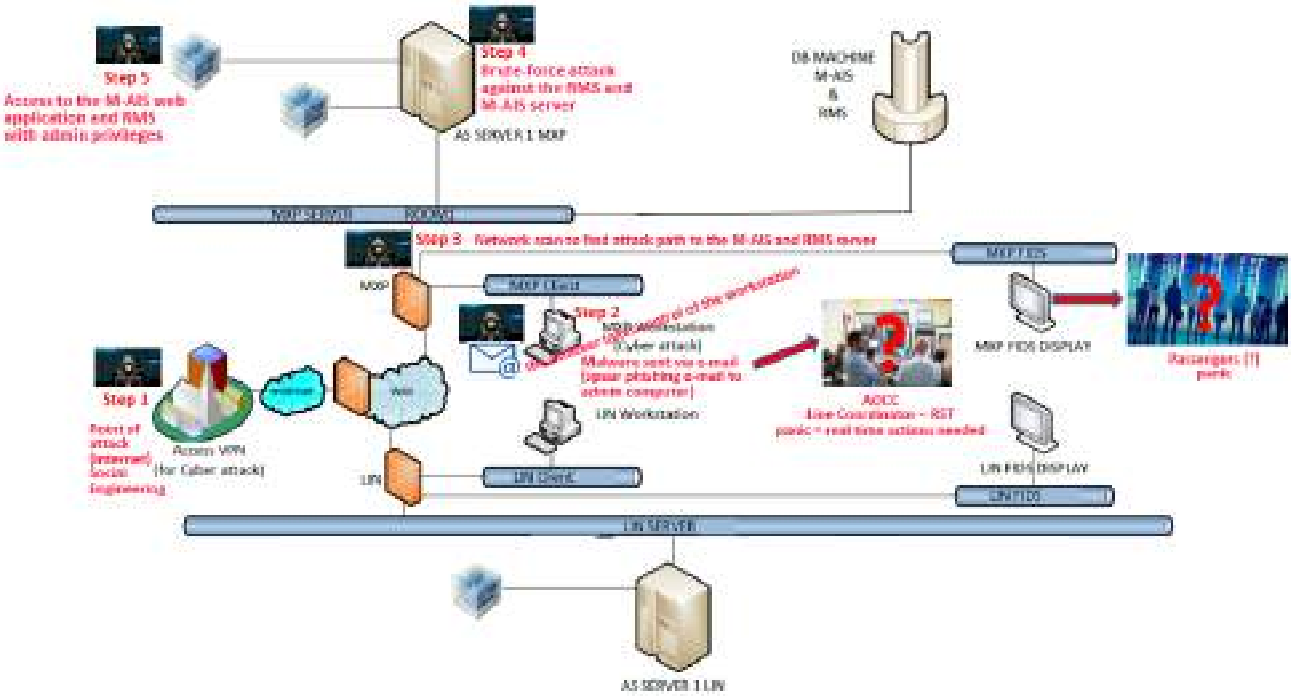
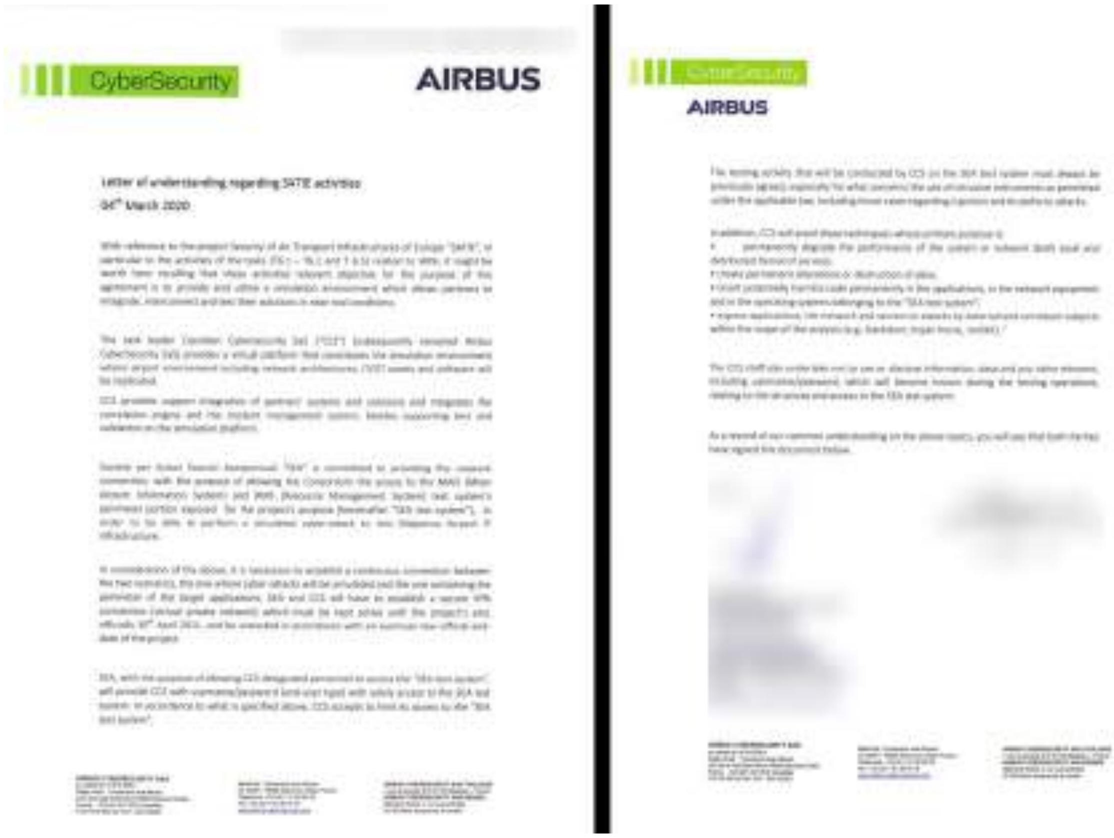

Step 5
Access to the M-AIS web application and RMS with admin privileges
Step 4
Brute-force attack against the RMS and M-AIS server
AS SERVER 1 MXP
DB MACHINE
M-AIS
&
RMS
MXP SERVER
ROOM1
Step 3 Network scan to find attack path to the M-AIS and RMS server
MXP FIDS
MXP
MXP Client
Step 2
MXP Workstation
(Cyber attack)
Malware sent via e-mail (spear phishing e-mail to admin computer)
MXP FIDS DISPLAY
Passengers (!) panic
Step 1
Point of attack (internet) Social Engineering
Access VPN
(for Cyber attack)
Internet
WAN
AOCC
Line Coordinator – RST
panic = real time actions needed
LIN Workstation
LIN FIDS DISPLAY
LIN
LIN Client
LIN FIDS
LIN SERVER
AS SERVER 1 LIN

Figure 2.13: Cyber-attack steps



CyberSecurity AIRBUS

Letter of understanding regarding SATIE activities

04th March 2020

[illegible]

CyberSecurity

AIRBUS

[illegible]

Figure 2.14: "Letter of Understanding regarding SATIE activities"

2.3.2.2 Airport operational servers

The main airport systems involved were:

- **M-AIS**, the Airport Operations Database (AODB), which receives, stores, and dispatches all airport operational data and thus is the central core of all airport IT systems;
- **RMS**, the Resource Management System, which allocates both human and physical resources for ground operations and transmits all related info to M-AIS;
- **FIDS**, the Flight Information Display System, which handles all the passenger information displays in order to show the flight data received from M-AIS;
- The **Access Control System**, which ensures that only authorized staff can access the restricted areas of the airport.

All these systems can be accessed from the AOCC, the Airport Operations Control Centre, which was the “hub” around which the demonstration took place. But, for obvious security reasons, SEA could not accept to involve the actual, active servers of its production environment in the demonstration.

Therefore, it was decided to create a “shadow” environment (Figure 2.15) containing active replicas of all the main servers, except the Access Control System. The main issue for this activity was the need for these replicated systems to receive the same input data as the production ones, so that their databases contained real, dynamic data that could be used in the demonstration. The main data flows of the production servers were duplicated so that they could “feed” the databases of the shadow systems in the moment when they were being used.

In order to allow the SATIE Tools to analyse the behaviour of the M-AIS and RMS applications it was necessary to create dedicated views within their database. In fact, the applications are designed in such a way as to store their logging information (including all operator activities) in an Oracle database.

SEA created special Oracle accounts for the SATIE applications and granted them the privileges to access the views and retrieve the application logging data in real time. SEA supplied ACS with the connection strings for the Oracle Database and with sample instructions for application data retrieval. SEA gave assistance to ACS in the installation, configuration and set-up of the database client application which was installed on the Suricata workstation (see section 2.3.2.3). Several test sessions were held which allowed to determine the correct set-up for the client tools.

A test environment was created for the FIDS which included dedicated monitors of the same type as those used in the passenger terminal to display flight data to passengers for arrivals and departures. The software-emulated departures monitor was displayed in one of the screens in the SOC room during the land side attack.

Another issue was the need to limit the access of the demonstration workstations to the server network so as they could only reach the applications that they needed to use for the demo. It was decided to create a new, dedicated Virtual Local Area Network (VLAN) for the workstations, connected to the shadow server VLAN via a firewall. All connections from the workstations to the servers had to undergo Network Address Translation (NAT) in such a way as the real IP addresses of the servers would never be visible within the workstation VLAN.

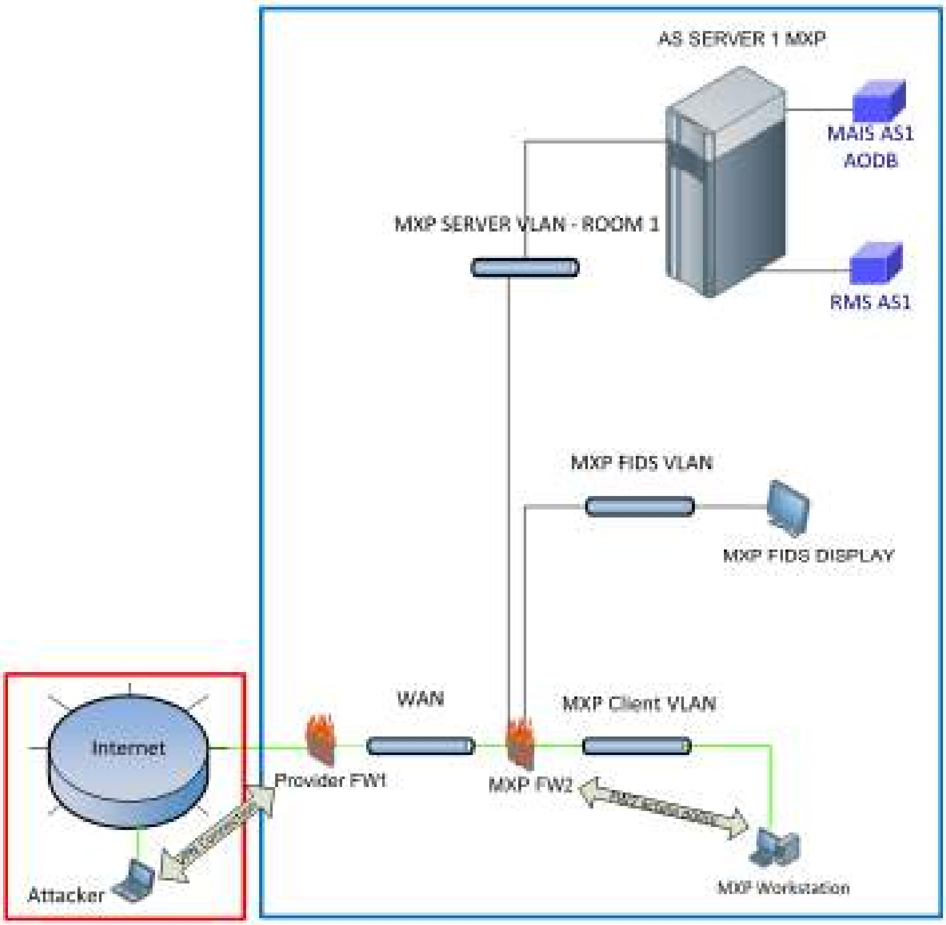


Figure 2.15: Shadow environment for the Milan Malpensa demonstration

2.3.2.3 Workstations

SEA provided and configured two workstations for the demonstration environment:

- One workstation was a Windows 10 workstation, in fact a replica of the workstations currently used by the AOCC operators.

  All the applications were installed that the operators need to use the main airport systems. A user dedicated to SATIE was created. The user was given access to a mailbox in the SEA Office365 e-mail environment. The mailbox would be used to receive the spear-phishing message in Scenario #3.

  The IP addresses for the M-AIS, RMS and FIDS servers had to be encoded in the “hosts” file of the workstation because the use of NAT made it impossible to use the airport Domain Name System (DNS) services.

  A software package was developed and installed on the workstation that simulates the real-time activity of an operator using both the M-AIS and RMS applications. Thanks to this simulator the SATIE Tools can analyse the network activity without the need for an operator to be always present.

  The workstation was equipped with an RDP (Remote Desktop Protocol) software that made it possible to operate it remotely through the VPN.

- The second workstation was a Linux workstation that was used to provide application and network traffic data to the SATIE Toolkit.

  SEA installed on this workstation an Ubuntu operating system with an SSH server that made it possible to operate it remotely through the VPN. ACS installed, on top of this, the Suricata component of SATIE, which extracts the data files from the network and sends them to the Malware Analyzer, and also sends network information to the Correlation Engine. A NetFlow collector was also installed to provide network data to ALCAD.

2.3.2.4 Networking

An IPsec VPN was established between the SEA network and the SATIE systems in Élancourt. It was designed, configured and tested in cooperation between SEA and ACS. A dedicated configuration was prepared on the SEA firewalls to enable access via the VPN to the workstations in Malpensa.

The VPN allowed to:

- Configure the workstations according to the needs of the SATIE software;
- Operate the workstations remotely;
- Receive data from the Suricata workstation;
- Simulate hacker attacks during the demonstration;
- Connect the UAC device with the SATIE systems.

The two workstations were connected to their dedicated network using an Ethernet switch.

As it was not possible to extract network traffic data directly from the switch, the initial plan was to have the switch "mirror" the network traffic of the Windows workstation and send it to the Suricata workstation for analysis. To this purpose, the Suricata workstation was equipped with an additional Ethernet port (Figure 2.16).

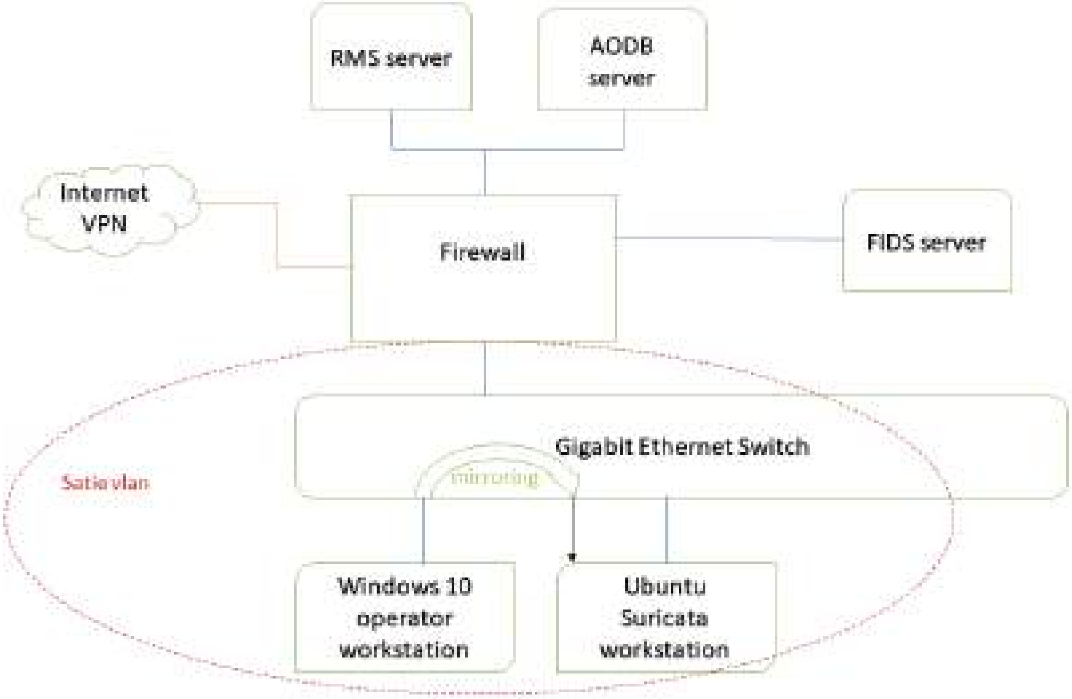


Figure 2.16: Network configuration with mirrored port

The first tests with the mirrored port showed the Suricata workstation did not receive the traffic data correctly. SEA examined the network configuration of the workstation and changed a few parameters in order to fix this issue. After this activity, several tests were successfully performed using network traffic analysers in order to certify that the network traffic was fully replicated. Yet the network packets received by the Suricata module appeared to be truncated, in such a way as to make it impossible to analyse them.

The final solution was to use a network “tap” to duplicate the network traffic. Instead of being connected to the switch for mirroring, the second Ethernet port of the Suricata workstation was connected to the tap (supplied by ACS) which was also connected to the Ethernet port of the Windows workstation.

The tap required two Ethernet connections to the Suricata workstation to operate correctly, but it was not possible to add yet another Ethernet card. So, an USB-to-Ethernet adapter was used instead (Figure 2.17).

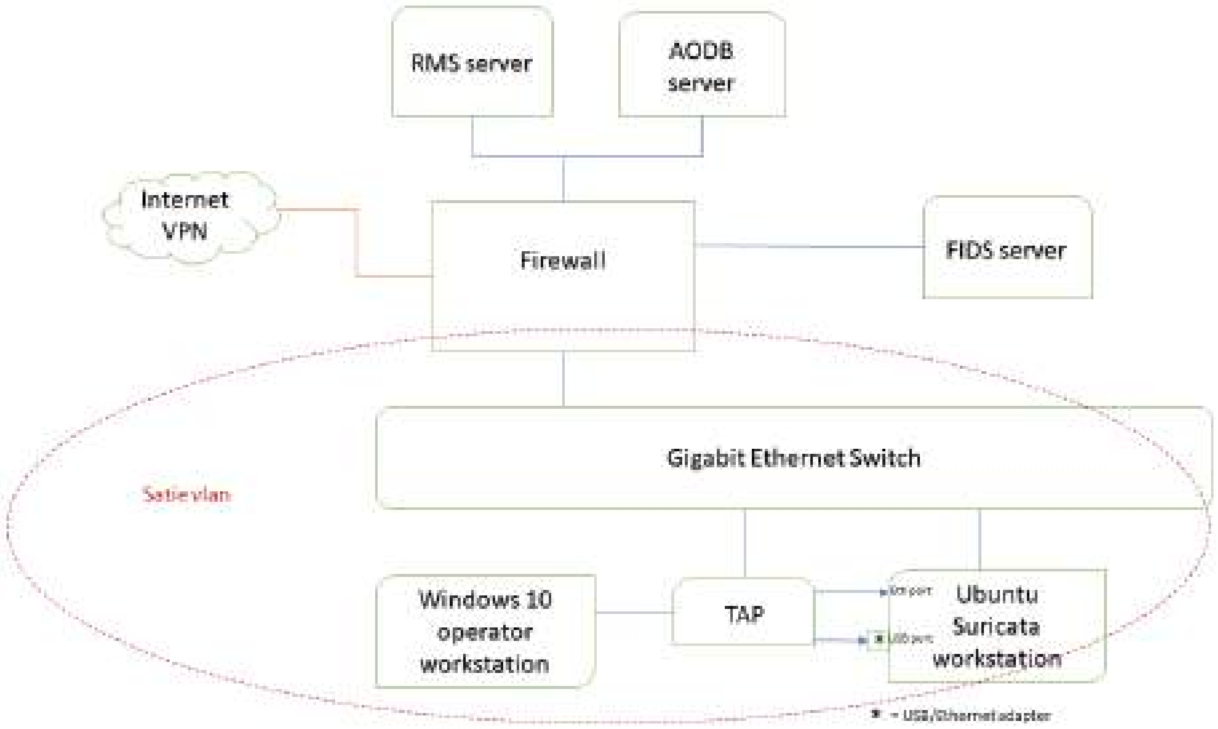


Figure 2.17: Final network configuration with network tap and USB-to-Ethernet adapter

2.3.2.5 Access control

The UAC solution components, including facial recognition software via IP camera and a fingerprint scanner, were connected to the equipment used to control the door of the AOCC room, which is handled by the airport’s Access Control System.

The Airport WIFI network was used to connect the internal switch of the UAC solution with the UAC PC, which was also configured to be reachable from the IPsec VPN.

2.4 Operations during the Milan Malpensa demonstration event

A set of coordinated activities took place, live, during the Milan Malpensa demonstration event. These activities were undertaken by SEA and the SATIE technical partners that actively participated in the event, both on-site and remotely. The demonstration event was performed live, in real-time, by one hacker, three SOC operators and two AOC operators, all volunteers from SEA’s ICT and Operations Departments, already trained through the SATIE training workshops and through the “self-training” sessions as mentioned in section 2.1.

At the beginning of the demonstration, the AOCC Room and the activities in it were introduced to the audience by one of the AOC operators. During the demonstration:

- The Technical Moderator (ACS) introduced to the audience the scenarios clearly explaining what was happening on the screen;
- The hacker started to manipulate the RMS and the M-AIS and explained the audience his actions on each of the systems, besides explaining how dangerous those actions might have been in real operations (also because there would eventually have been many more);
- The SOC operators interacted in real time with the tools in the SOC. They explained their actions in SATIE, besides explaining why they deemed a specific alarm had to be transformed into Incident to be sent to AOC;
- The AOC operators interacted in real time with the CAS and explained their actions, both on the screen and from an Operations point of view;
- IDEMIA demonstrated and explained the functionality of the Unified Access Control system live at the AOCC door for the purpose of Scenario #3;
- The SEA SATIE Project Manager intervened to explain more in details some aspects related to Safety and Security.

The workflow was disclosed step by step to have the audience understand very well what SATIE would be able to do in case of attack and the operators' reactions, and also to let them realize how quick the actions must be in case of a cyber-attack and a physical attack.

The Milan Malpensa demonstration event was set up as a live event, as said at the beginning of this section, and all the actions were performed in real-time from the various rooms specifically set up for the SATIE demonstration in Terminal 1: the SOC and AOC operators could manage real-time Alerts and Incidents through the IMP and the CAS respectively in real-time, while sharing their screens and explaining their actions to the audience.

Immediately after the attack, the SOC operators were notified with Alerts through the Incident Management Portal (IMP) and were able to further investigate them by using the SATIE Tools. In addition, they created Incident reports, and retrieved additional information for the Incidents through the relevant network graphs, the statistics and the impact propagation simulation results. As a consequence of their investigation, they wrote a clear analysis, translating into operational language what they had discovered in the various steps of the investigation before closing the Incidents and sending them to the AOC operators.

The AOC operators were monitoring the Crisis Alerting System (CAS), and used CAS to manage Incidents and implement the necessary standard operational procedures to mitigate their effect. The AOC operators could see the Incident details and video feeds of CCTV cameras, and were able to send email notifications to the First Responders e.g. Italian Police, Fire Brigade, First Aid, Security Office. Through the collaboration perspective, they were also able to exchange SMS's with the Police and other different airport entities. In short, the SOC operators had access to the following end-user interfaces of the relevant SATIE Tools engaged in the scenario:

- Incident Management Portal (IMP);
- Correlation Engine;
- Malware Analyser.

It is worth mentioning that the ALCAD was used in this scenario as a service (i.e. no dedicated UI), but the users had opportunity to verify and act on information coming from ALCAD e.g. through the Incident Management Portal.

The participating AOC operators had access to the Incident reports generated, the relevant network graphs, the statistics and the impact propagation simulation results, thus they were able to evaluate the Incidents and take appropriate actions to mitigate the attacks (e.g. communicate with other airport security personnel and First Responders).

In short, the AOC operators had access to the following end-user interfaces of the relevant SATIE Tools engaged in the scenario:

- Impact Propagation Simulation (IPS);
- Crisis Alerting System (CAS).

2.5 Demonstration scenarios

The objective of the attack scenarios' performances of the three airports involved in the project is to demonstrate the SATIE Solution towards a real airport environment under real conditions. The attacks were agreed among all partners and built based on historical information and needs expressed by airport as end-users in this project. The goal is to represent cyber-physical threats that can develop into attacks which are increasingly complex and difficult to predict. The scenarios developed aim to illustrate how SATIE can detect complex cyber and physical attacks and how its integrated components are capable of providing valuable results and give insights to the SOC and AOC operators to handle the situation of an ongoing attack effectively and mitigate the harm to airport security and people's safety.

Scenario #3 aims at testing the usefulness of SATIE in the course of a combined, simultaneous attack in land side and in air side, and in specific restricted, sensitive, area.

All threat scenarios used in the SATIE project were defined and finalized in deliverable D6.1 "Simulation Platform and Integrated SATIE solutions" (6) and in deliverable D6.2 "Test, validation and demonstration scenarios" (1) (the first two Confidential, therefore unavailable deliverables of WP6 to the public).

Scenario #3 was named "The cry for help" and initially consisted of two physical attacks and two cyber-attacks:

- "The Schengen gate": cyber-attack against the RMS – the land side attack;
- "The Aircraft stands": cyber-attack against the M-AIS – the air side attack;
- "The Intruder": physical attack against the access control – the physical attack;
- "The Blackout": physical attack against power and communication.

The fourth attack was not performed, because of the COVID-19 restrictions that also applied to SEA's personnel, and because of the economic crisis brought by the pandemic.

The simultaneity of these remaining three attacks, the cyber-attacks by the hacker and the physical attack by the terrorist, made the scenario particularly realistic. The objective of this attack scenario performance is to demonstrate the SATIE Solution towards a real airport environment under real conditions.

The story behind the Scenario #3 demonstration involves a terrorist planning an attack at the airport and hiring a hacker to carry out a cyber-attack to the airport systems heavily impacting Airport Operations both in land side and in air side. The terrorist will carry out the physical attack.

The prelude of the attack is a spear-phishing email sent to an admin computer in the AOCC room. Once an AOCC employee opens the email on an admin computer and clicks on the link, unknown to them, the malware is downloaded and executed. This malware allows the hacker to take remote control of the workstation. They can then perform a network scan to determine the network address and port of the M-AIS and RMS servers – their main targets. Then, through a brute force attack on the credentials, the hacker gains access to the M-AIS web application and the RMS application in order to alter data in both systems. At this point, following the instructions of the terrorist, they start manipulating information.

The attack scenario in land side, "The Schengen gate", starts with a cyber-attack on the RMS: the hacker changes the boarding gates of multiple Schengen flights to non-Schengen boarding gates, within a time range of two hours. The information is automatically displayed in the Flights Information Display System (FIDS) monitors in the Terminal. As a consequence, a huge number of passengers, with Schengen and non-Schengen destinations, will be assembled at the passport control. Since the personnel at the passport control check both the passport and the ticket, they would also quickly realise that Schengen passengers try to pass the non-Schengen checkpoint and temporarily block the crossings. The passengers would become panicked as it is very close to boarding time, and confusion would be generated.

The attack scenario in air side, the "Aircraft stands" starts with a cyber-attack on the M-AIS: the hacker manipulates the aircraft stands assignment, assigning two incoming flights to the same stand in a time - range of 15 minutes. As a result, because of aircraft rotation, departing flights will result leaving from the same stand, therefore a big confusion would be generated because all entities involved in the aircraft rotation for each of the flights assigned in that stand (catering – fuelling – passengers' bus – cleaning – loading/unloading) program their activities on that specific stand and, as a result, they would be double or triple. This would be particularly dangerous in low-visibility conditions.

The physical attack scenario, "The Intruder" starts with the terrorist stealing a badge from an unaware AOCC employee. As a result, he can access the lift to the AOCC and successfully reaches the door of the AOCC and attempts to enter the room. In all these three cases, SATIE proved useful and immediately raised the alarms.

A very good synthesis of this scenario is contained in the Scenario #3 video, that will be available (after the project's end) on the website of the project (7) and was also shown during the demonstration event.

The Figure 2.18 clearly shows the SATIE Tools used for the demonstration of Scenario #3 and during the video.

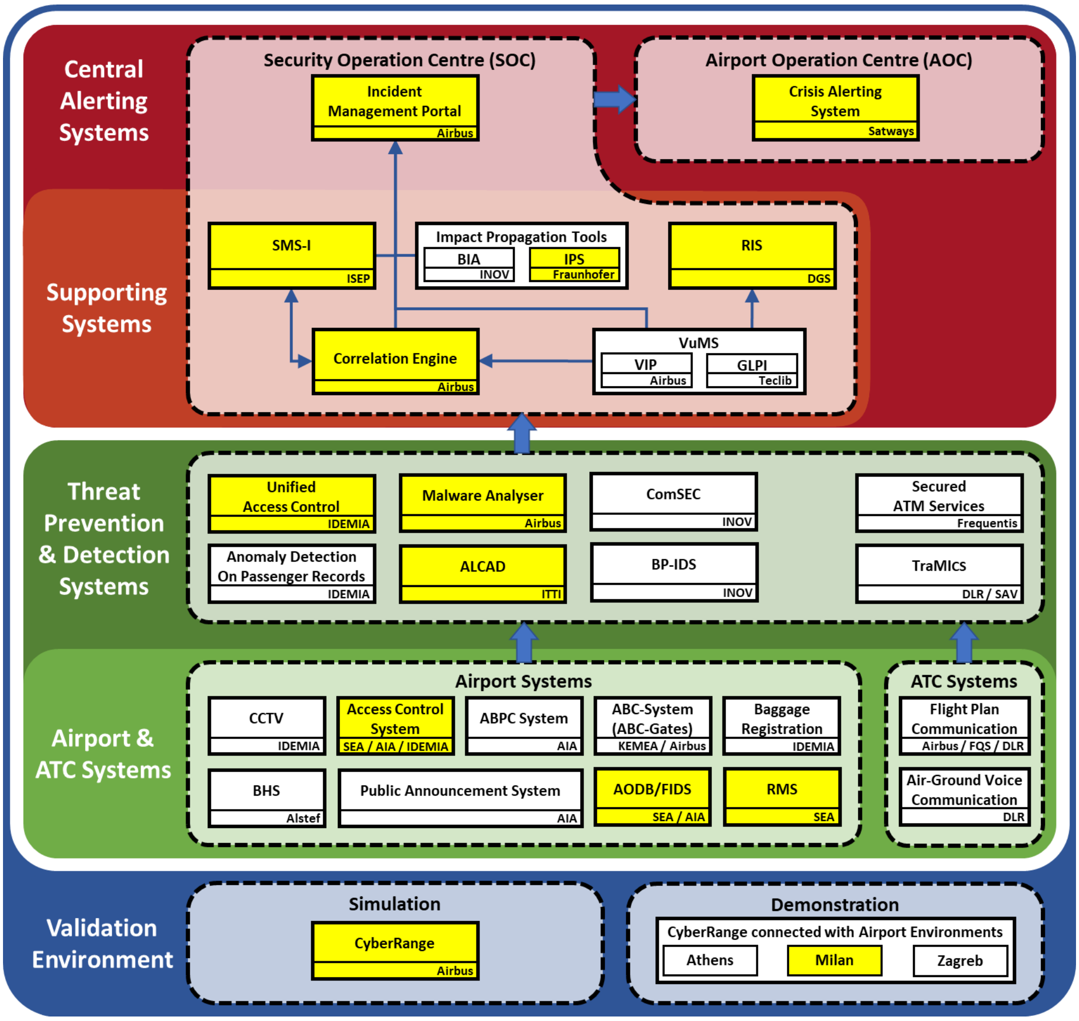


Figure 2.18: SATIE Tools used for the demonstration of Scenario #3

The roles considered in Scenario #3 are as follows:

- **Hacker:** SEA Airport Operations Applications Manager;
- **Terrorist:** IDEMIA Augmented Vision Product Manager;
- **Employee:** ACS R&T Engineer, acting as a SEA AOCC employee in the demonstration;
- **SOC operators:** SEA ICT Security Manager and SEA ICT Help Desk Specialists;
- **AOC operators**: SEA AOCC Deputy Manager and SEA Airport Duty Manager. The role of the AOC operators in Scenario#3 is covered by the Airport Duty Managers.

Table 2.1 contains, in details, the explanation of the demonstration steps and includes the Moderator's, the hacker's and the operators' useful interventions to explain the various steps.

The demonstration began with a live feed overview of the AOCC room, where the AOC operators explained the working positions in the room, including the one where the Airport Duty Manager normally operates. They also explained that, in order to avoid interfering with the daily operation, they would use the Airport Duty Manager back-up office for the Demo. The explanation on how the "Tools Involved" are used during the demonstration is contained in chapter 3.

Table 2.1: Scenario #3 "Land side – air side and physical attack" demonstration steps explained

Scenario Part	Scenario Step	Involved Tools	Moderator	Demonstration Set-Up
Landside and airside attack	Attacker launches spear phishing attack	No SATIE Tools		A spear phishing email is sent to the AOCC employees, who then become the initial targets. One of the employees falls into the trap and opens the attachment.
	Malware is down-loaded and starts running	No SATIE Tools		Upon the opening of the attachment, the malware is automatically downloaded from the email and it starts running. It infects the AOCC employee's machine.
	Malware is initially detected	Incident Management Portal (section 3.3) Malware Analyser (section 3.2) Correlation Engine (section 3.1)	The Moderator introduces the alarm that is visualized in the Incident Management Portal. The Moderator explains the possibilities of the tools.	When the malware infects the machine, the Malware Analyser detects the threat and sends a "*High risk file detected*" message to the Correlation Engine, which further processes the information and sends two Alerts to the Incident Management Portal. SOC operators start the analysis and explain they need to open the Correlation Engine (Graylog) to investigate the origin of the Alarm, then they open

Scenario Part	Scenario Step	Involved Tools	Moderator	Demonstration Set-Up
				ORION (the Malware Analyzer).
	Malware spreads across the network	Application Layer Cyber Attack Detection (section 3.4) Incident Management Portal (section 3.3)	The Moderator explains the possibilities of the Application Layer Cyber Attack Detection tool.	Malware performs a port scan attack to find RMS and M-AIS servers. The port scan attack is detected by the ALCAD and one “*ALCAD detect Port Scanning*“ Alert is raised to the IMP. SOC operators start the analysis and explain they need to open the Correlation Engine (Graylog) to investigate the origin of the Alarm. SOC operators explain they send the aggregated alarm (Malware analyser + ALCAD) to AOC operators. They also prepare and send, through the Incident Management portal, an analysis explaining that they might block an infected PC in the AOCC. SOC operators also send a message to the Network Manager
			The Moderator says that for demonstration purposes the hacker is allowed to go on and explains that Malware needs weeks to take possession of the workstation. A few technical explanations are also given.	The AOC operators explain that the alarm does not impact the operations directly. Anyway, they have found the infected PC and the person assigned to that pc has been moved to another workstation.
Land side attack	A) Modification of the boarding gates	Correlation Engine (section 3.1) Incident Management	The Moderator introduces the Hacker who explains the links between RMS, the system to assign the gates (and other resources), and FIDS the	The Hacker modifies the passenger boarding gates. Schengen flights are now boarding from non-Schengen gates.

Scenario Part	Scenario Step	Involved Tools	Moderator	Demonstration Set-Up
		Portal (section 3.3)	information system for passengers in the Terminal.	The strange boarding gates changes are raising "*Wrong gate changes*" Alerts in the Correlation Engine which are then sent to the Incident Management Portal. SOC operators start the analysis and explain they need to open the Correlation Engine (Graylog) to investigate the origin of the Alerts.
	A) Escalates Incident to CAS	Incident Management Portal (section 3.3) Crisis Alerting System (section 3.6)	The Moderator explains that boarding gates changes could have been more if this had been a real cyber-attack.	The SOC operators explain they realize the magnitude of the situation and therefore decide to aggregate all the Alerts in the IMP and write the result of the analysis. They send the Incident and the analysis to the CAS.
	A) AOC operators take corrective actions through CAS	Crisis Alerting System (section 3.6) Impact Propagation Simulation (Section 3.7)	The Moderator explains that SATIE is the channel through which the ICT world communicates with Operations.	When AOC operators receive the Incident through CAS, they decide to check the CCTV cameras, visualise the Impact Propagation Simulation and the Agent Based Model and alert the authorities about the incident. The communication was established through CAS, both via automatic messages sent to some members of a list, and via SMS's sent in real time through the "Collaboration" page. The AOC operators also explain that they call Line Manager requiring to switch off the FIDS and send Terminal operators to manage the passenger flow. They also explain that a feedback is needed from

Scenario Part	Scenario Step	Involved Tools	Moderator	Demonstration Set-Up
				Terminal operators confirming the situation is under control. The AOC operators agree to close the Alarm.
Air side attack	B) Modifications of the aircraft stands	Correlation Engine (section 3.1) Incident Management Portal (section 3.3)	The Hacker explains that M-AIS is the database providing information to all airport stakeholders. The Hacker explains that a stand change implies a series of actions related to the aircraft rotation because of which all entities involved in the transit operations (catering – fuelling – passenger bus – cleaning – loading/ unloading) program their activities on that specific stand. The most dangerous thing is an "Apron jam" in case of low visibility conditions.	The Hacker changes data in the M-AIS system which is used to assign aircraft stands. This raises "Double stand assignments" Alerts in the Incident Management Portal from the Correlation Engine. SOC operators start the analysis and explain they need to open the Correlation Engine (Graylog) to investigate the origin of the Alerts to try to understand what is happening.
	B) Escalates Incident to CAS	Incident Management Portal (section 3.3) Crisis Alerting System (section 3.6)	The Moderator explains that stand changes could have been more if this had been a real cyber-attack.	The SOC operators explain they realize the magnitude of the situation and therefore decide to aggregate all the Alerts in the Incident Management Portal and write the results of the analysis. They send the Incident and the analysis to CAS.
	B) AOC operators take corrective actions through CAS	Crisis Alerting System (section 3.6) Impact Propagation Simulation (section 3.7)		Once the second Incident from the SOC operators is received, the AOC operators explain what they do on CAS and alert the authorities about the Incident. The communication was established through CAS, both via automatic

Scenario Part	Scenario Step	Involved Tools	Moderator	Demonstration Set-Up
				messages sent to some members of a list, and via SMS's sent in real time through the "Collaboration" page. The AOC operators explain the procedures applied such as: - Requesting the Control Tower to stop the traffic on the Apron; - Send fire fighters; - Find free aircraft stands; - Send "Follow me" vehicles. They also explain that a feedback is needed to confirm that the circulation on the Apron can be restarted and, from the SOC operators, to confirm that the anomaly in M-AIS does not exist anymore. The AOC operators agree to close the Alarm.
Physical attack	AOCC employee badge is stolen	No SATIE Tools	The Moderator says that the physical attack is feasible because of a stolen badge The Project Coordinator plays the video share (min. 12:40 -13:08)	Employee badge ends up in the attacker's hands and grants access to the staff elevator which leads to the AOCC room.
	Attacker tries to enter the AOCC room with the stolen badge	Unified Access Control (section 3.5)		The attacker tries to enter the AOCC room by swiping the stolen badge over the access control machine. At the same time, the facial recognition software installed at the entrance of the AOCC room scans the face of the attacker.
	SOC operators are alerted about a physical attack	Unified Access Control (section 3.5)		When the mismatch between the face of the attacker and the badge is found, the UAC sends a *"Threat detected to the AOC*

Scenario Part	Scenario Step	Involved Tools	Moderator	Demonstration Set-Up
		Correlation Engine (section 3.1) Incident Management Portal (section 3.3)		*Room entrance*” message to the Correlation Engine, which raises an Alert in the IMP to alert the SOC operators. The SOC operators send the Incident and the analysis to CAS. The SOC operators explain they realize that, as this situation appears to be very dangerous, they should do a quick investigation, and, without wasting time, decide to immediately write a brief analysis and escalate this Incident to the CAS.
	AOC operators are alerted and called for security patrol	Crisis Alerting System (section 3.6)		AOC operators receive the Alert in CAS. They explain that, as they are responsible for all the people in the AOCC Room they alert both Police and the Airport Security Guards that a possible physical breach in the AOCC room is ongoing. The attacker is restrained by the security agents soon after. The AOC operators agree to close the Alarm.

3 SATIE response

This chapter presents how the SATIE Solution and the accompanying components have been used to detect the cyber and physical threats of the attack scenarios described in section 2.5. The response of each individual tool is shown, from the detection to the analysis, the response and the mitigation. It also explains how they interact to form the SATIE Solutions that helps to respond to the threat in a minimum of time.

3.1 Correlation Engine

The Correlation Engine was used in Scenario #3; it received events from the physical and cyber, SATIE threat detection systems. The main detection systems are ALCAD and Malware Analyser for the cyber part, and UAC for the physical part. They receive also events directly from the airport systems (Figure 3.1).

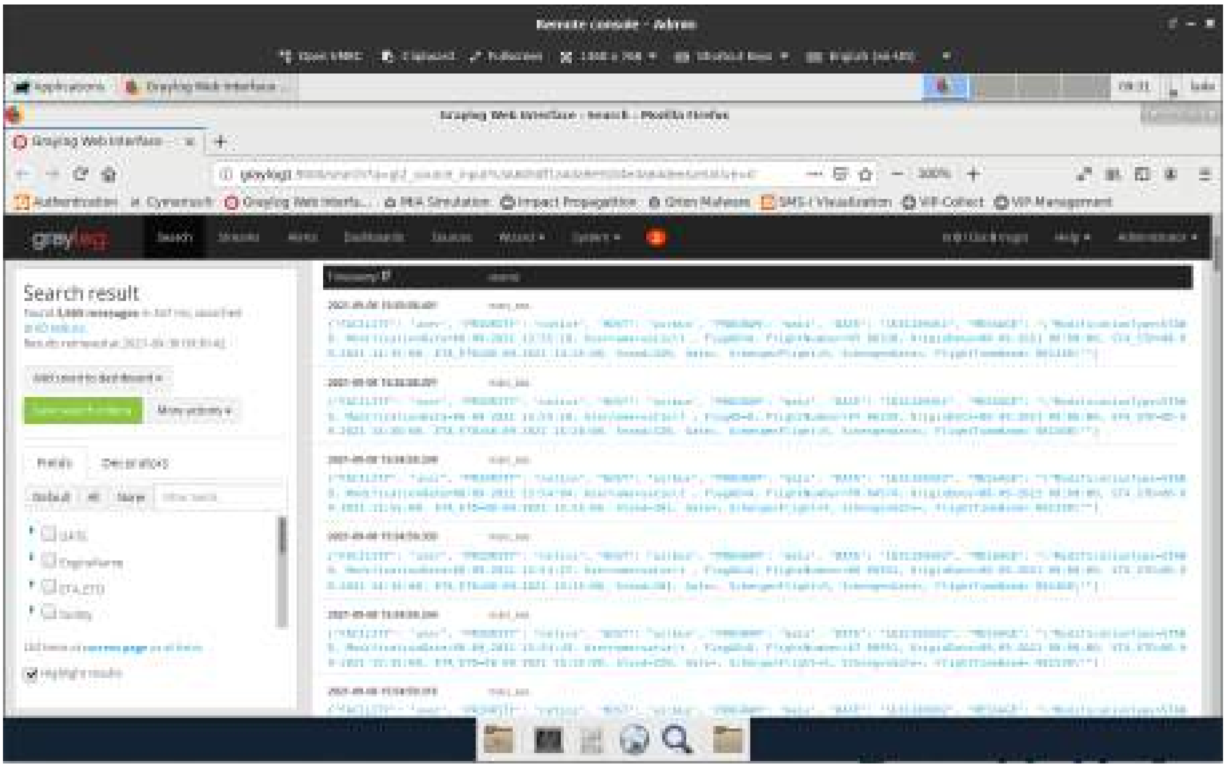
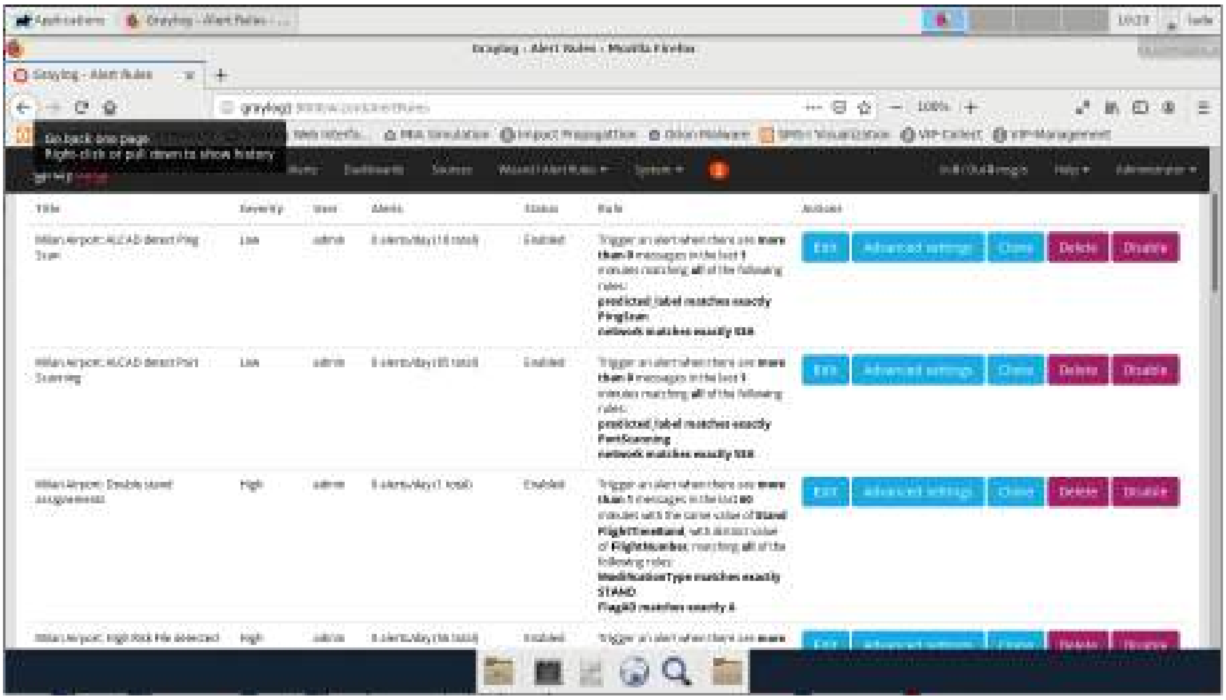


Figure 3.1: Correlation Engine showing events

With different rules defined, Alerts were raised to the Incident Management Portal. Figure 3.2 shows examples of rules. Table 3.1 shows the Alerts raised during the scenario.



Title	Severity	User	Alerts	Status	Rule	Actions
Milan Airport: ALCAD detect Ping Scan	Low	admin	0 alerts/day (18 total)	Enabled	Trigger an alert when there are **more than 0** messages in the last **1** minutes matching **all** of the following rules: **predicted_label matches exactly PingScan** **network matches exactly 168**	Edit Advanced settings Clone Delete Disable
Milan Airport: ALCAD detect Port Scanning	Low	admin	0 alerts/day (85 total)	Enabled	Trigger an alert when there are **more than 0** messages in the last **1** minutes matching **all** of the following rules: **predicted_label matches exactly PortScanning** **network matches exactly 168**	Edit Advanced settings Clone Delete Disable
Milan Airport: Double stand assignments	High	admin	0 alerts/day (1 total)	Enabled	Trigger an alert when there are **more than 1** messages in the last **80** minutes with the same value of **Stand FlightTimeband**, with distinct value of **FlightNumber**, matching **all** of the following rules: **ModificationType matches exactly STAND** **FlagAD matches exactly A**	Edit Advanced settings Clone Delete Disable
Milan Airport: High Risk File detected	High	admin	0 alerts/day (56 total)	Enabled	Trigger an alert when there are **more**	Edit Advanced settings Clone Delete Disable

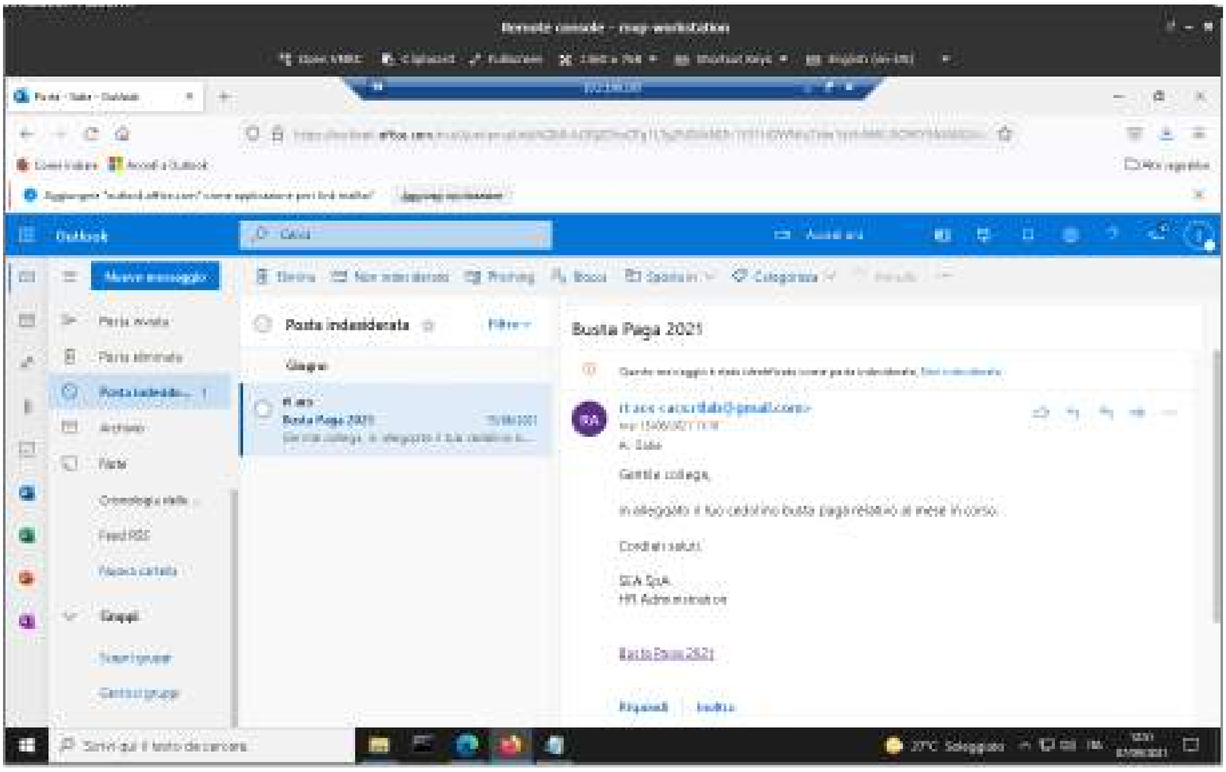
Figure 3.2: Correlation Engine rules

Table 3.1: Alerts raised during the scenario

Time	Title	Detection systems	Affected Assets
00:03	High risk file detected	Malware Analyser	MXP Workstation
00:07	ALCAD detect Port Scanning	ALCAD	MXP Workstation
00:15	Wrong gate changes	MAIS	FIDS
00:22	Double stand assignments	MAIS	FIDS
00:35	ID not match at AOC door	UAC	Airport’s Access Control System

3.2 Malware Analyser

During the scenario, the Malware Analyser has to detect the first step when a corrupt Word document is downloaded from an email on the computer as visualized in Figure 3.3 below.



Busta Paga 2021

Gentile collega,

in allegato il tuo cedolino busta paga relativo al mese in corso.

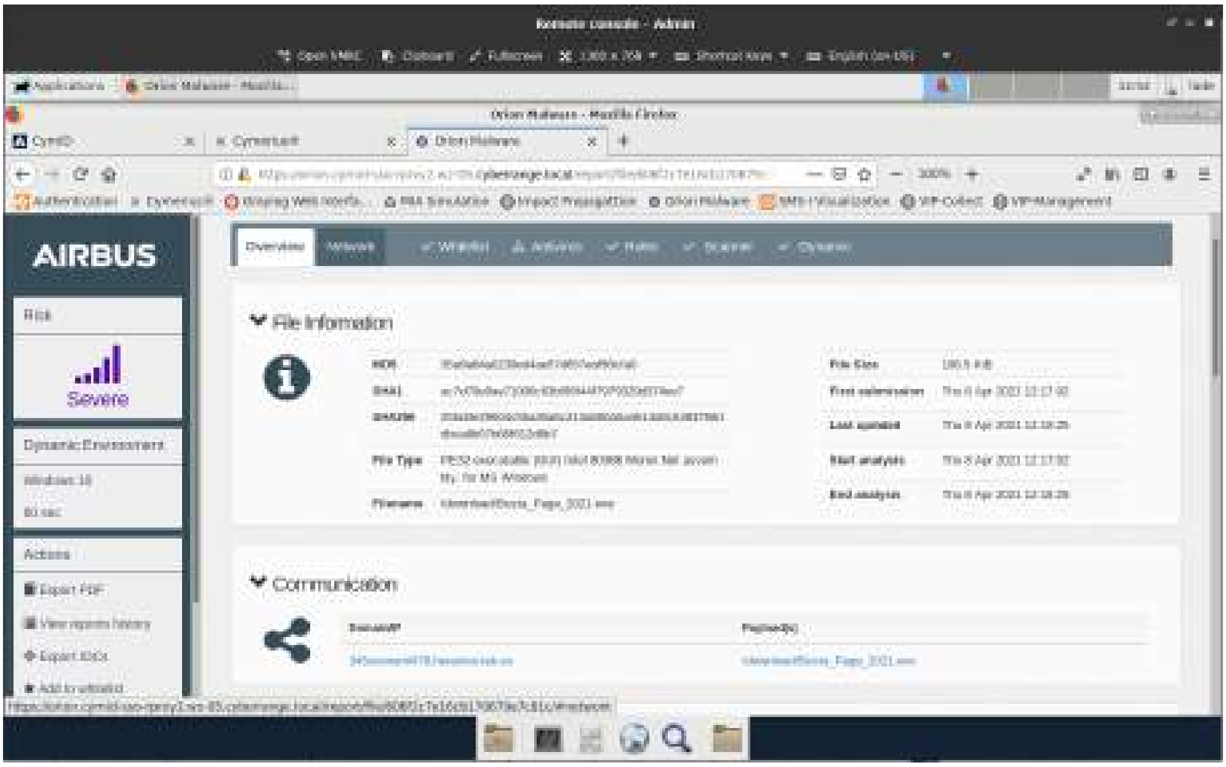
Cordiali saluti

SEA SpA
HR Administration

Busta Paga 2021

Figure 3.3: Email with Malware

The file was extracted from the network and sent to the Malware Analyser (Orion). The file was detected as a severe risk, due to the fact that it is actually an executable file trying to open a remote connection, as shown in Figure 3.4.



File Information

Communication

Figure 3.4: Malware Analyser report

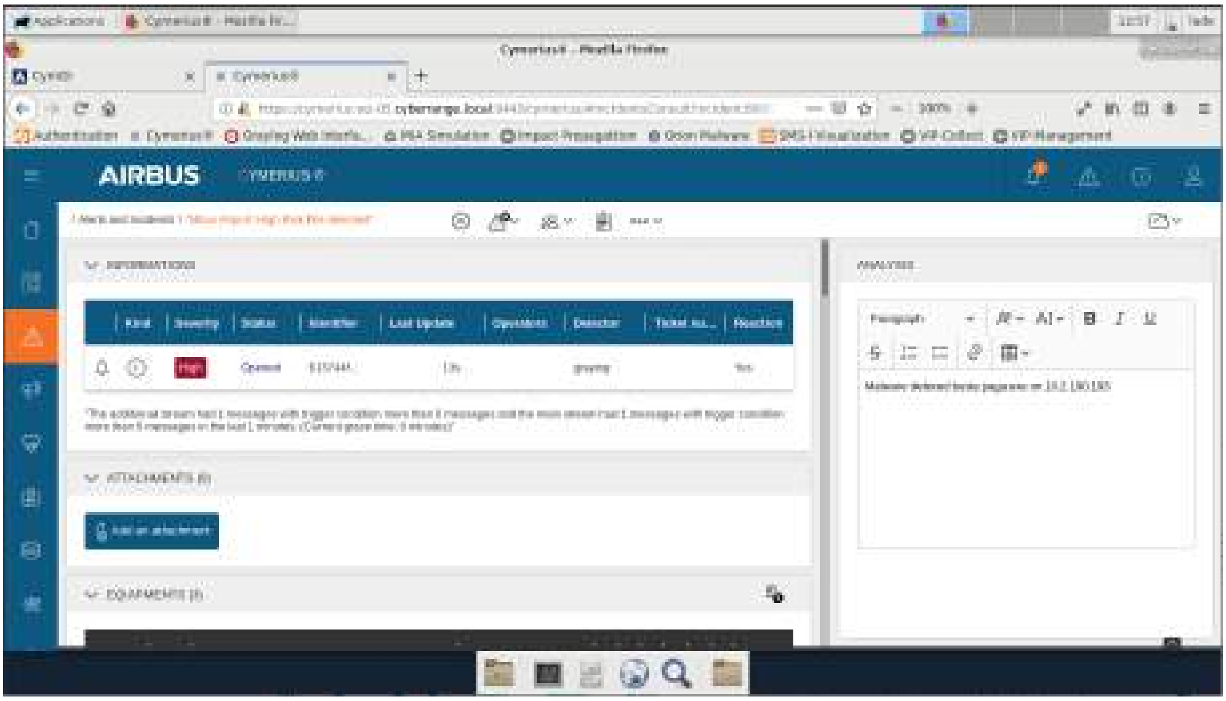
3.3 Incident Management Portal (IMP)

The Incident Management Portal receives Alerts from the Correlation Engine. An operator checks each Alert and assigns it to another operator who will be in charge of the investigation. The operator can classify the Alert as an Incident or close it. If the Alert is classified as an Incident, this Incident will be sent to the Impact Propagation Simulation (IPS) and Crisis Alerting System (CAS). Table 3.2 depicts the Alerts and Incidents raised during the scenario.

Table 3.2: Alerts and Incidents raised during the scenario

Time	Title	Severity	Affected Assets	Operator actions
00:03	High risk file detected	High	MXP Workstation	The operator raised an Incident and sent it to IPS and CAS. The operator asks to disconnect immediately the computer from the network
00:07	ALCAD detect Port Scanning	Low	MXP Workstation	The operator identified thanks to the IP source, that the Alert is related to the first one. Nothing more to do, excepting to check that the infected computer is disconnected from the network.
00:15	Wrong gate changes	Medium	FIDS	The operator raised an Incident and sent it to IPS and CAS
00:22	Double stand assignments	High	FIDS	The operator raised an Incident and sent it to IPS and CAS
00:35	ID not match at AOC door	High	UAC	The operator raised an Incident and sent it to IPS and CAS.

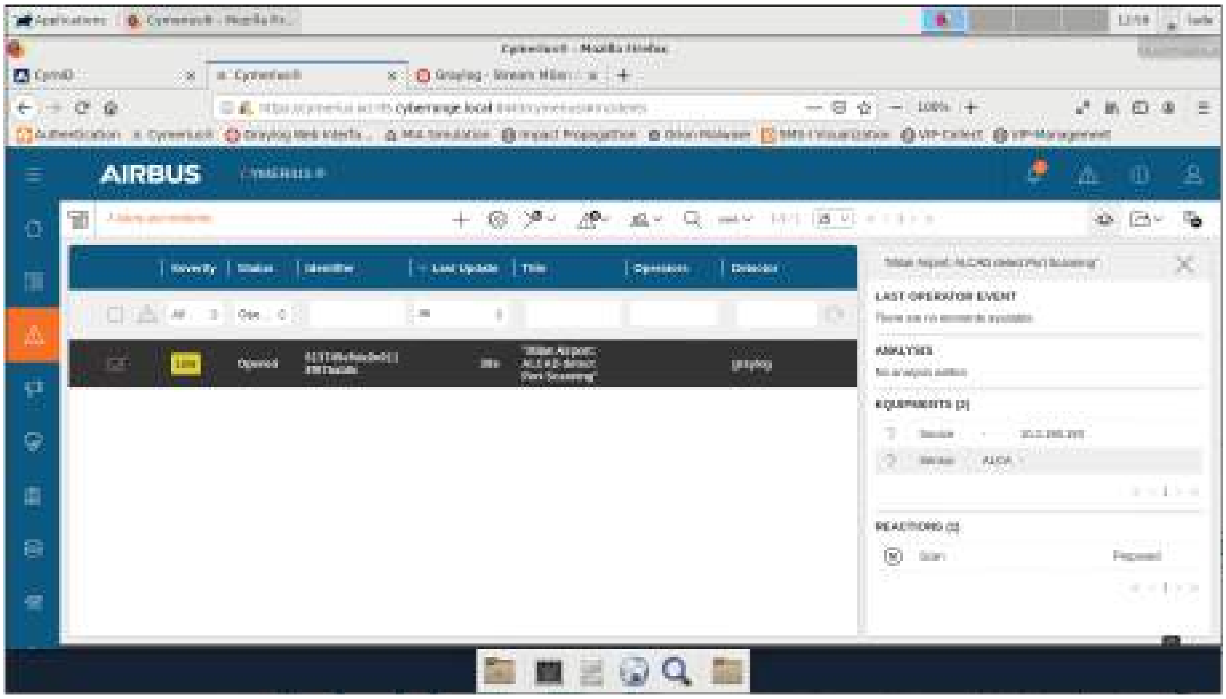
The first step is to send an email with a link to an infected file. The Alert was escalated to the Incident Management Portal. The operator was able to quickly identify the infected workstation with IMP. Thanks to the Malware Analyser (Orion), the operator was able to understand what the malware was trying to do. He immediately asks to disconnect the workstation from the network. Figure 3.5 shows the Alert in IMP.



Kind	Severity	Status	Identifier	Last Update	Operators	Detector	Ticket nu...	Reaction
	High	Opened	[illegible]	[illegible]		graylog		[illegible]

Figure 3.5: IMP showing the Alert “High Risk File detected”

The second step is a network scan that ALCAD detected. The operator identify that the source of the network scan is the same as the workstation corrupted by the malware. The operator decided after checking with the IT that the workstation is disconnected from the network, to close the Alert. The Figure 3.6 shows the Alert in IMP.



Severity	Status	Identifier	Last Update	Title	Operators	Detector
Low	Opened	[illegible]	[illegible]	"Milan Airport: ALCAD detect Port Scanning"		graylog

Figure 3.6: IMP showing the Alert “ALCAD detect Port Scanning”

For demonstration purpose it was assumed that the workstation was not disconnected and that the attacker was able to proceed and identify the M-AIS to change the gate, and assigned a non-Schengen departure gate to a Schengen flight. The Figure 3.7 shows the Alert in IMP with the analysis made by the operator and sent to the CAS.

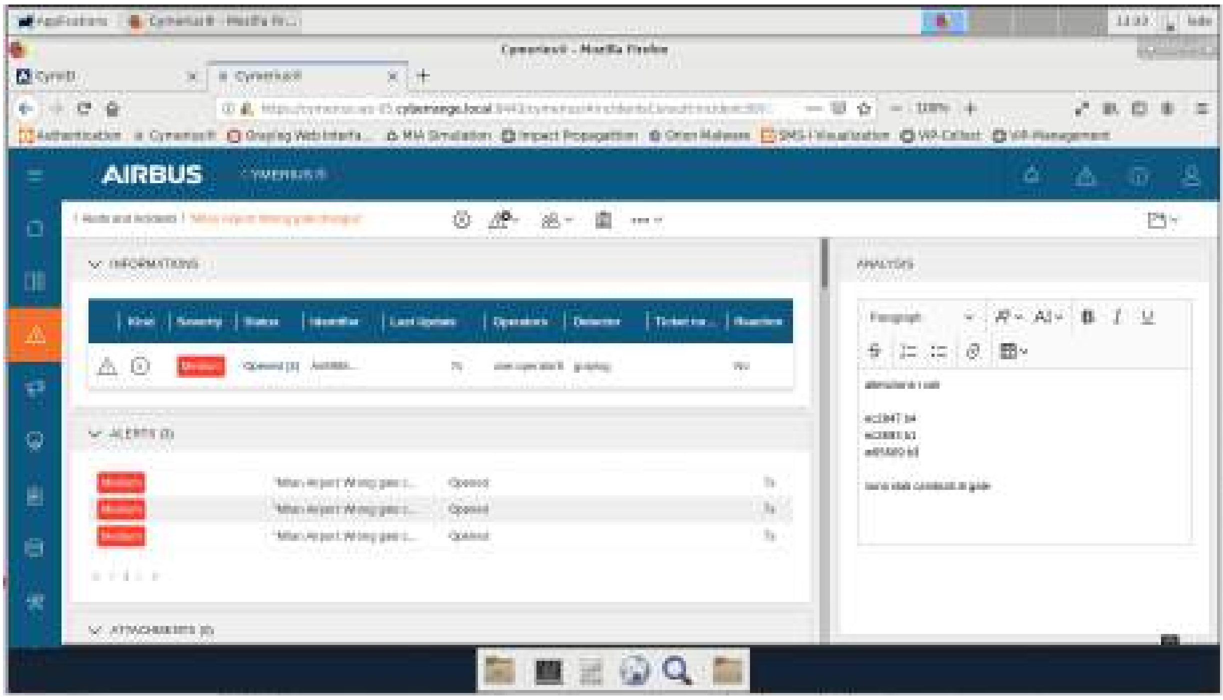


Figure 3.7: IMP showing the Alert "Wrong gate changes"

The following step is the assignment of two flights to the same stand. The Figure 3.8 shows the Alert received in IMP. Thanks to the SATIE Tools the operator was able to quickly identify the flights and inform the AOC with the CAS.

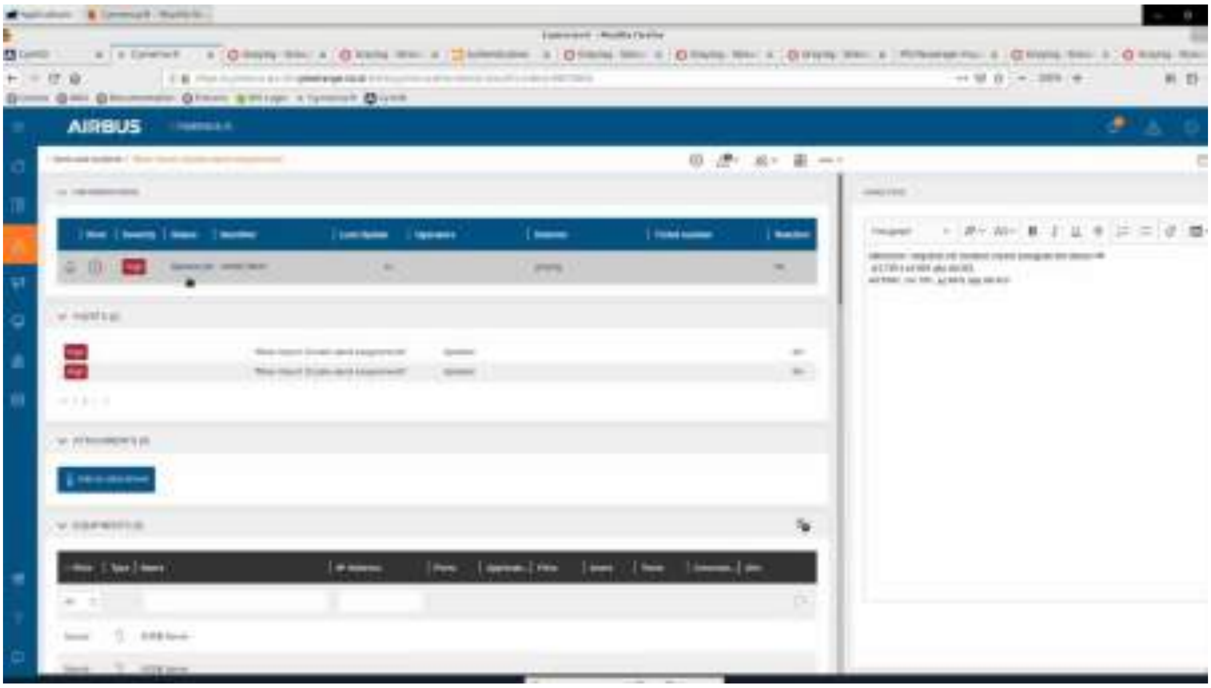


Figure 3.8: IMP showing the Alert "Double stand assignment"

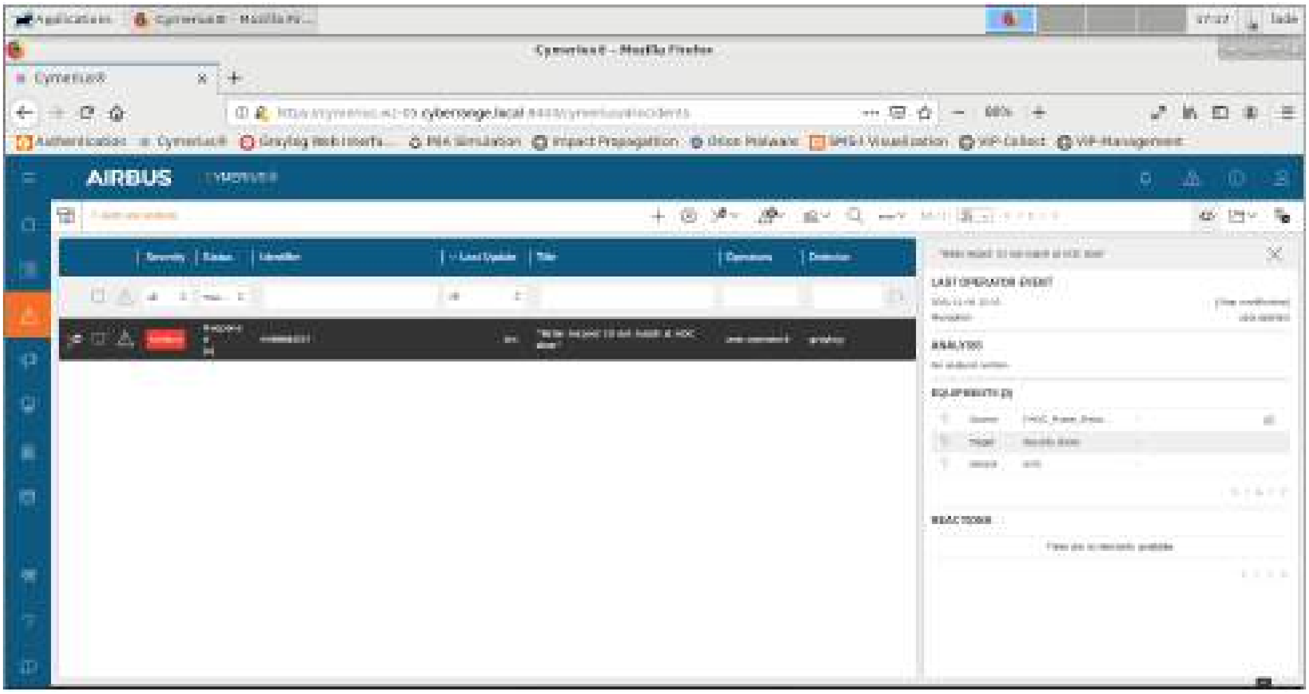


Figure 3.9: IMP showing the Alert “ID not match at AOC door”

The last step is the attempt to access the AOCC door entrance with a stolen badge. Figure 3.9 shows the Alert received in IMP. Thanks to the SATIE Tools the SOC operator immediately sends the Incident to the AOC operator through the CAS.

3.4 ALCAD

An overview of the flow of information and ALCAD response is shown in Figure 3.10. Once the malicious actor performs a scanning attack on the network, his/her activities are reflected in the network characteristics. The information about the network traffic is sent from hardware and software network probes – such as routers and computer terminals – to the collector, where it is aggregated. The data is then sent to the ALCAD processing cluster. Relevant features – such as flow duration, number of bytes in/out, destination ports etc. – are extracted from the data. Further on, the Machine Learning algorithm processes the data to detect any anomalous activity. In case when an anomaly is detected, the ML algorithm attempts to detect the type of the attack. Once completed, if anomaly was detected, an Alert is generated by ALCAD containing all important information. This Alert is sent to the Correlation Engine. The Alert is then assigned a priority – usually low in case of scanning attacks – and displayed to the operator in the Incident Management portal. Please see Table 3.2 for more details.

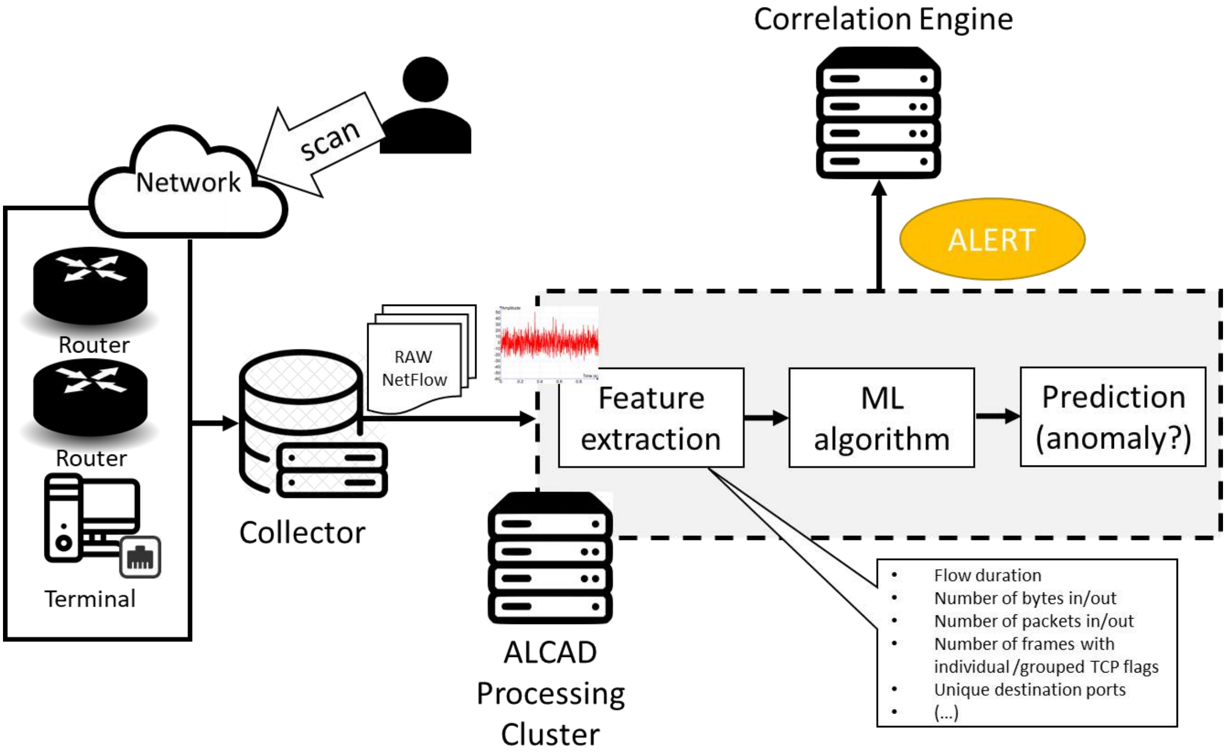


Figure 3.10: General ALCAD response flow in the demonstration

3.5 Unified Access Control (UAC)

The Unified Access Control solution has been deployed at the Milan Airport AOCC entrance door to detect abnormal scenarios such as tailgating attempts or a stolen access card. The Unified Access Control is combining facial recognition software (Augmented Vision) on the IP camera located at the entrance door and a fingerprint/card reader (MorphoWave). This setup can be seen also in Figure 3.11.

In the scenario of the Milan Airport attack, the MorphoWave is used as a card reader and the Unified Access Control will verify the ID of the user via both identification processes:

- Via facial recognition thanks to Augmented Vision;
- Via contactless card access thanks to MorphoWave.

If the user IDs retrieved from the Augmented Vision and the MorphoWave are the same, it means that the user that taps the card on the reader is the true owner of the card. Therefore, the system will trigger the door opening.

If the user IDs retrieved from Augmented Vision and the MorphoWave are different, it means that the user that taps the card on the reader is different compared to the true owner of the card, which can most likely mean that the card has been stolen. Therefore, the system will behave as follows:

- The door will remain closed (the UAC does NOT send an event to open the door);
- The UAC will trigger a live Alert the SOC Correlation Engine with the following statement “Alert – ID not match at AOCC door”.

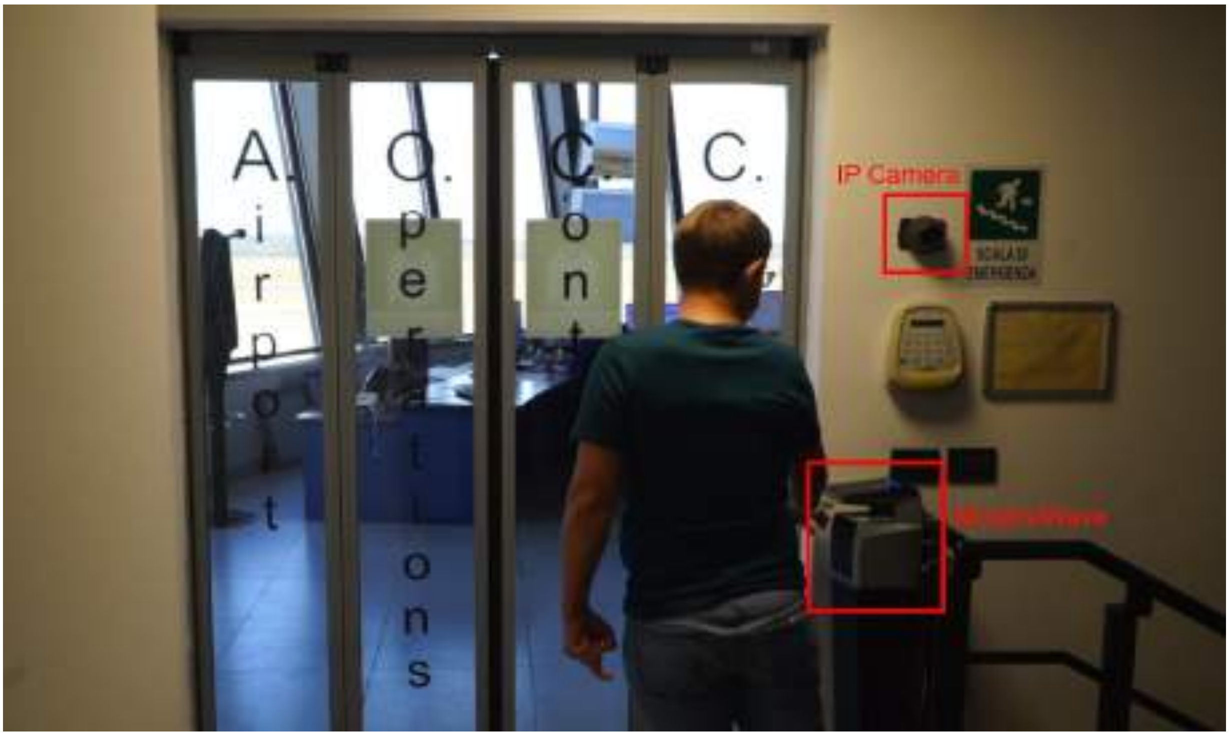


Figure 3.11: The Unified Access Control Tool deployed at the Milan Airport AOCC entrance door

During the execution of the scenario, a contractor of Milan Airport (with user ID 111) has stolen the access card of an employee (user ID 222) and tried to infiltrate the AOCC room to perform malicious operations.

When he arrived at the AOCC entrance door, the Unified Access Control recognized the attacker with his face ID “111”. However, when he tapped the card of the employee, the system retrieved the ID “222” from the stolen card. The UAC compares the IDs from both sensors and immediately detects the discrepancies in the identification process for access (Figure 3.12).

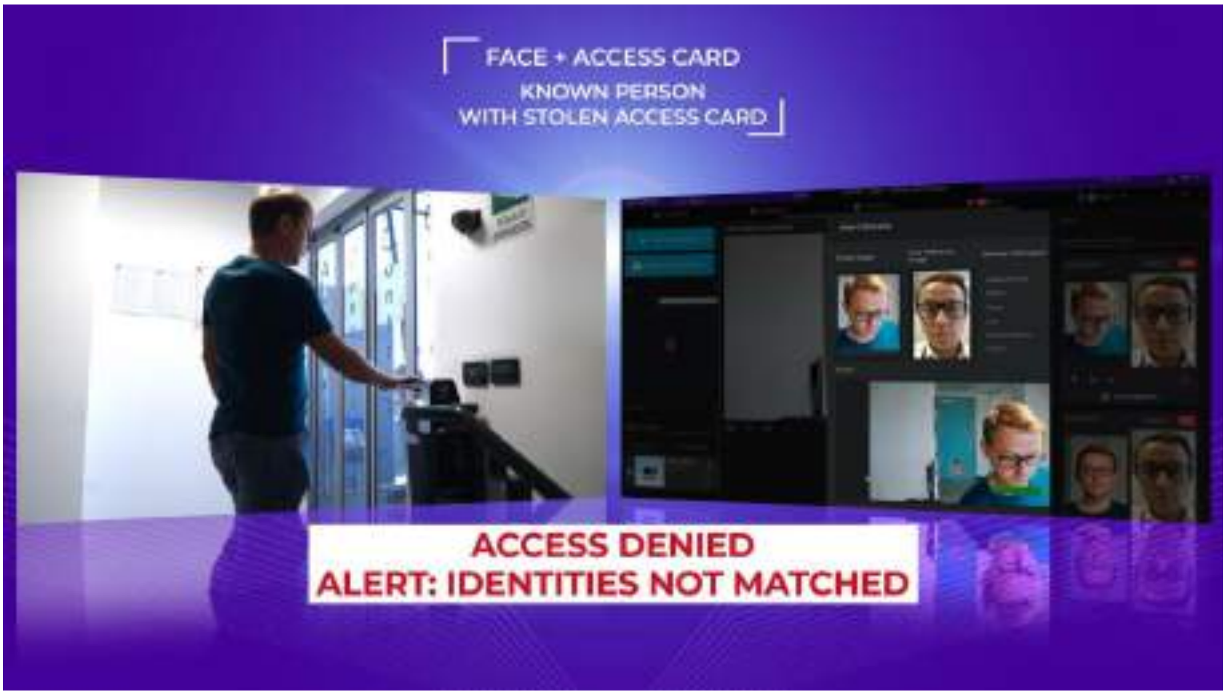


Figure 3.12: The Unified Access Control Tool in operation during live demonstration (left is actual scene and right is view from Augmented Vision / IP camera)

In that scenario, the door remained closed (no access event sent to the door) and an Alert was automatically raised to the SATIE Correlation Engine as “Alert – ID not match at AOCC door”, which is exemplified in Table 3.3.

Table 3.3: Example of an Alert sent to the IMP from the UAC

Time (CEST)	Incident ID	# of unique Alerts	Type of Alert	Systems/assets impacted
15:35	1234	1	Alert – ID not match at AOC door	Airport Access Control System

As this type of abnormal detection is considered as a serious physical threat on airport operations, a rule was edited in the Correlation Engine such that every time it receives an Alert of this type “ID not match”, this Alert would be automatically escalated to the Incident Management Portal for further actions.

In that attack scenario at Milan Airport, the Alert “ID not match” was escalated to the Crisis Alerting System so that the AOC operators could take further actions by sending security team on site to stop the attacker.

3.6 Crisis Alerting System (CAS)

The Crisis Alerting System (CAS) has been deployed on the CyberRange platform, and was accessed by the Milan Airport AOC operators through their workstations’ browsers. It provided the AOC operators with alarm management, notification and collaboration functionalities, thus supporting their response operations against the critical situations that were designed and implemented according to the scenarios created.

During the execution of the scenario, a number of Incidents were forwarded from the SOC to the AOC operators, as displayed in Table 3.4.

Table 3.4: Incidents forwarded to the AOC operators (CAS)

Time (CEST)	Incident ID
13:29:17	89884706
13:43:39	89884716
14:00:00	89884721
14:13:38	89884723

For every new Incident that was created in SOC and forwarded to the CAS, a new alarm was created and handled by the AOC operators accordingly. Through CAS, the AOC operators were able to monitor the situational picture of the airport, as well as the passengers and employees, by combining information from the SOC with information from the other airport security systems like the CCTV.

Furthermore, CAS enabled the communication between the AOC operators and the public safety agencies, through its collaboration functionalities. By this enhanced collaboration mechanism, all the involved personnel and responders were constantly informed about any new information gathered by the AOC operators.

The AOC operators, used the "Alarm Management" perspective provided by CAS, in which they got a list of the active security related events (sent by SOC) and they were able to inspect all the alarm details as well as the results of the Impact Propagation Simulation as depicted in the following figure. On each selected alarm a list of recommended actions was available to be executed by the CAS operator. This list of actions was based on the Milan airport's operational procedures.

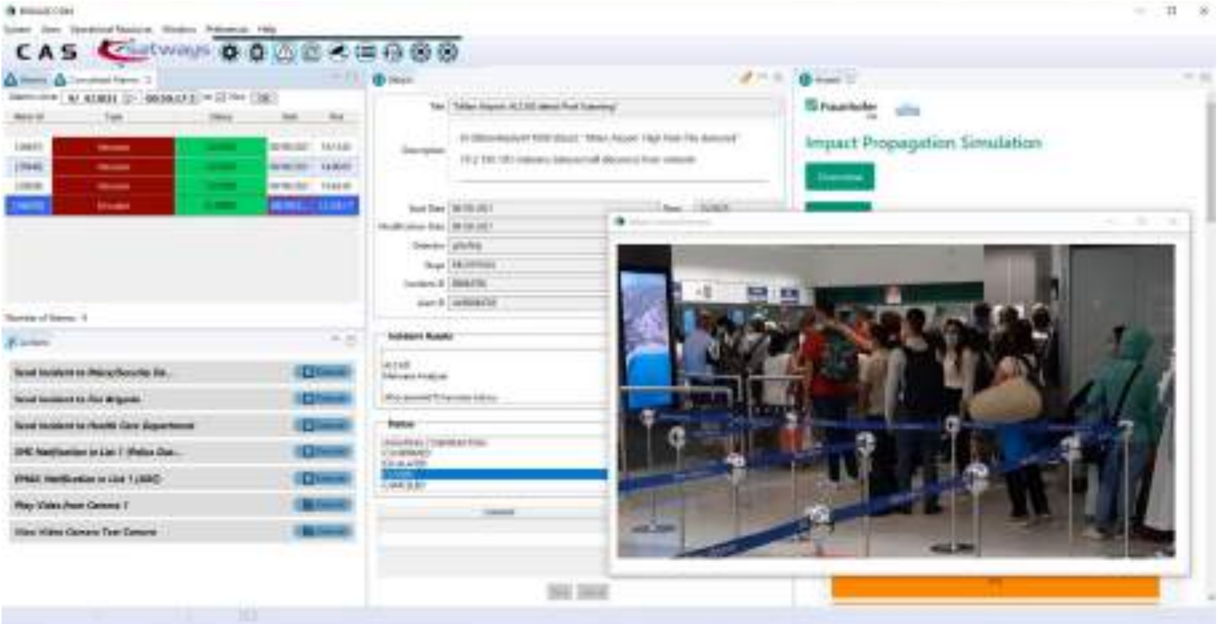


Figure 3.13: CAS – Alarm Management perspective

Furthermore, the CAS operators used the "Collaboration" perspective (Figure 3.14) through which the communication between the AOC operators and the public safety agencies that were involved in the alarm mitigation, was realised. The following figure depicts a general use case of the "Collaboration" perspective. Also, CAS operators found that the SMS and email functionalities were extremely useful and actually used them while handling most of the alarms, in order to notify external actors, that did not have access to the CAS, expanding the set of communication recipients.

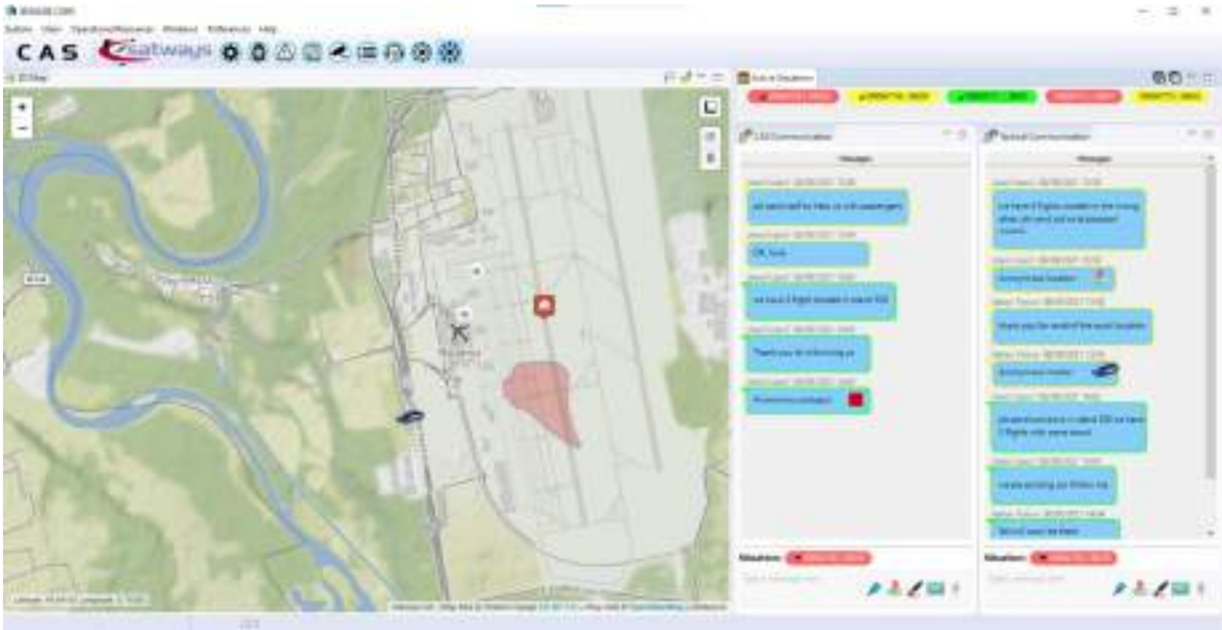


Figure 3.14: CAS – Collaboration perspective.

The Impact Propagation Simulation component was also accessible through the CAS (Figure 3.13), and the operators had the opportunity to consult its results before proceeding with actions. More details on the IPS tool are given below.

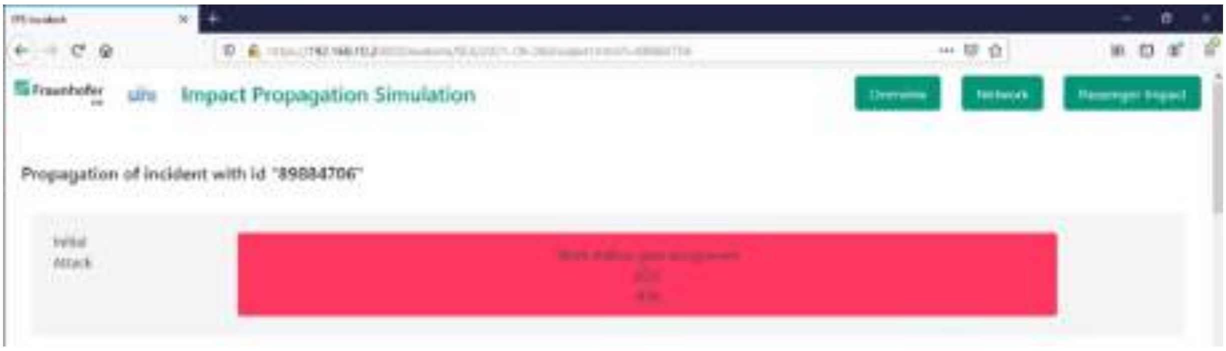
3.7 Impact Propagation Simulation (IPS)

The IPS received single and aggregated Incidents during the demonstration on 8th September. The Incidents are listed in Table 3.5. The SOC operator can choose Alerts which he classifies as Incident and forwards them either as single or aggregated Incident to the IPS and Crisis Alerting System (CAS). By checking the results of IPS, the SOC operator can gain more information about what impacts to expect next.

Table 3.5: Incidents received in IPS during the demonstration

Time (CEST)	Incident ID	# of unique Alerts	Systems/assets impacted	ABM trigger
15:29	89884706	2	Work station for gate assignment	-
15:43	89884716	6	AODB server, gates B01-B04	Schengen
15:59	89884721	1	AODB server, aircraft stand	-
16:13	89884723	1	AOC room entrance, security doors	-

For example, in Figure 3.15, the first Incident received with ID “89884706” and the asset identified are presented in the Incident view of IPS.



Propagation of incident with id "89884706"

Initial Attack

Figure 3.15: First Incident received in IPS from IMP on 8th September

In this incident-view, only one impacted asset can be presented. However, the network view enables to present all received Incidents in specific graphs (8). Figure 3.16 presents the network topology of all assets and their interrelations along with the impacted assets during the whole day. The same impacts are given in Figure 3.17 but here the number of undisturbed assets is presented as a function of time. The assets of the first three Incidents have been correctly identified but the last asset has been mapped to 'finger door' by mistake. This will be investigated in the future and adapted in IPS.

As given in Table 3.5, one Incident has triggered the Agent-Based Model (ABM) where the congestion of passengers due to the gate manipulation has been simulated (see Figure 3.18).

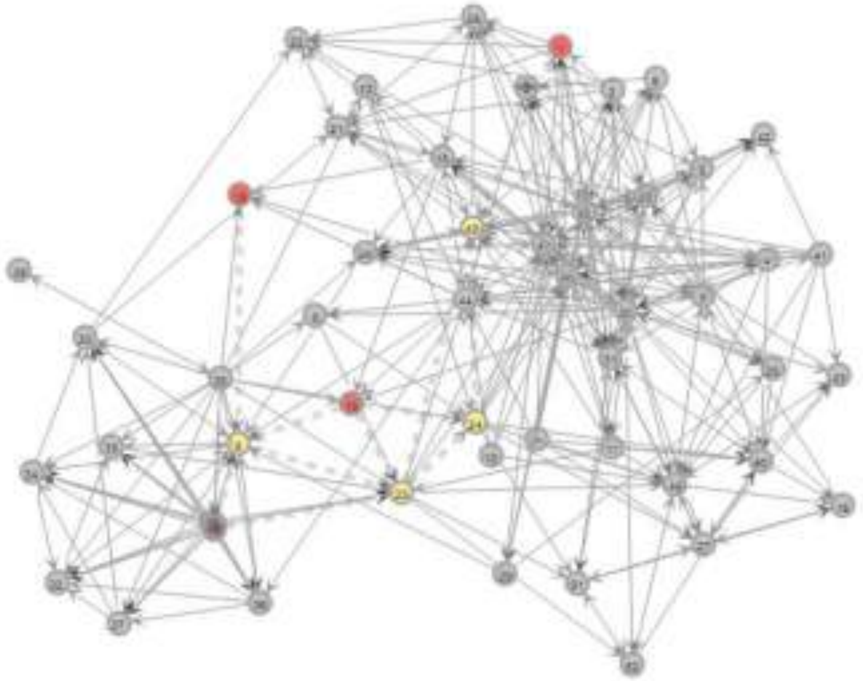


Figure 3.16: Network representation of the assets. All nodes that have been attacked (red) on 8th September

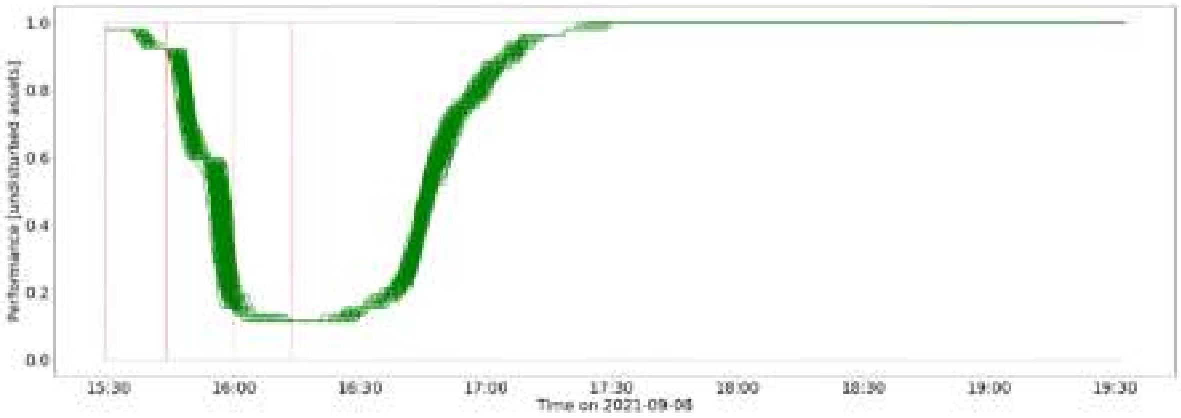


Figure 3.17: All four Incidents (red vertical lines) received on 8th September. The number of nodes of the network which is undisturbed is given as green lines for repeated simulations

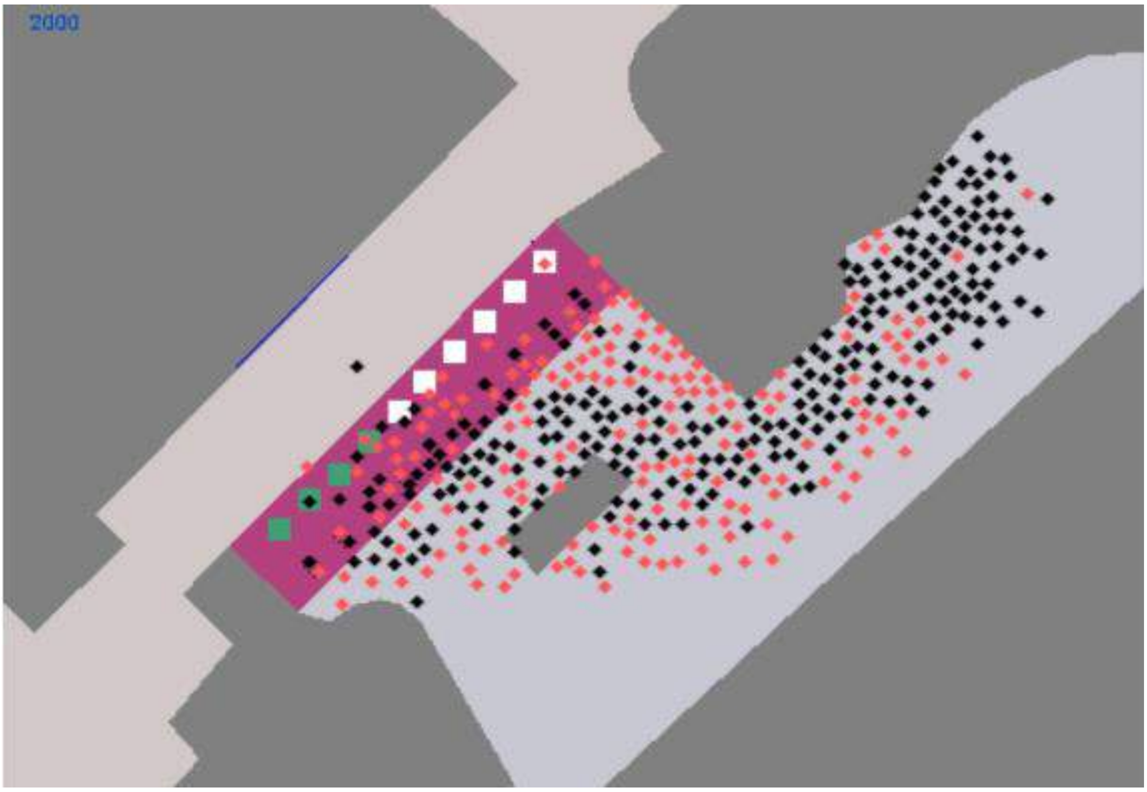


Figure 3.18: Screenshot of the ABM video which has been shown similarly on 8th September triggered by the Incident with ID ‘89884716’

All this information, is also visible to the AOC operator. During the demonstration, the AOC operator checked the IPS regularly and specifically for the second Incident that triggered the Agent-Based Model (ABM).

3.8 Investigation Tool (SMS-I)

The SMS-I tool deals with the analysis of data from heterogeneous systems, over different time frames and correlates them to find evidence of the causes of an attack, allowing the improvement of the forensics investigation at airports. It provides to the SOC operator information about the system’s events, Alerts, and Incidents through graphical dashboards and Alert classification suggestions. The intelligent data process is supported by a machine learning engine that allows the identification of anomalous situations that can be related to possible incident occurrences. An intelligent dashboard is provided to support decision makers in a deep analysis of how the breaches and the assets were explored and compromised.

During this demonstration, based on the Alerts received from the Correlation Engine and Incidents marked by the SOC operator in the IMP, SMS-I provided multi-dimensional analytics over cyber and physical dimensions. The results are displayed to the operator via an intelligent dashboard that supports the investigation of activities and event timelines. Figure 3.19 shows a representation of all Alerts and Incidents that occur during the execution of different scenarios. This representation provides to the SOC operator a view of the events in a chronological order, which can be very helpful for their security analysis.

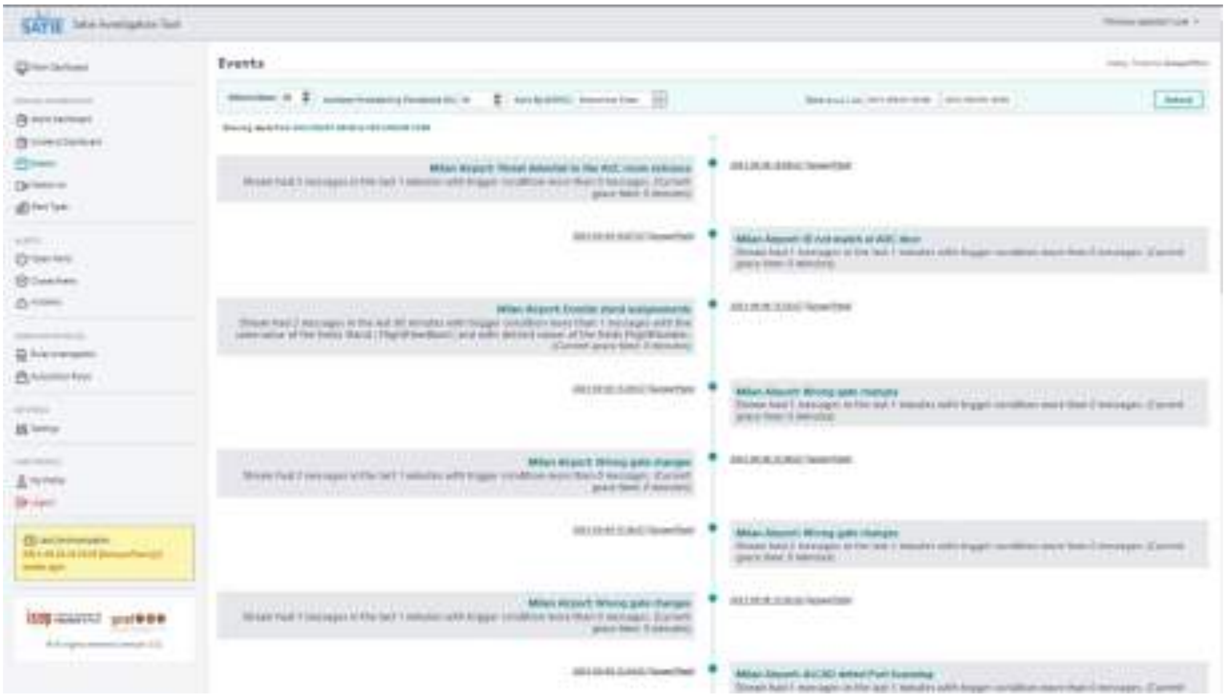


Figure 3.19: Alerts and Incidents displayed in SMS-I

The SOC operator can get all the information of each event clicking on it, which can help him in the investigation of the attack. Also, a list of all Incidents is available in the intelligent dashboard (Figure 3.20). The colour of the cards allows the SOC operator to quickly and easily understand the severity level of each Incident.

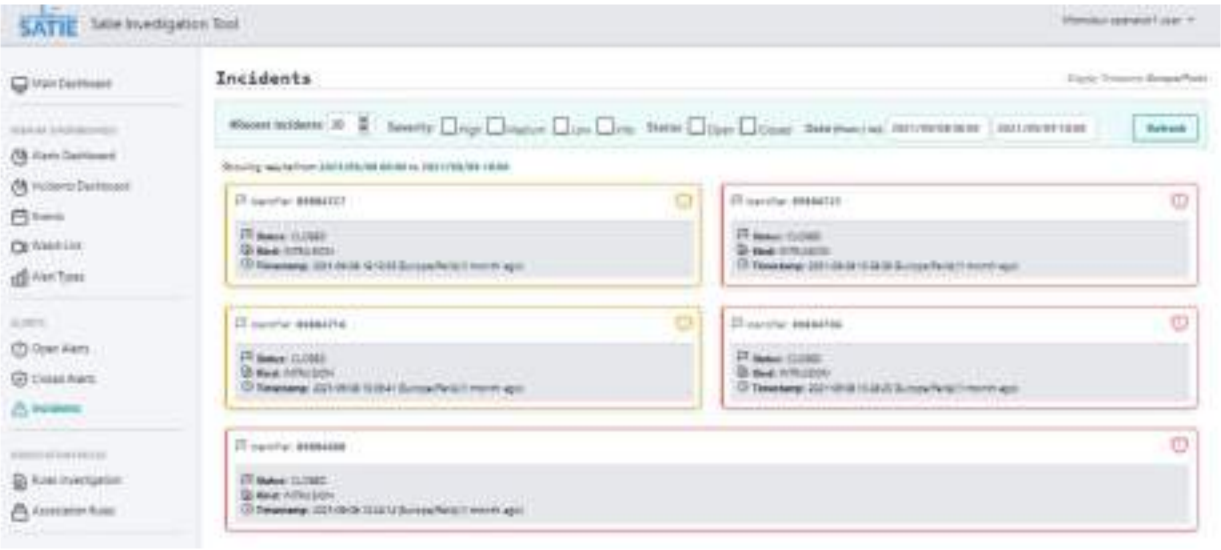


Figure 3.20: SMS-I’s Incidents List

For each Incident, the SOC operator can see its details and understand which Alerts originate the Incident (Figure 3.21). For example, if two Alerts were aggregated to generate an Incident both Alerts can be seen in the Incident details.

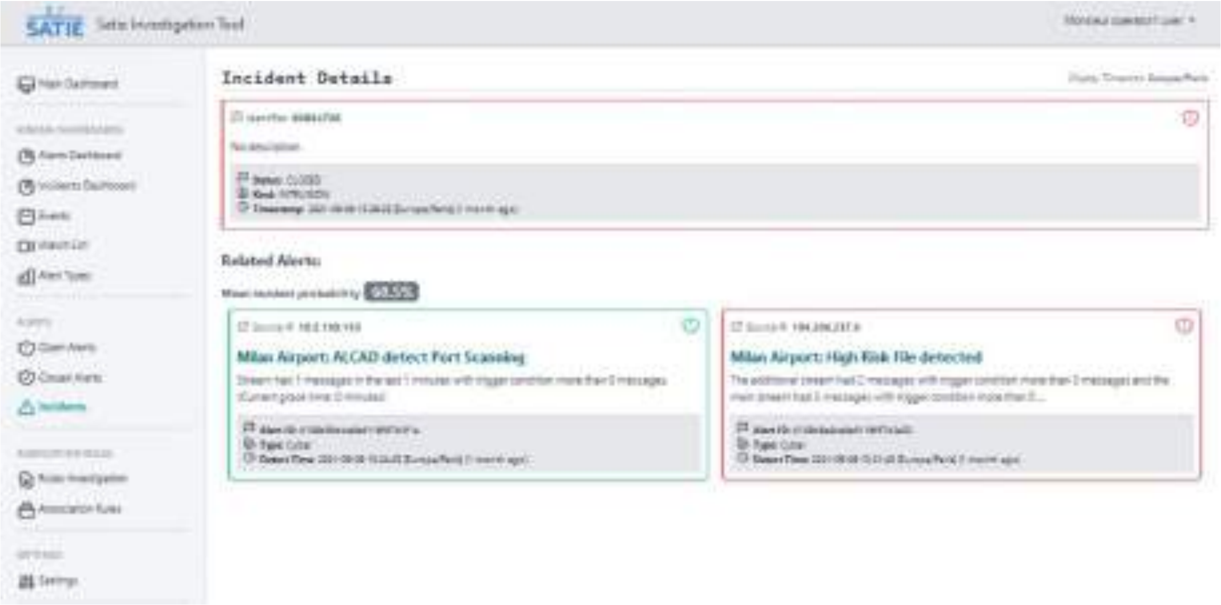


Figure 3.21: Incident details displayed in SMS-I

The Alert details can also be analysed by the SOC operator (Figure 3.22). Several details are provided, namely the sensor that raised the Alert, the severity, and the type of the sensor. The probability of this Alert being an Incident is also provided and can help the SOC operator understand that an Alert that appears to be a low severity Alert might be an Alert that needs more attention and should be reported with a higher severity.

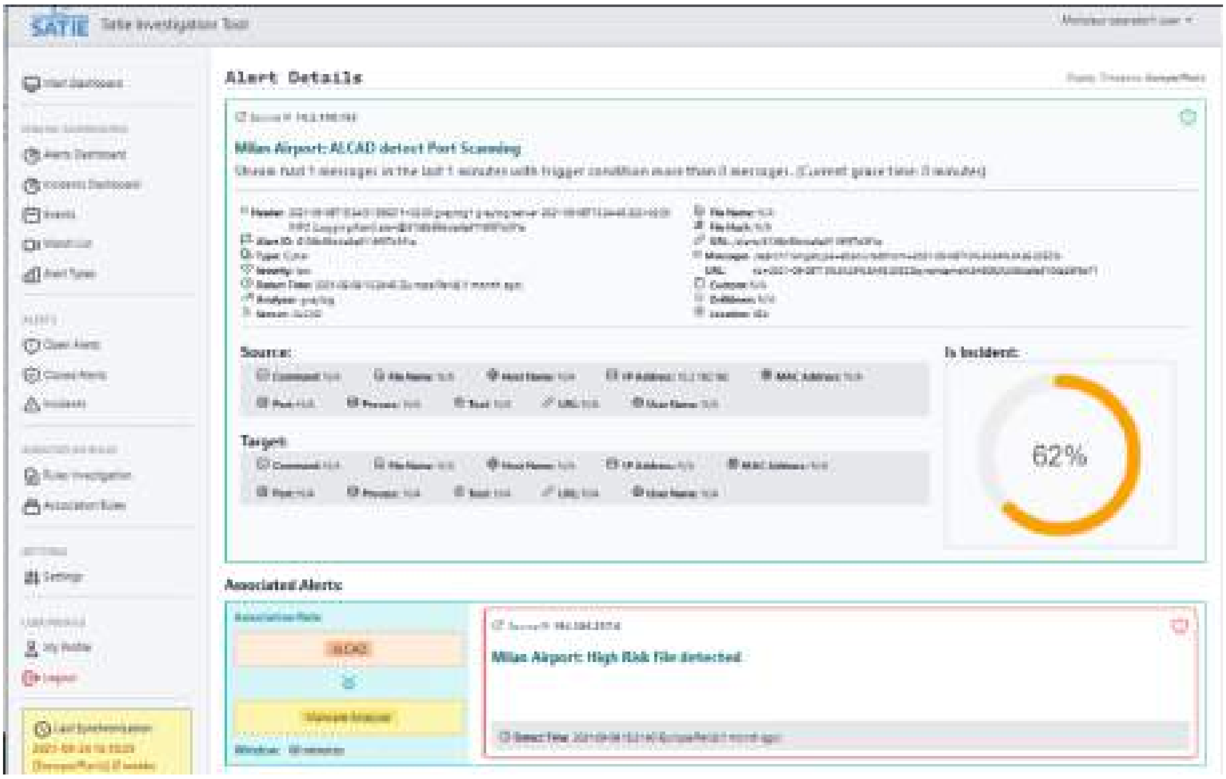


Figure 3.22: Alert details displayed in SMS-I

This can be illustrated with the port scanning Alert raised during the demonstration. It was reported as a low severity Alert, but the intelligent engine gives a high probability (62%) of this Alert be an Incident. It occurs because the intelligent engine understands that this Alert is usually related to a malicious file Alert, a high severity Alert. Moreover, a rule was generated by the association rules engine (Figure 3.23) that identifies probable relationships between these two types of Alerts. Therefore, using association rules, the SOC operator can understand that the malware Alert and the network scan Alert are correlated and should be reported as being part of the same Incident.

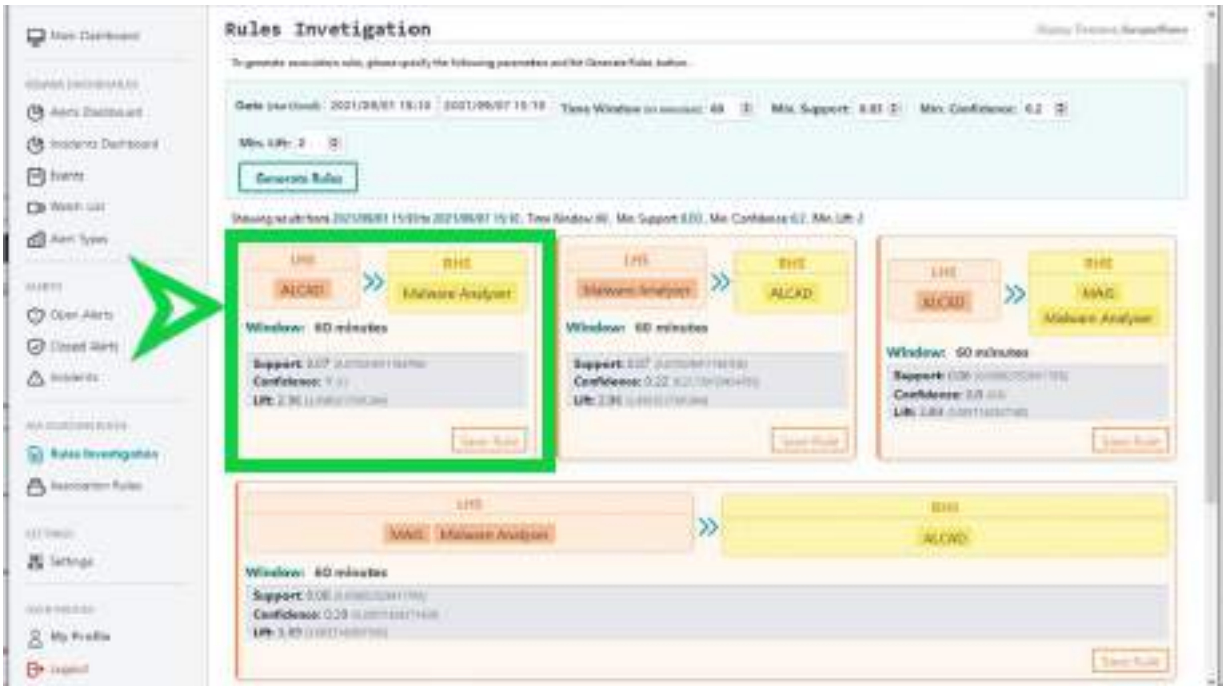


Figure 3.23: Association Rules generated by the SMS-I tool

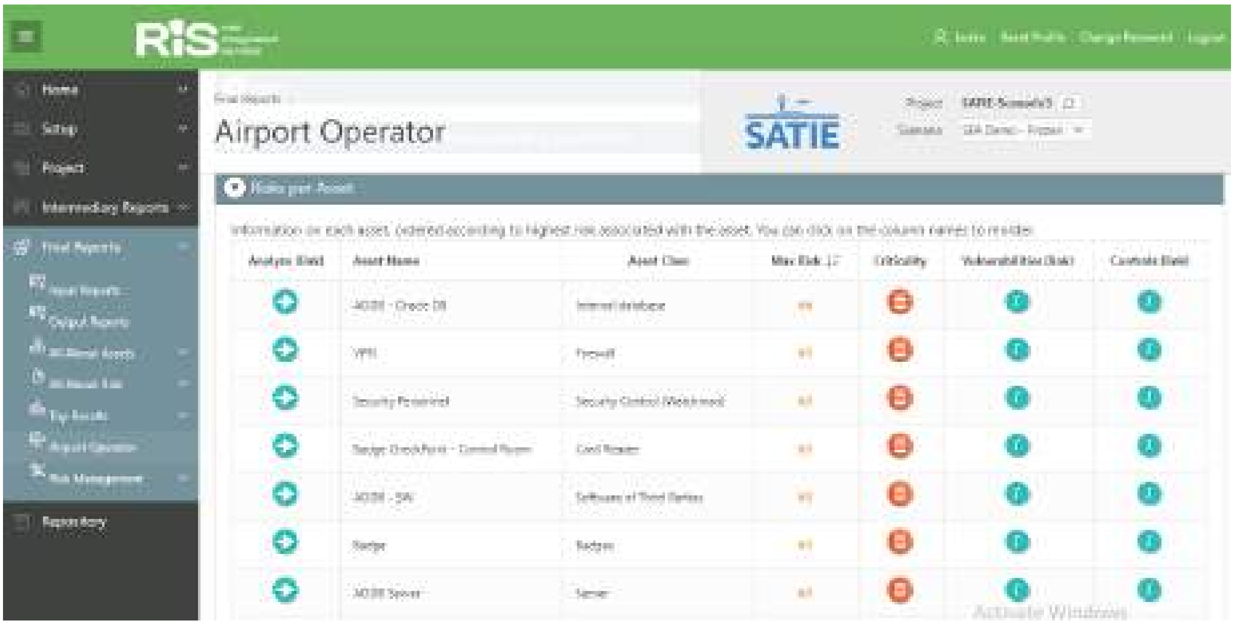
The mean value of the incident probability is shown in the incident details (Figure 3.21). This mean is calculated using the incident probability of each Alert, already referred in the Alert details description. The mean of incident probability helps the SOC operator understand what the probability of the intelligent system is to classify this Incident properly. This is very important to improve the SOC operator's confidence and trust in the intelligent system.

Note that the views shown are just some of the views available in the SMS-I intelligent dashboard. The SOC operator can use the views more suitable for him, and which help him to get more information during the analysis of the events.

3.9 Risk Assessment Platform (RIS)

The Risk Integrated Service (RIS) tool is to be used during the preparatory phase for airport personnel. It offers the SOC and AOC operators an overview of where the highest risks are within the airport environment: which assets are most at risk, which vulnerabilities the airport is most exposed to, as well as which threats are associated with the highest risks. The RIS methodology is governance-based, meaning that it uses relevant standards and regulations to assess how well the various controls are in place, which in turn decrease exposure to vulnerabilities, which can be used by threats to cause damage to the assets in question. Airport personnel should complete the risk assessment at regular intervals, updating the asset inventory and each asset's criticality level, and in particular updating exactly how well each control and security measure is in place for each airport operation.

The results of the risk assessment for the scenario taking place at SEA overall show high risks to information being altered in the AODB and risks that badges could be lost or stolen. These were exactly some of the attacks that occurred in this scenario. And thus, this stresses the importance of risk managers to perform assessments regularly and identify high risks to understand where to put their efforts to mitigate such risks.



Final Reports

Airport Operator

Project: SATIE-Scenario5

Scenario: SEA Demo - Frozen

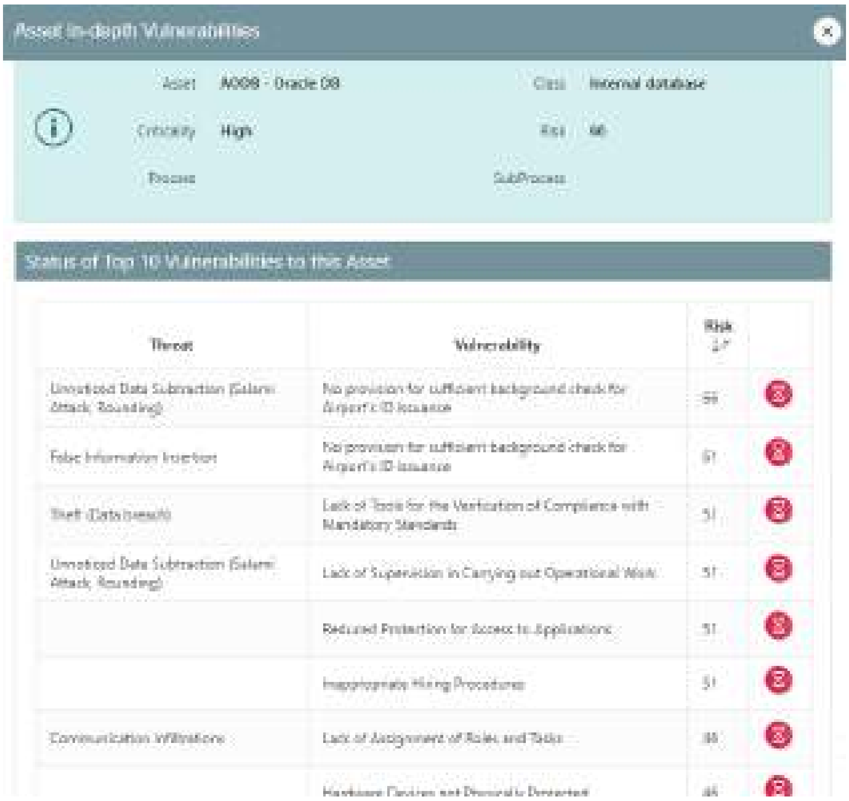
Risks per Asset

Information on each asset, ordered according to highest risk associated with the asset. You can click on the column names to reorder.

Analysis Field	Asset Name	Asset Class	Max Risk	Criticality	Vulnerabilities (Risk)	Controls Field
●	AODB - Oracle DB	Internal database	[illegible]	●	●	●
●	VPN	Firewall	[illegible]	●	●	●
●	Security Personnel	Security Control (Watchman)	[illegible]	●	●	●
●	Badge CheckPoint - Control Room	Card Reader	[illegible]	●	●	●
●	AODB - SW	Software of Third Parties	[illegible]	●	●	●
●	Badge	Badges	[illegible]	●	●	●
●	AODB Server	Server	[illegible]	●	●	●

Figure 3.24: The Airport Operator page of RIS showing the assets with the highest risks

In the risk assessment, the assets with the highest risks are generally related to gaining access (e.g. VPN, security personnel, badges), and the asset with the highest risk is the Airport Operations Database (AODB; see Figure 3.24). The threats contributing the most to that high risk are shown in Figure 3.25 and include false information insertion, communication infiltration and data breach.



Asset in-depth Vulnerabilities

Asset	AODB - Oracle DB	Class	Internal database
Criticality	High	Risk	68
Process		SubProcess	

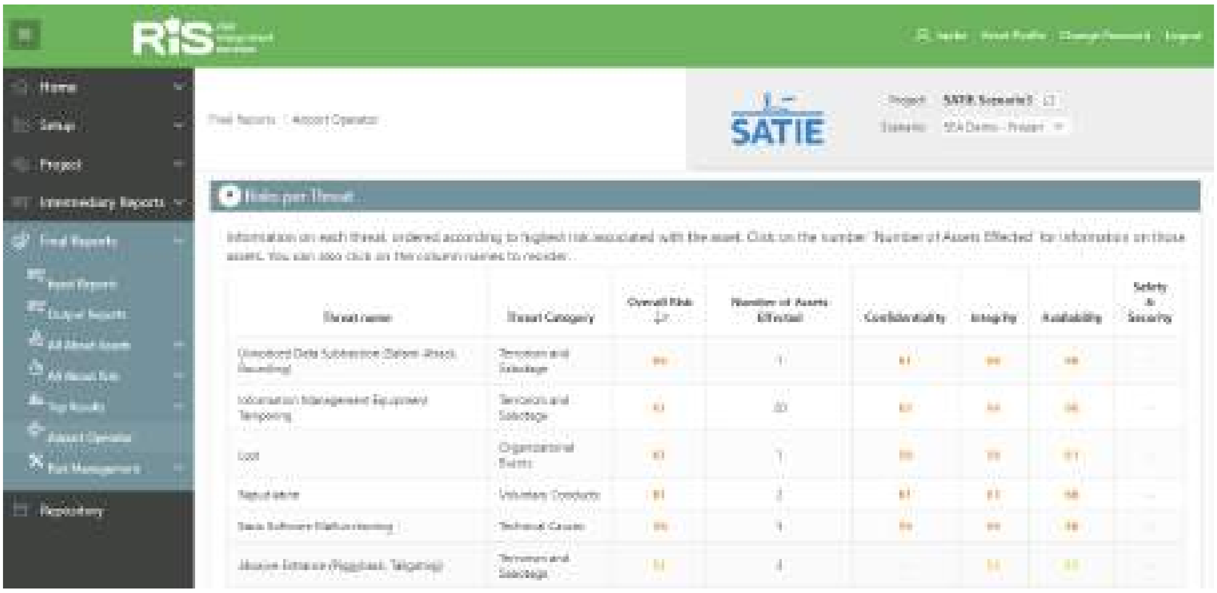
Status of Top 10 Vulnerabilities to this Asset

Threat	Vulnerability	Risk	
Unnoticed Data Subtraction (Salami Attack, Rounding)	No provision for sufficient background check for Airport's ID issuance	59	
False Information Insertion	No provision for sufficient background check for Airport's ID issuance	57	
Theft (Data breach)	Lack of Tools for the Verification of Compliance with Mandatory Standards	51	
Unnoticed Data Subtraction (Salami Attack, Rounding)	Lack of Supervision in Carrying out Operational Work	51	
	Reduced Protection for Access to Applications	51	
	Inappropriate Hiring Procedures	51	
Communication Infiltrations	Lack of Assignment of Roles and Tasks	48	
	Hardware Devices not Physically Protected	46	

Figure 3.25: The threats and vulnerabilities contributing the most to the high AODB risk

A risk manager seeing these results would understand that there are high risks that someone could insert false information in the AODB in some way. Given the importance of the data inside the AODB, this could cause numerous problems, from passengers going to incorrect gates or at the incorrect times causing crowds and confusion, to planes being redirected to incorrect stand assignments potentially creating congestion or even a crash on the apron.

The threats with the highest associated risks overall in this scenario include Information Management Equipment Tampering which can impact 20 assets (see Figure 3.26). With such a potential widespread impact on the assets, this threat should be mitigated.



Final Reports / Airport Operator

Project: SATIE Scenario3
Scenario: SEA Demo - Present

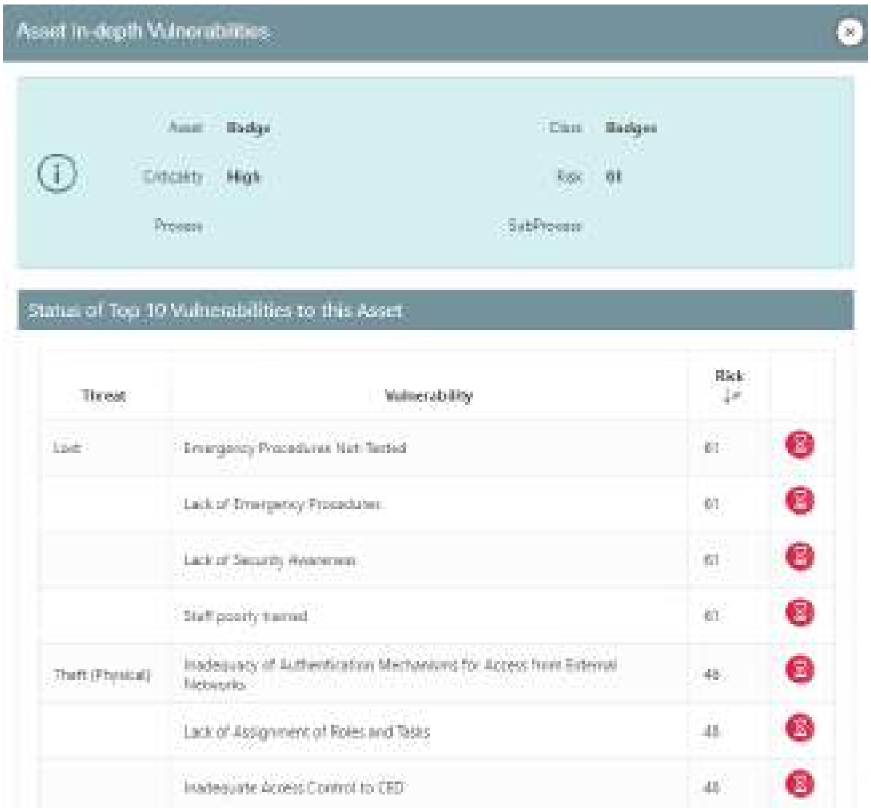
Risks per Threat

Information on each threat, ordered according to highest risk associated with the asset. Click on the number 'Number of Assets Effected' for information on those assets. You can also click on the column names to reorder.

Threat name	Threat Category	Overall Risk	Number of Assets Effected	Confidentiality	Integrity	Availability	Safety & Security
Unnoticed Data Subtraction (Salami Attack, Rounding)	Terrorism and Sabotage	[illegible]	1	[illegible]	[illegible]	[illegible]	-
Information Management Equipment Tampering	Terrorism and Sabotage	[illegible]	20	[illegible]	[illegible]	[illegible]	-
Loot	Organizational Events	[illegible]	1	[illegible]	[illegible]	[illegible]	-
[illegible]	Voluntary Conducts	[illegible]	2	[illegible]	[illegible]	[illegible]	-
Basic Software Malfunctioning	Technical Causes	[illegible]	1	[illegible]	[illegible]	[illegible]	-
Abusive Entrance (Piggyback, Tailgating)	Terrorism and Sabotage	[illegible]	4	-	[illegible]	[illegible]	-

Figure 3.26: The riskiest threats in the SEA scenario

Looking again at the assets with the highest risks, most of them are complex, but it may be surprising to see something as simple as a badge with a high risk. The threats and vulnerabilities contributing the most to this risk are shown in Figure 3.27.



Asset In-depth Vulnerabilities

Asset	Badge	Class	Badges
Criticality	High	Risk	61
Process		SubProcess	

Status of Top 10 Vulnerabilities to this Asset

Threat	Vulnerability	Risk	
Lost	Emergency Procedures Not Tested	61	●
	Lack of Emergency Procedures	61	●
	Lack of Security Awareness	61	●
	Staff poorly trained	61	●
Theft (Physical)	Inadequacy of Authentication Mechanisms for Access from External Networks	48	●
	Lack of Assignment of Roles and Tasks	48	●
	Inadequate Access Control to CED	48	●

Figure 3.27: The threats and vulnerabilities contributing the most to the high badge risk

The two main threats are lost and theft of the badges, and these can exploit the vulnerabilities related to poorly-trained staff with a lack of security awareness. Badges are something that all staff carry and have to display visibly, potentially making them susceptible to loss or theft. Therefore, a risk manager seeing these results would understand that the staff's security awareness should be improved, likely with better training, to prevent these threats to the badges. If an unauthorized person steals or finds a lost badge, they could potentially gain access to security restricted areas and become a severe threat to the airport.

Put together, there are various ways of viewing the risk results: according to asset, according to vulnerability and according to threat. But in the end, they all come down to better implementing the applicable security measures and controls. Therefore, RIS offers a 'What-if Scenario' to model how the risks would change if various controls were applied better so that a risk manager could see if improving a particular security control would greatly reduce risks in general or to specific, highly-critical assets. It allows the airport to best determine where to apply their time and financial efforts to reduce risks and improve their situation.

For use during the demonstration, the risk assessment results were not based on any real situation neither at the Milan airport, nor any other airport, but they represent realistic results. Similarly, the scenarios represented realistic, potential attacks that compromised employees or malicious people could attempt. However, this highlights the importance for airports to have a full understanding of where their highest risks are, to better address time and effort mitigating those risks, such that it would be much more difficult – if not impossible – for an attacker to succeed. For the full results of the real risk assessments performed for these scenarios, please see the EU-restricted deliverable D2.3 (9).

4 Evaluation results

This section presents the evaluation results of the Milan Malpensa Airport demonstration. These provide a tangible assessment of the success factors, including information gained from questionnaires and evaluation participants feedback. Moreover, to validate the SATIE Solution, partners have defined an online evaluation questionnaire to retrieve useful information. The target of the questionnaire was the audience of the Milan Malpensa Airport demonstration event. They participated in the demonstration as observers and provided useful input concerning the SATIE Solution. The evaluation questionnaire form communicated to the audience is presented in the Annex - Evaluation questionnaire.

To measure the Milan Malpensa Airport demonstration success, the following two main aspects were considered:

- Calculate the final value for each KPI related to the Milan Malpensa Airport demonstration;
- Evaluate the responses from the questionnaires filled in during the demonstration.

Section 4.1 presents the Key Performance Indicators (KPIs) related to the Milan Malpensa Airport demonstration and assesses the final values according to its performance. Section 4.2 presents the evaluation results derived from the responders, statistical results of the reported answers, additional feedback gained from the responders regarding the SATIE Innovation Elements (IEs) and information about the evaluation participants, such as the type of entities they reside.

4.1 KPIs calculation

KPIs have been defined to assess the SATIE project success. The final values of KPIs are assessed directly from data gathered from the execution of the Milan Malpensa Airport demonstration and presented in Table 4.1. Moreover, the table displays the KPIs which are relevant to the Milan Malpensa Airport demonstration, the respective objective (O), the initial targeted values of KPIs, the final assessed values of KPIs and illustrate whether these KPIs final (current) values reached the target providing respective justification and comments where needed. Furthermore, the formula calculation for the KPIs final estimation is presented wherever is required.

In the following, the KPIs related to the Milan Malpensa Airport demonstration are presented and a brief description about the assessment is provided:

SATIE KPI #Number of different attacks implemented in the demonstration of the final scenarios.

This measurement includes all cyber and physical attacks conducted in all SATIE Airports' demonstrations. Under this paragraph, the cyber and physical attacks implemented during the Milan Malpensa Airport's Scenario #3 are considered, as well as the total number of different attacks considering data belonging to the other demonstrations.

Regarding the demonstration of Scenario #3, five (5) cyber-attacks were performed:

- Spear phishing email crafted to targeted AOCC employees with malware attached;
- Malware spreads through the network to infect the RMS and M-AIS;
- Malware allows the attacker to modify data in the RMS and M-AIS systems to mix and mess the passengers' boarding gates (Schengen boarding gates → Non-Schengen boarding gates);
- Flight Information Display System compromised through the RMS system and displayed wrong and confusing information to the passengers in the terminal;
- Malware allows the attacker to modify data in the M-AIS system to change the aircraft stands on the apron;

and the following one (1) physical attacks:

- The attacker trying to enter the AOCC room. With a stolen AOCC employee badge, the attacker tries to enter the AOCC room by swiping the badge over the access control machine.

Because the Milan Malpensa demonstration event was the last event to take place from all three demonstrations, we can refer to the data from the Athens and Zagreb demonstrations in order to conclude the fulfilment of this KPI. In the deliverables reporting the demonstrations which took place in the other airports (Zagreb - D6.4 (3) and Athens - D6.5 (4)), we can collect the information that in Athens, there were 8 cyber-attacks and 2 physical attacks demonstrated, while in the Zagreb demonstration, there were 7 cyber-attacks showcased. Therefore, there was a number of 17 different attacks demonstrated in the first two demonstration events, which adds up with the 6 different attacks demonstrated in the Milan Malpensa Airport, resulting in 23 different attacks implemented in all 3 demonstrations altogether.

SATIE KPI #Number of capabilities demonstrated (Demo SEA).

For the current KPI estimation, all Innovation Elements (IEs) that were illustrated during the Scenario #3 execution in the Milan Malpensa Airport demonstration event are enlisted below:

IE1: Risk assessment platform with cyber-physical threat analysis (RIS);

IE4: Unified Access Control (UAC) with correlation between Biometric data and access tokens;

IE8: Cyber Threat Detection Systems - Malware Analyser and ALCAD - on critical networks and business processes;

IE9: Correlation Engine for cyber-physical threat detection;

IE10: Data analytics for forensics investigation and fast recovery (SMS-I);

IE11: Impact Propagation Tools (IPT) - Impact Propagation Simulation (IPS) - for anticipated impact assessment;

IE12: Cyber-physical Incident Management Portal (IMP) for enhanced SOC awareness;

IE13: Crisis Alerting System (CAS) for coordinated security and safety responses;

IE14: Emulation platform for improved cyber defence strategies.

As a result, nine (9) capabilities were demonstrated in the Milan Malpensa Airport event, reaching the target, which was to perform with at least nine of them.

SATIE KPI #Number of participants trained.

This KPI value addresses the number of participants from Milan Malpensa Airport trained to be able to use SATIE Toolkit. In particular, three SOC operators, two AOC operators and one observer were trained, so the final value of KPI was six which reached targeted three.

SATIE KPI #Number of security practitioners/ participants answering a questionnaire (Demo SEA).

This KPI value was calculated according to the evaluation questionnaire responders, defined in section 4.2. Sixteen (16) participants from the security industry were answering the questionnaires, which successfully overpassed the targeted of three (3).

SATIE KPI #Number of project external demo visitors (Demo SEA) online/physical.

To assess the current value of this KPI, all external demonstration visitors (physical and online visitors) are considered. Unfortunately, due to COVID-19 security and safety indications and travel restrictions, together with the available space in the main demonstration room, only eleven (11) invitees were able to join the event physically. In addition to that, external demonstration visitors were twenty-six (26) people who attended online.

Table 4.1: Current values of the KPIs with respect to the Milan Malpensa demonstration event

KPI	Objective	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
Number of different attacks implemented in the demonstration of the final scenarios.	O8	23	23	Yes	This calculation includes data from the previous two demonstrations events, which took place in Athens and Zagreb. They had a total of 17 different attacks demonstrated, and adding the 6 Milan Malpensa demonstrated attacks, the final result is 23. This KPI refers to the total amount of different attacks implemented, not just the ones from the Milan Malpensa demonstration.	All attacks (cyber or physical) implemented in the Milan Malpensa demonstration event, plus the different attacks implemented in the previous two demonstrations in Athens and Zagreb.
Number of capabilities demonstrated (Demo SEA)	O8	9	9	Yes	The Milan Malpensa demonstration event presented nine (9) Innovation Elements which fulfil this specific KPI.	Counting how many SATIE Innovation Elements (IEs) were demonstrated during the Milan Malpensa Airport event.
Number of participants trained (Demo SEA)	O8	3	6	Yes	3 SOC operators, 2 AOC operators and 1 observer were trained for the Milan Malpensa Airport demonstration.	3 roles were trained: AOC, SOC and Observer.
Number of security practitioners/participants answering a	O8	3	16	Yes	The Milan Malpensa demonstration overpassed successfully this KPI's target, having many physical	Security practitioners were counted as individuals and not per

KPI	Objective	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
questionnaire (Demo SEA)					attendees with a high rate of effectively answering the questionnaire, as well as many new (not present to the other two demonstrations) online participants.	organisation.
Number of project external demo visitors (Demo SEA) online/physical	O8	20 when online / 15 when physical	26 online / 11 physical	Yes	Due to COVID-19 security and safety protocols and to the respective travel restrictions and limitations, there were only eleven (11) physical external visitor in the Milan Malpensa Airport demonstration event, and twenty-six (26) online present externals.	Project external demo visitors were counted as individuals and not per organisation.

4.2 Evaluation questionnaire results

In this section, the participants subjective assessment of the SATIE Solution as shown during the Milan demonstration is presented. A subset of the questions already asked during the simulation validations (described in D6.2 (1) and D6.3 (2)) was used and – if needed - adapted to the demonstration (questions addressing parts of the SATIE solution not shown during the demonstration have been omitted from the questionnaires compared to the simulation validation questionnaires). The questionnaire was the same as the one used in the Athens and Zagreb demonstrations and described in the respective reports D6.4 (3) and D6.5 (4). During the event, only participants external to the project were asked to answer the questionnaires. Hence, the results presented here are only from these "independent external" participants. The term of "independent external" participant is defined as any demonstration participant that **was *not* a SATIE internal personnel** or a participant from any company/institution invited that **did *not* have a strong connection to the SATIE project before the demonstration event**. Thus, the results consist of non-biased opinions. The affiliation of participants can be seen in Table 4.6. The total number of considered questionnaire responses was N=16, which is considered as a very good value because it is the highest from all three demonstrations. The evaluation of operators was already performed during the simulation validations and is described in D6.3 (2) and not included in this report. Table 4.2 presents an overview over the results of the answers of the participants. The measurement scale used for the evaluation questionnaire was ranging from 1 (representing the worst level) till 7 (representing the best level) in agreement with the statements presented in Table 4.2.

Table 4.2: Results of evaluation questionnaire responders

Statement	Average	Minimum	Maximum	Standard deviation	No. of Participants
The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	6.27	5	7	0.88	15
The SATIE Solution is an excellent way to monitor and raise security alerts.	6.44	5	7	0.81	16
The SATIE Solution provides all relevant information.	5.71	4	7	0.99	14
The SATIE Solution enables a faster detection of cyber threats compared to current systems.	5.94	4	7	0.93	16
The SATIE Solution enables a faster detection of physical threats compared to current systems.	5.80	3	7	1.32	15
The SATIE Solution enables a faster response to cyber threats compared to current systems.	5.81	4	7	1.05	16
The SATIE Solution enables a faster response to physical threats compared to current systems.	5.67	3	7	1.35	15
The use of the SATIE Solution increases the efficiency compared to current systems.	6.13	5	7	0.74	15
I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	6.07	4	7	0.92	14
The SATIE Solution is innovative compared to others on the market.	5.93	4	7	1.27	14
I think the SATIE Solution will boost airports’ revenues.	5.07	1	7	1.82	14
I think airports will like to secure their systems with the SATIE Solution.	5.64	4	7	1.01	14
I think that the shown scenario(s) were suitable to illustrate the SATIE Solution’s capabilities.	6.00	4	7	0.89	16
The SATIE Solution has good usability.	6.13	4	7	0.81	16
Summary	5.90	3	7	1.06	

As shown in Table 4.2 and Table 4.3 the agreement to the statements were high. The SATIE Solution was considered to be a significant improvement to current security-monitoring systems, was rated as innovative and an excellent way to monitor and raise security Alerts with a good usability. It was agreed that the SATIE Solution provides all relevant information and enables both a faster detection of cyber and physical threats. This idea is sustained also by Table 4.4, which presents in the users' top picks systems used primarily by operators, but also detector systems. Besides a faster detection, also the response to cyber and physical attacks was rated as faster compared to current systems. The participants agreed to the statement that the SATIE Solution increases the efficiency compared to current systems. Slightly lower, but still agreement, could be observed for the statement regarding the ease of integrating the SATIE Solution with necessary airport systems and the statement that the SATIE solution will boost revenues for airports. The shown scenarios at Milan demonstration were rated as suitable to illustrate SATIE Solution´s capabilities. Concluding, the participants agreed that airports will like to secure their systems with the SATIE Solution.

The participants had the opportunity to choose Innovation Elements which stood out for them and were offered a free text field to explain their choice (see Table 4.4 for all details). The Unified Access Control and the CAS received the highest frequency with N=6. For the CAS it was highlighted that all Incidents are orchestrated and collected at one point and its early warning capabilities and collaboration features, resulting in fast responses to Incidents. The Anomaly Detection on Passenger Records was rated as extremely useful and clearly addressing a known asymmetric current threat. The ALCAD was stated to be a fascinating solution to monitor and analyse network traffic and a unique solution that will allow to analyse the network traffic of airport applications and intercept any cyber-attack. The correlation engine was highlighted as an excellent example how to make use of AI/ML for decision-making processes and the SMS-I was valued for being a single point of control to manage cyber and physical Alerts and Incidents. Additionally, the IMP was considered to deliver excellent situation awareness and offering several options for further analysis. One participant highlighted that "it is excellent to be able to integrate the BIA into a single management platform. It is a true innovation in the management of how cyber threats spread to the organization's assets and evaluates the impact caused on the services and on the organization's critical business objectives".

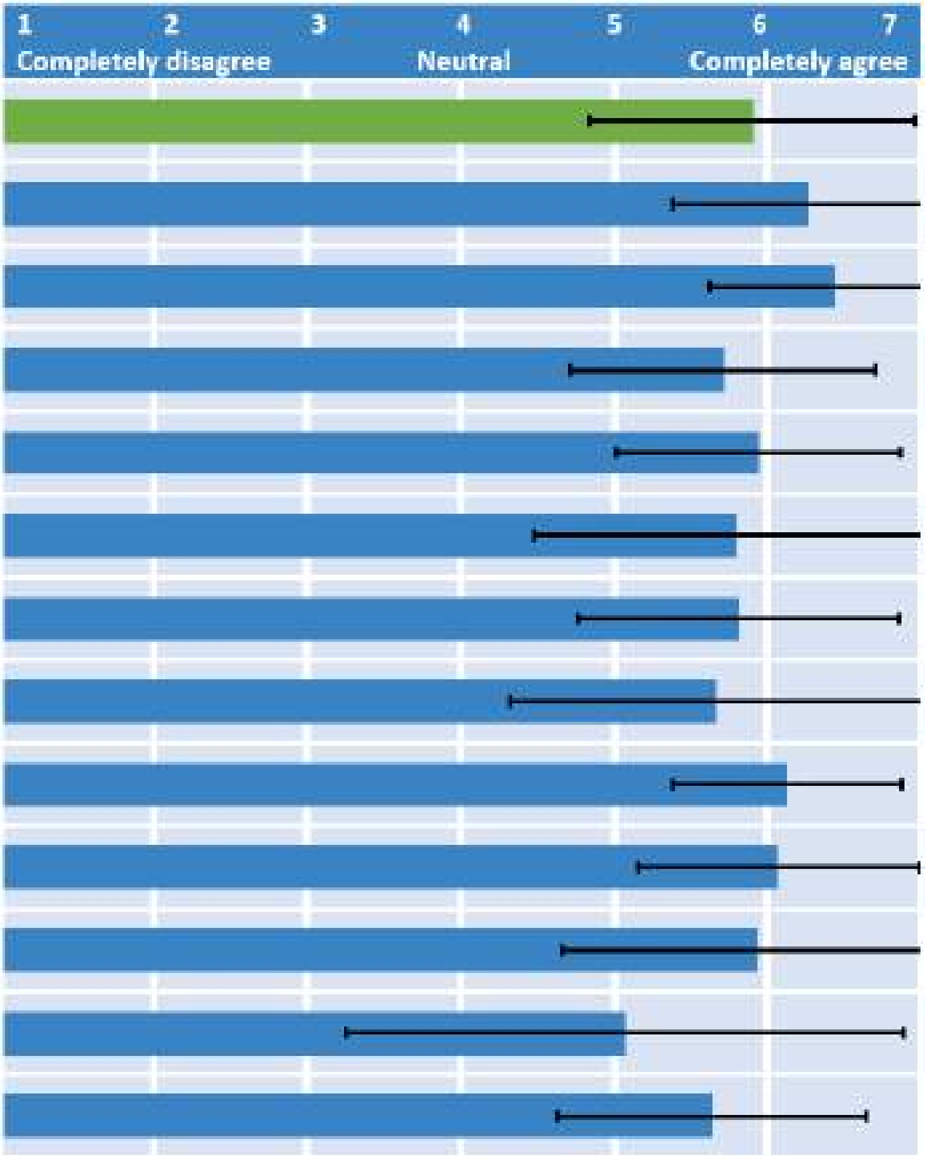
Unfortunately, it has to be noted that the IPS was by mistake not included in the list of IEs for this question. Hence, the responders have not been able to select IPS as IE which stood out for them. Therefore, no feedback was given for IPS. This is also applicable for this question in the demonstration reports of Zagreb (D6.4 (3)) and Athens (D6.5 (4)), and the Practitioners Workshop (D7.3 (10)), as the same questionnaire was used.

In an additional question, all participants had the opportunity to add further remarks and general feedback (see Table 4.5 for a complete summary). "It would be interesting to use this solution in another CI and see if it benefits" was mentioned as a suggestion for future work and it was recommended to "have the recording of the demos available in order to show it to other colleagues involved in the process". One comment mentioned that the "system must be applied at cargo facilities and tarmac check points. Furthermore, it should be applicable in any door access such as lost & found or any other vulnerable point of entrance into a sterile area.". Additionally, the integration with different applications was highlighted.

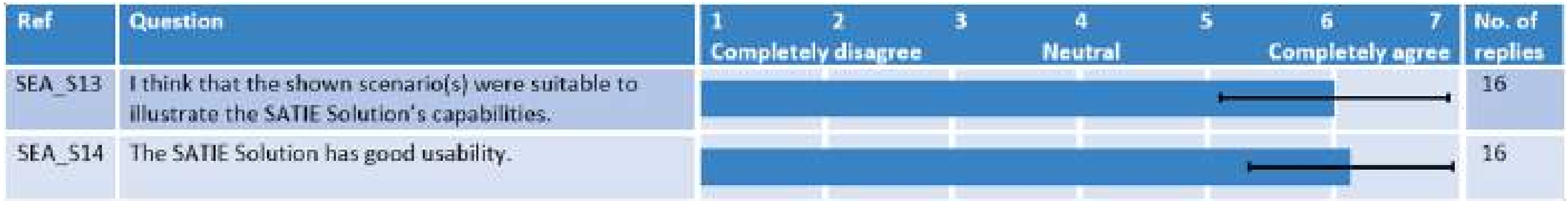
Besides that, the overwhelming amount of feedback was very positive. According to the participants the demonstration at Milan Airport showed that the SATIE Solution is a very robust suite of features that (when integrated properly, managed correctly and used efficiently) can be a significant force multiplier for airports to ensure resilience and security. Furthermore, participants wrote that the SATIE project represents a great opportunity for the cyber protection of airports. The participant argues that it will be important to be able to deepen the solution and then be able to access the services that will be provided by SATIE. One participant even asked: "what are the elements/tools that can be commercialized individually and within the next 6 months?" which really demonstrates the high interest in the solutions SATIE offers.

The questions asked during the demonstration event were an adapted subset of the ones presented to the simulation validation participants and exactly the same that have been asked to the participants at the Athens and Zagreb demonstrations. This offered the opportunity to compare the results of the Milan demonstration with the results from the Athens and Zagreb demonstration, and the simulation validation activities. Even though the participants were different regarding their operational background and experience (see Table 4.6) in this demonstration and compared to the other demonstration and simulation validations, the responses received were similar. The results from Athens, Zagreb and Milan demonstrations were strikingly similar despite the different scenarios presented and the different participants. This strengthens the assumption of representativeness of the results and is an indication of the validity and reliability of the obtained results. Both, operational experts trained to use the novel SATIE Tools, and security experts just observing the demonstration attack scenarios and the actions of SATIE system operators, evaluated the SATIE Solution very positive. The biggest area for improvements expressed by all expert groups was the integration of the SATIE Tools with the current airport systems. In conclusion, however, the similarities of answers and the positive feedback in the different groups of participants are an encouraging reinforcement of the SATIE Solution benefits.

Table 4.3: Statistical results concerning the evaluation questionnaire answers



Ref	Question	No. of replies
Statements	Overall	
SEA_S01	The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	15
SEA_S02	The SATIE Solution is an excellent way to monitor and raise security alerts.	16
SEA_S03	The SATIE Solution provides all relevant information.	14
SEA_S04	The SATIE Solution enables a faster detection of cyber threats compared to current systems.	16
SEA_S05	The SATIE Solution enables a faster detection of physical threats compared to current systems.	15
SEA_S06	The SATIE Solution enables a faster response to cyber threats compared to current systems.	16
SEA_S07	The SATIE Solution enables a faster response to physical threats compared to current systems.	15
SEA_S08	The use of the SATIE Solution increases the efficiency compared to current systems.	15
SEA_S09	I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	14
SEA_S10	The SATIE Solution is innovative compared to others on the market.	14
SEA_S11	I think the SATIE Solution will boost airports' revenues.	14
SEA_S12	I think airports will like to secure their systems with the SATIE Solution.	14



Ref	Question	1 Completely disagree	2	3	4 Neutral	5	6	7 Completely agree	No. of replies
SEA_S13	I think that the shown scenario(s) were suitable to illustrate the SATIE Solution's capabilities.								16
SEA_S14	The SATIE Solution has good usability.								16

Table 4.4: Innovation Elements' feedback

Question	"Which of the Innovation Elements (IE) stood out for you, and why?"	
Innovation Element	**Frequency**	**Reasons**
Unified Access Control (UAC)	6	
Crisis Alerting System (CAS)	6	A) All alerts are orchestrated and collected at one point, comparable to a digital CERT. B) Early warning capabilities and collaboration/comms features. C) Enables fast response to incidents
Anomaly Detection on Passenger Records (PAD)	3	Extremely useful and clearly addresses a known asymmetric current threat
Traffic Management Intrusion and Compliance System (TraMICS)	3	
Malware Analyser	3	
Application Layer Cyber Attack Detection (ALCAD)	3	A) Fascinating solution to monitor and analyse network traffic. B) Unique solution that will allow to analyse the network traffic of airport applications and intercept any cyber-attacks.
Correlation Engine	3	Excellent example how to make use of AI/ML for decision-making processes
Investigation Tool (SMS-I)	3	Single point of control to manage cyber and physical alerts and incident
Incident Management Portal (IMP)	3	Excellent situational awareness and several incident options for further analysis
Risk Integrated Service (RIS)	2	
Vulnerability Intelligence Platform (VIP)	2	
Secured Communication on the BHS (ComSEC)	2	

Question	"Which of the Innovation Elements (IE) stood out for you, and why?"	
Innovation Element	**Frequency**	**Reasons**
Secured ATM Services	2	
Business Impact Assessment (BIA)	2	It is excellent to be able to integrate the BIA into a single management platform. It is a true innovation in the management of how cyber threats spread to the organization's assets and evaluates the impact caused on the services and on the organization's critical business objectives.
Digital Twin of the Baggage Handling System (BHS)	2	
Gestion Libre de Parc Informatique (GLPI)	1	
Business Process-based Intrusion Detection System (BP-IDS)	1	
CyberRange	1	

Table 4.5: General feedback and suggestions

Question	"Is there anything else you would like to mention about the SATIE Solution?"
Type of feedback	**Feedback answers**
Improvement proposal	I am curious if the solution will be used further and if there is an interest in further maintenance and in implementing features. It would be interesting to use this solution in another CI and see if it benefits.
Positive reinforcement	Integration with different applications
Improvement proposal	It would be useful to have the recording of the demos in order to show it to other colleagues involved in the process
Positive reinforcement	Overall SATIE is a very robust suite of features that in my opinion (when integrated properly, managed correctly and used efficiently) can be a significant force multiplier for airports to ensure resilience and security.
Positive reinforcement	The project represents a great opportunity for the cyber protection of airports. it will be important to be able to deepen the solution and then be able to access the services that will be provided by you

Question	**"Is there anything else you would like to mention about the SATIE Solution?"**
Type of feedback	**Feedback answers**
Improvement proposal	The system must be applied at cargo facilities and tarmac check point. Furthermore, it should be applicable in any door access such as lost & found or any other vulnerable point of entrance into a sterile area.
Positive reinforcement	There is nothing I'd like to add.
Positive reinforcement	What are the elements/tools that can be commercialized individually and within the next 6 months?

Table 4.6: Affiliation of participants

Question	**“Please choose the type of organization you work in.”**
Types of organisation	**Number of participants**
Governmental Authority	1
Regulatory Authority	2
Research/Academic	4
Airline	1
Airport	4
Consulting	2
Transport	2
Total	**16**

5 Conclusion

The SATIE Project aims to create a holistic, unified toolkit for cyber-physical threat prevention, detection and mitigation for SOC and AOC operators in airport environments. The platform combines, into a unique system, tools that collect information in real-time about various systems such as passenger and baggage data, speaker recognition in controller-pilot radio communication, existing vulnerabilities of airport assets, how threats can propagate through the assets, suspicious network activity, face recognition when requesting authentication through access control, and many others. The innovative aspect of this project is to bring such diverse information together, particularly correlating physical and cyber information. In SATIE, cyber and physical security are handled with the same priority and tools operated on multiple, fully integrated levels.

The SATIE demonstrations (the three of them: Athens, Zagreb and Milan Malpensa) have shown that a cyber threat cannot only transform into a different cyber threat through connected systems, but cyber threats can also transform themselves into physical threats, and vice versa. The examples shown emphasize the need for a combined cyber-physical security system such as SATIE, so that, the operations and security personnel at an airport can cooperate with the IT security personnel. In this way, they both have a full situation awareness and are able to understand quicker when an incident is occurring.

The current report presents the main objective of the Milan Malpensa Airport demonstration, the preparation activities for the event, the overview of the event, the cyber and physical infrastructure deployed, a detailed step-by-step description of the scenario, the corresponding technical operations and the SATIE involved tools response.

During the Milan Malpensa demonstration event, both the SOC and AOC operators had the possibility to test and evaluate the SATIE Solution through a real operational scenario. The outcomes of this trial represent a positive reinforcement for SATIE, after a careful analysis of the feedback received from the participants (section 4.2).

In the course of the Milan Malpensa demonstration, the IT security specialists (SOC operators) and personnel assigned to the management and control of the airport operations (AOC operators) successfully performed a model of cooperation analysing and declining the presence of uncommon and possibly dangerous situations, solving them by taking actions to guarantee the correct functioning of the airport system.

It has been shown that this kind of synergetic action permits the detection of a complex, multiple attack that might become particularly critical for the regular exercise of airport activities, often with interference on security and safety issues.

In the course of the demonstration the cooperation between SOC operators and AOC operators was made more efficient by two fundamental elements: I) the standardization of the languages adopted by simplifying those that are too technical; II) the active personal involvement of the individual reference persons belonging to the SOC or AOC entity.

It is important to make a premise here: The mitigation measures adopted to alleviate or even eliminate the threats depends on the airport operator's understanding of the severity of the incident, as well as their speed to contact and inform necessary airport entities to then react. This communication chain varies according to the procedures described by each airport's applicable regulations and manuals.

SATIE bridges the gap between the ICT world and the operations world. The innovation with SATIE is that it is not only an ICT decision support tool that reveals a cyber or physical or combined threat in real time, but a solution that establishes a new way of communication in real time. As described above, that was perfectly exemplified during the Milan Malpensa demonstration, in the course of the interaction between the ICT and Operations departments, as well as during the real-time collaboration between the AOC operators and the airport's first-responders.

6 References

1. **SATIE Project.** *D6.2 - Test, validation and demonstration scenarios.* 2020.

2. —. *D6.3 - Test and validation results on the simulation platform.* 2021.

3. —. *D6.4 - Report about demonstration and results in the Zagreb Airport.* 2021.

4. —. *D6.5 - Report about demonstration and results in the Athens Airport.* 2021.

5. —. *D7.2 - Training Handbook.* 2021.

6. —. *D6.1 - Simulation platform and integrated SATIE Solutions.* 2020.

7. —. Security of Air Transport Infrastructure of Europe. [Online] https://satie-h2020.eu/.

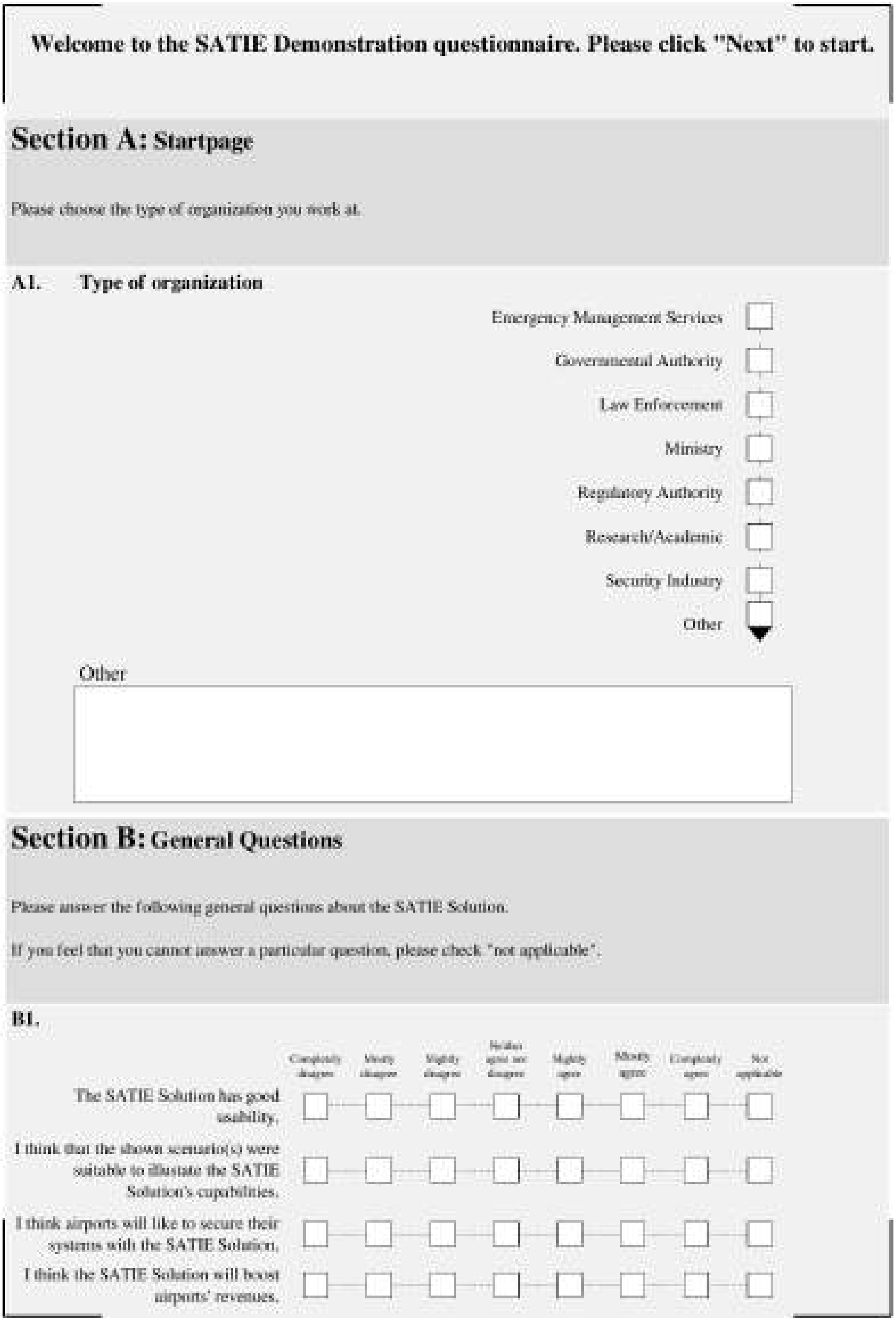
8. **Köpke, C., et al.** *Security and Resilience for Airport Infrastructure.* s.l. : ESREL 2020 PSAM 15, 2020.

9. **SATIE Project.** *D2.3 - Cyber-physical risk analysis.* 2020.

10. —. *D7.3 - Best practices for updating airport security standard and policies.* 2021.

11. —. *D4.1 - Specification of data exchanges, interfaces and log semantic.* s.l. : https://cordis.europa.eu/project/id/832969/results, 2020. Project deliverable.

7 Annex - Evaluation questionnaire



Welcome to the SATIE Demonstration questionnaire. Please click "Next" to start.

Section A: Startpage

Please choose the type of organization you work at.

A1. Type of organization

Emergency Management Services □

Governmental Authority □

Law Enforcement □

Ministry □

Regulatory Authority □

Research/Academic □

Security Industry □

Other □

Other

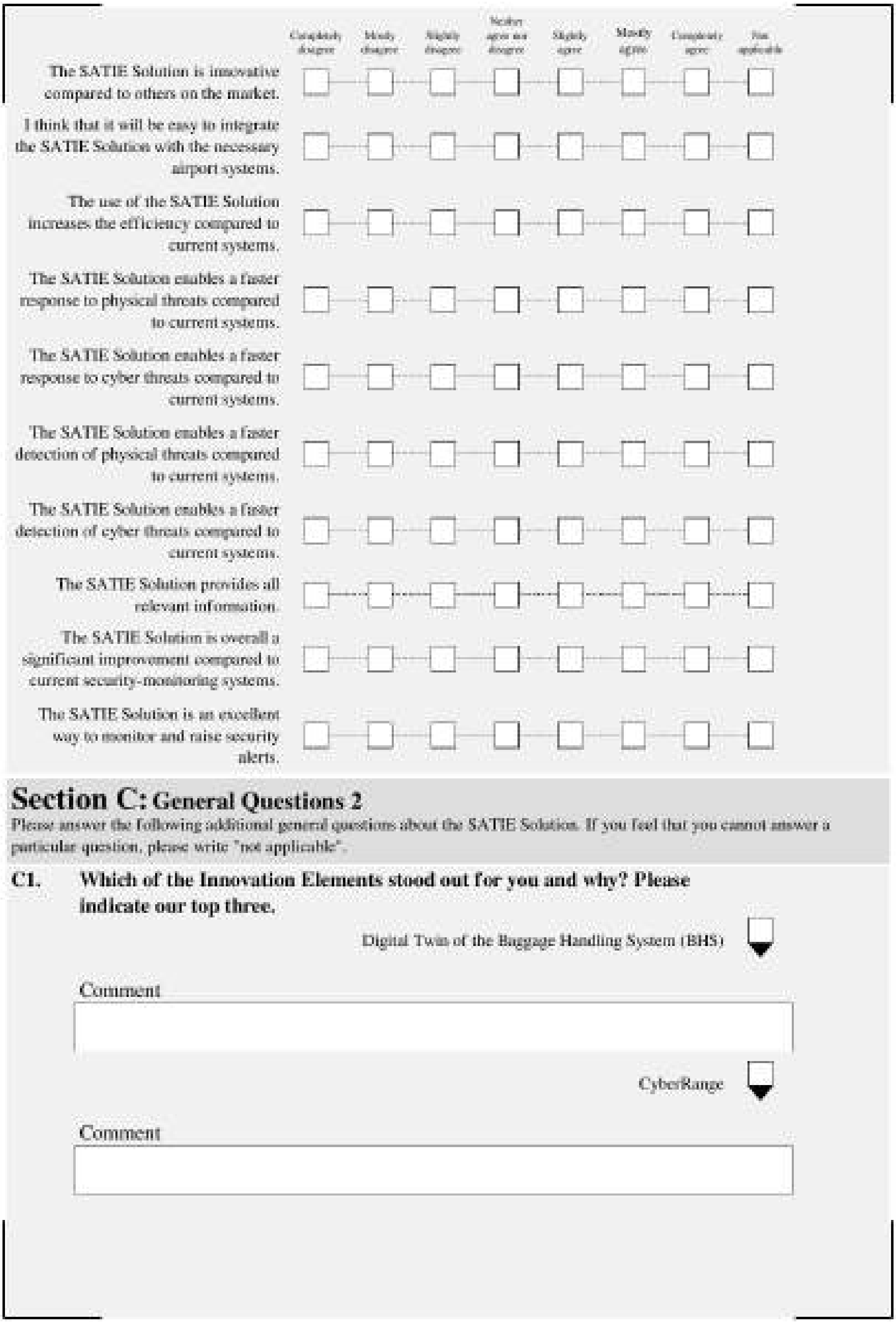
Section B: General Questions

Please answer the following general questions about the SATIE Solution.

If you feel that you cannot answer a particular question, please check "not applicable".

B1.

	Completely disagree	Mostly disagree	Slightly disagree	Neither agree nor disagree	Slightly agree	Mostly agree	Completely agree	Not applicable
The SATIE Solution has good usability.	□	□	□	□	□	□	□	□
I think that the shown scenario(s) were suitable to illustrate the SATIE Solution's capabilities.	□	□	□	□	□	□	□	□
I think airports will like to secure their systems with the SATIE Solution.	□	□	□	□	□	□	□	□
I think the SATIE Solution will boost airports' revenues.	□	□	□	□	□	□	□	□



	Completely disagree	Mostly disagree	Slightly disagree	Neither agree nor disagree	Slightly agree	Mostly agree	Completely agree	Not applicable
The SATIE Solution is innovative compared to others on the market.	□	□	□	□	□	□	□	□
I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	□	□	□	□	□	□	□	□
The use of the SATIE Solution increases the efficiency compared to current systems.	□	□	□	□	□	□	□	□
The SATIE Solution enables a faster response to physical threats compared to current systems.	□	□	□	□	□	□	□	□
The SATIE Solution enables a faster response to cyber threats compared to current systems.	□	□	□	□	□	□	□	□
The SATIE Solution enables a faster detection of physical threats compared to current systems.	□	□	□	□	□	□	□	□
The SATIE Solution enables a faster detection of cyber threats compared to current systems.	□	□	□	□	□	□	□	□
The SATIE Solution provides all relevant information.	□	□	□	□	□	□	□	□
The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	□	□	□	□	□	□	□	□
The SATIE Solution is an excellent way to monitor and raise security alerts.	□	□	□	□	□	□	□	□

Section C: General Questions 2

Please answer the following additional general questions about the SATIE Solution. If you feel that you cannot answer a particular question, please write "not applicable".

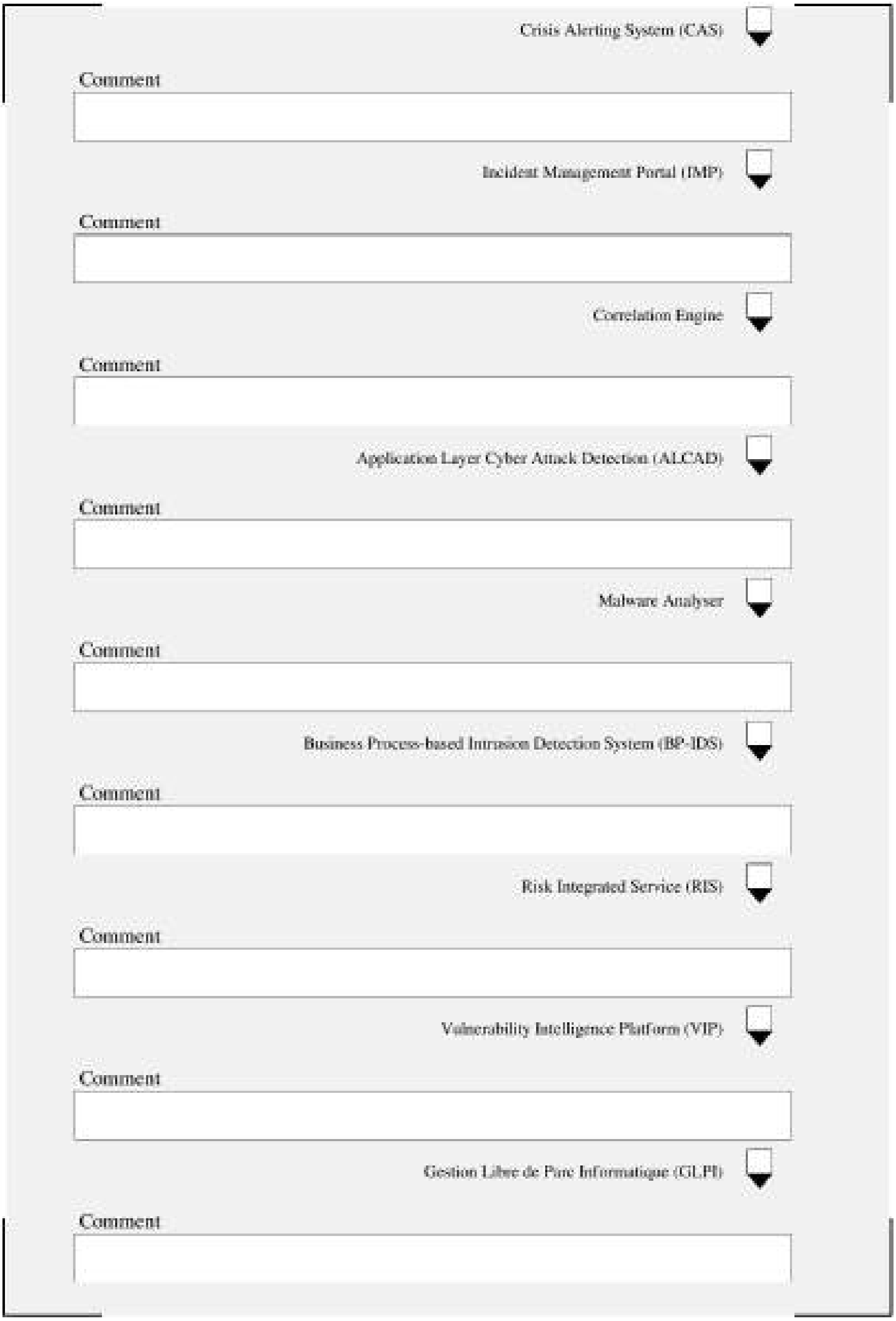
C1. Which of the Innovation Elements stood out for you and why? Please indicate our top three.

Digital Twin of the Baggage Handling System (BHS) ▼

Comment

CyberRange ▼

Comment



Crisis Alerting System (CAS) ▼

Comment

Incident Management Portal (IMP) ▼

Comment

Correlation Engine ▼

Comment

Application Layer Cyber Attack Detection (ALCAD) ▼

Comment

Malware Analyser ▼

Comment

Business Process-based Intrusion Detection System (BP-IDS) ▼

Comment

Risk Integrated Service (RIS) ▼

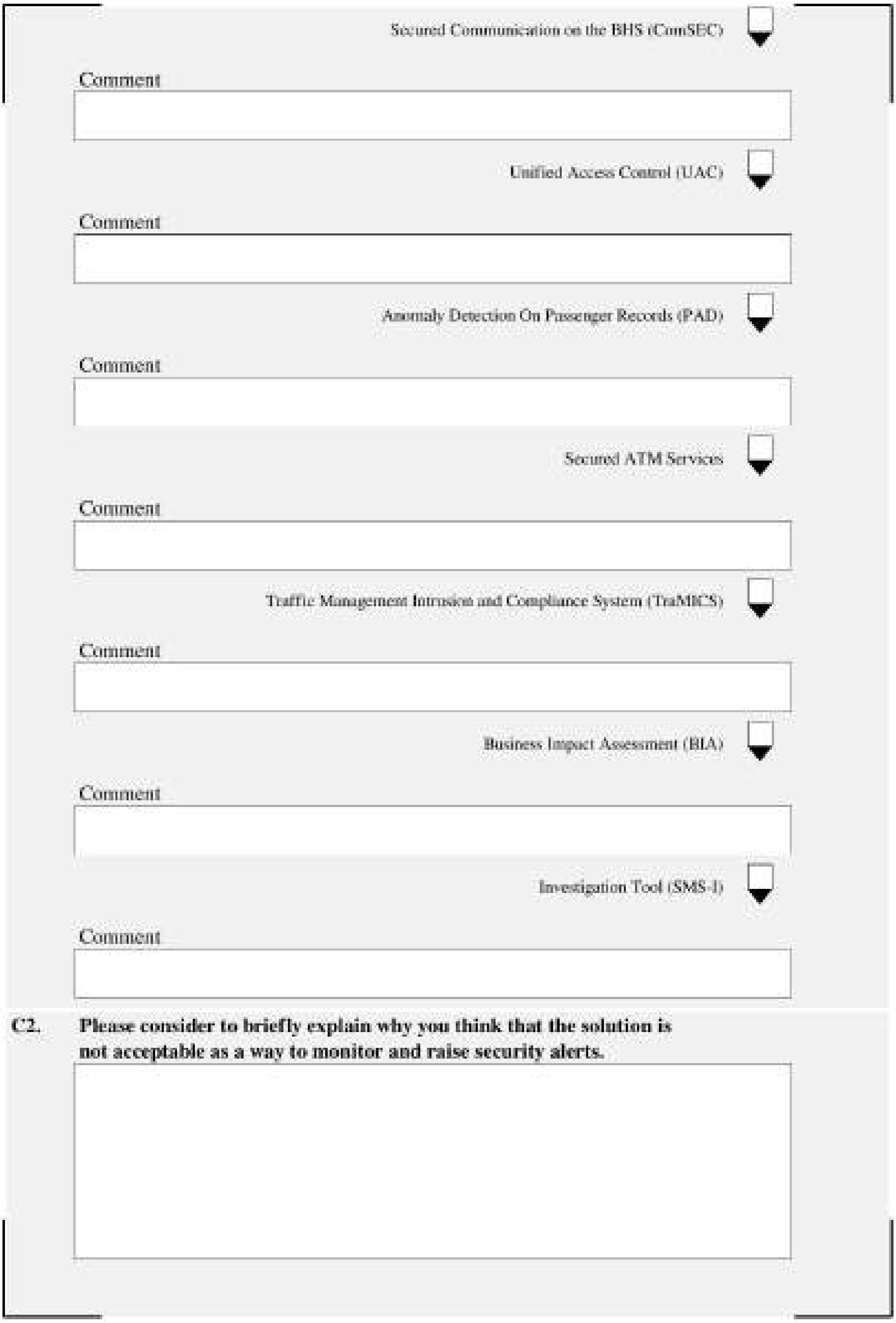
Comment

Vulnerability Intelligence Platform (VIP) ▼

Comment

Gestion Libre de Parc Informatique (GLPI) ▼

Comment



Secured Communication on the BHS (ComSEC) ▼

Comment

Unified Access Control (UAC) ▼

Comment

Anomaly Detection On Passenger Records (PAD) ▼

Comment

Secured ATM Services ▼

Comment

Traffic Management Intrusion and Compliance System (TraMICS) ▼

Comment

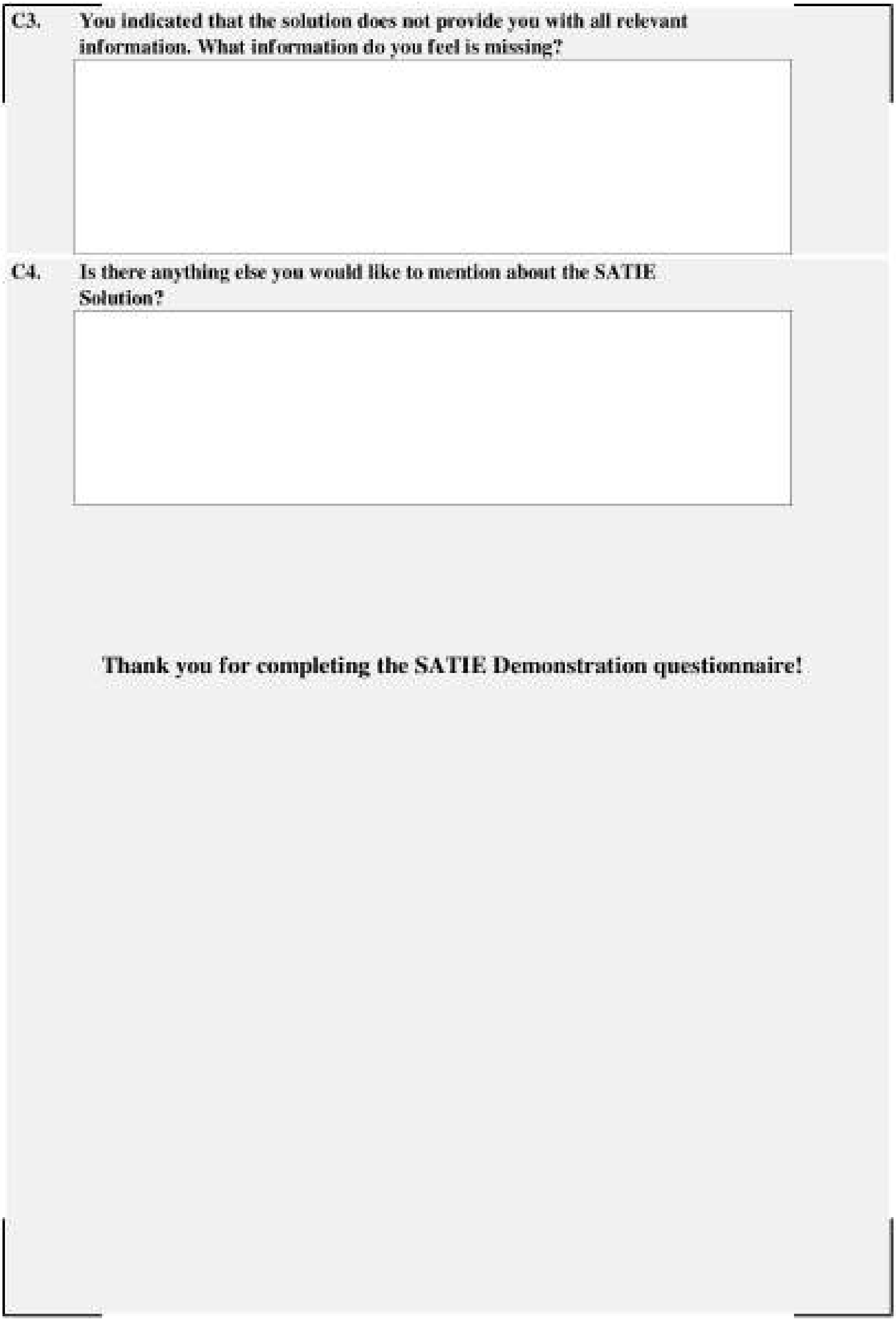
Business Impact Assessment (BIA) ▼

Comment

Investigation Tool (SMS-I) ▼

Comment

C2. Please consider to briefly explain why you think that the solution is not acceptable as a way to monitor and raise security alerts.



C3. You indicated that the solution does not provide you with all relevant information. What information do you feel is missing?

C4. Is there anything else you would like to mention about the SATIE Solution?

Thank you for completing the SATIE Demonstration questionnaire!