Security of Air Transport Infrastructures of Europe

D6.5 –Report about demonstration and results in Athens Airport

Deliverable Number	D6.5
Author(s)	AIA, IDE, TLB, ITTI, FHG, SAT, ACS, ISEP, DGS, KEMEA, DLR, ERI, SEA, ZAG
Due/delivered Date	M28/2021-08-31
Reviewed by	DLR, KEMEA, ACS
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	Nikolaos Papagiannopoulos (AIA)	Content contributor
2	Eleni Maria Kalogeraki (AIA)	Content contributor
3	Tim Stelkens-Kobsch (DLR)	Content contributor
4	Nils Carstengerdes (DLR)	Content contributor
5	Andrei-Vlad Predescu (DLR)	Content contributor
6	Eftichia Georgiou (KEMEA)	Content contributor
7	Ilias Gkotsis (KEMEA)	Content contributor
8	Vasiliki Mantzana (KEMEA)	Content contributor
9	Kelly Burke (DGS)	Content contributor
10	Corinna Köpke (FHG)	Content contributor
11	Thomas Oudin (ACS)	Content contributor
12	Thomas Mauger (IDE)	Content contributor
13	Sebastien Clavert (IDE)	Content contributor
14	Eva Catarina Gomes Maia (ISEP)	Content contributor
15	Leonidas Perlepes (SATWAYS)	Content contributor
16	David Lancelin (ACS)	Technical Review
17	Vasileios Kazoukas (KEMEA)	Security Review
18	Meilin Schaper (DLR)	Quality Review

Document revisions

Revision	Date	Comment	Author
V0.01	2021-06-22	Initial draft	Nikolaos Papagiannopoulos
V0.02	2021-06-22	Contribution to the inital draft	Tim Stelkens-Kobsch, Nils Carstengerdes, Andrei-Vlad Predescu
V0.03	2021-07-09	Content added to section 2	Eleni-Maria Kalogeraki
V0.04	2021-07-12	Content added to section 2	Eftichia Georgiou, Vasiliki Mantzana
V0.05	2021-07-12	Content added to section 3.9	Kelly Burke
V0.06	2021-07-12	Content added to section 3.6	Corinna Köpke
V0.07	2021-07-15	Content added to section 4	Andrei-Vlad Predescu, Nils Carstengerdes
V0.08	2021-07-27	Content added to section 2	Eleni-Maria Kalogeraki
V0.09	2021-07-27	Content added to section 3.9	Kelly Burke
V0.10	2021-07-31	Content added to section 3.5	Thomas Mauger
V0.11	2021-08-02	Content added to section 3.6	Corinna Köpke
V0.12	2021-08-03	Content added to sections 3.1, 3.2 and 3.3	Thomas Oudin
V0.13	2021-08-04	Content added to section 2	Eftichia Georgiou, Vasiliki Mantzana, Ilias Gkotsis
V0.14	2021-08-04	Content added to section 3.8	Eva Catarina Gomes Maia
V0.15	2021-08-05	Content added to section 2 and section 4. Formatting issues fixed in the whole document.	Eleni-Maria Kalogeraki
V0.16	2021-08-06	Intermediate review and comments	Meilin Schaper
V0.16	2021-08-06	Content added to section 3.4	Sebastien Clavert
V0.17	2021-08-11	Corrections and edits in section 2.2.2, section 3.1, section 3.2, section 3.3 and section 4.1	Thomas Oudin
V0.18	2021-08-11	Content added to section 2 and section 4. Formatting issues fixed in the whole document.	Eleni-Maria Kalogeraki
V0.19	2021-08-13	Content added to section 3.7	Leonidas Perlepes

Revision	Date	Comment	Author
V0.20	2021-08-18	Ready for review version.	Eleni-Maria Kalogeraki
V0.30	2021-08-23	Final technical check and approval for submission	David Lancelin, Technical Manager
V0.40	2021-08-27	Quality review	Andrei-Vlad Predescu, Meilin Schaper
V0.50	2021-08-30	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V1.0	2021-08-31	Final quality check and approval for submission	Tim Stelkens-Kobsch, Project Coordinator

Executive summary

The main objective of this deliverable is to report on the performance of the Athens Airport demonstration, which was carried out under real conditions; utilizing Athens Airport critical infrastructure. These scenarios incorporate a considerable number of potential cyber and physical attacks that could cause a devastating impact to airports operations and people's safety, defined in T6.2.

Furthermore, the current deliverable is the outcome of T6.4 presenting information regarding the overall preparation and procedures of the demonstration (e.g. end-users trained for the demonstration and the experience they obtained through the use of the SATIE interface during the performance of the two threat scenarios, logistics and business and technical operations undertaken for the demonstration, etc.), the airport systems engagement in the demonstration and the systems integration to the SATIE solution through an emulation platform, the SATIE Tools that were demonstrated and evaluated through the execution of the two threat scenarios and the produced results, the evaluation and feedback received from external attendees and from interviews gained by end-users to refine the risk analysis.

Table of Content

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
ABC	Automated Border Control
ABM	Agent Based Model
AC	Access Control
ADPR	Anomaly Detection on Passenger Records
AOC	Airport Operations Centre
AODB	Airport Operational Database
CAS	Crisis Alerting System
CCTV	Closed-circuit television
CE	Correlation Engine
EU	European Union
EC	European Comission
FIDS	Flight Information Display system
GPO	Group Policy Object
HP	Hellenic Police
IE	Innovation Element
IMP	Incident Management Portal
IPS	Impact Propagation Simulation
KPI	Key Performance Indicator
LEA	Law Enforcement Agency
LED	Light-Emitting Diode
MA	Malware Analyser
MITM	Man-In-The-Middle
NOC	Network Operations Centre
OS	Operating System
PA	Public Announcement
PAD	Passenger Anomaly Detection
Q&A	Questions and Answers
RAT	Remote Administration Tool

Acronym	Definition
RIS	Risk Integrated Service
SATIE	Security of Air Transport Infrastructures of Europe
SMS	Short Message Service
SMS-I	Investigation Tool
SOC	Security Operations Centre
UAC	Unified Access Control
USB	Universal Serial Bus
VIP	Vulnerability Intelligence Platform
XML	Extensible Markup Language

1 Introduction

The SATIE Solution adopts a holistic approach towards threat prevention, detection, response, and mitigation which can help airports to address cyber and physical attacks to the protection of critical systems and people's safety. One of the most critical aspects of the SATIE project to illustrate and communicate its feasibility is the demonstration scenarios in different airport environments. The Athens Airport demonstration event was set up to implement this task and to create the opportunity to demonstrate the SATIE solution efficiency and collect feedback from end-users and airport's stakeholders and security practitioners according to their operational and security requirements.

The main objective of this deliverable is to report on the performance of the Athens Airport demonstration, which was carried out under real conditions; utilizing Athens Airport critical infrastructure. These scenarios incorporate a considerable number of potential cyber and physical attacks that could cause a devastating impact to airports operations and people's safety, defined in T6.2.

Furthermore, the current deliverable is the outcome of T6.4 presenting information regarding the overall preparation and procedures of the demonstration (e.g. end-users trained for the demonstration and the experience they obtained through the use of the SATIE interface during the performance of the two threat scenarios, logistics and business and technical operations undertaken for the demonstration, etc.), the airport systems engagement in the demonstration and the systems integration to the SATIE solution through an emulation platform, the SATIE Tools that were demonstrated and evaluated through the execution of the two threat scenarios and the produced results, the evaluation and feedback received from external attendees and from interviews gained by end-users to refine the risk analysis.

Due to the COVID-19 pandemic, which was followed by specific safety protocols and travel limitations, the Athens Airport demonstration was carried out as a hybrid (both cyber and physical event), nonetheless, it was only web attended by external participants.

2 Athens International Airport demonstration

The demonstration event in Greece were organized and coordinated by Athens International Airport (AIA) with the active involvement of KEMEA and the technical support of all the partners.

In this context, several training seminars and trial workshops were organized with operators and anyone else who expressed interest to try and validate the proposed SATIE Solution.

Targeting towards this direction, the current section describes all important issues that came out from the demonstration-specific operations performed in Greece.

Section 2.1 presents an overview of the Athens demonstration event. Section 2.2 describes the airport sites utilized during the Athens Airport demonstration, including event localization and logistics information (section 2.2.1), the Athens Airport's cyber and physical infrastructure used for the execution of the demonstration scenarios and the airport's environment integration with the SATIE Solution (section 2.2.2). Section 0 reflects all the operations that took place by the demonstration organisers, the technical participants, the engaged end-users (Security Operations Centre (SOC) and Airport Operations Centre (AOC)) operators and the related SATIE user interface they had access during the demonstration performance. Section 0 describes in detail the threat scenarios that were executed to demonstrate and validate the SATIE solution the roles of the players within the scenarios, the SATIE involved Tools that were utilized to address the cyber and physical attacks, the simulation and demonstration activities performed during the scenarios execution.

2.1 Demonstration overview

The SATIE Athens Demonstration event was carried out on the 11th of June, 2021 at the Athens International Airport (AIA) premises in Spata 19019 (postal code), Attica, Greece (Figure 2.1). Due to the COVID-19 health and safety protocols and travelling restrictions, it was a hybrid (virtual and physical) event, only web attended by external participants.

In the context of the Athens demonstration event, the end-users (AIA SOC and AOC operators with the Hellenic Police (HP) Automated Border Control (ABC) Officer) had been trained in using the SATIE Tools during the SATIE training days that took place remotely on the 23rd-24th of February 2021. The training was supported by a comprehensive training handbook (see SATIE D7.2) (1) and a simulation event, which occurred on the 26th of April, 2021 (see SATIE D6.3) (2). The scope of the training workshop was to get the SOC and AOC operators of the Athens Airport as well as the Hellenic Police ABC Officers familiarized with the SATIE Tools, in order to use them during the simulation and demonstration events. In April 2021, the validation of the SATIE Solution in the simulation environment was performed. Fifteen (15) participants from the three airports, including two SOC operators (Hellenic Police ABC officer and AIA) and one AOC operator from AIA along with supporting personnel of thirty (30) people from the project partners participated. Five complex cyber-physical threat scenarios in a different order for each airport were executed, thus, there were 15 run-throughs in total.

During the demonstration event in Athens Airport the trained SOC and AOC operators used and validated the SATIE Solution in the scope of two realistic cyber and physical attack scenarios (as described in detail in the following sections). AIA in collaboration with KEMEA, the Project Coordinator, and other SATIE partners communicated the Athens demonstration event to a considerable number of end-users (i.e. airport operators, stakeholders and individual experts) and motivated them to participate in the testing and evaluation 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 has been collected so far by networking in conferences and workshop events.
- Engaging partners and stakeholders to communicate with their contact points, motivating potential end-users.

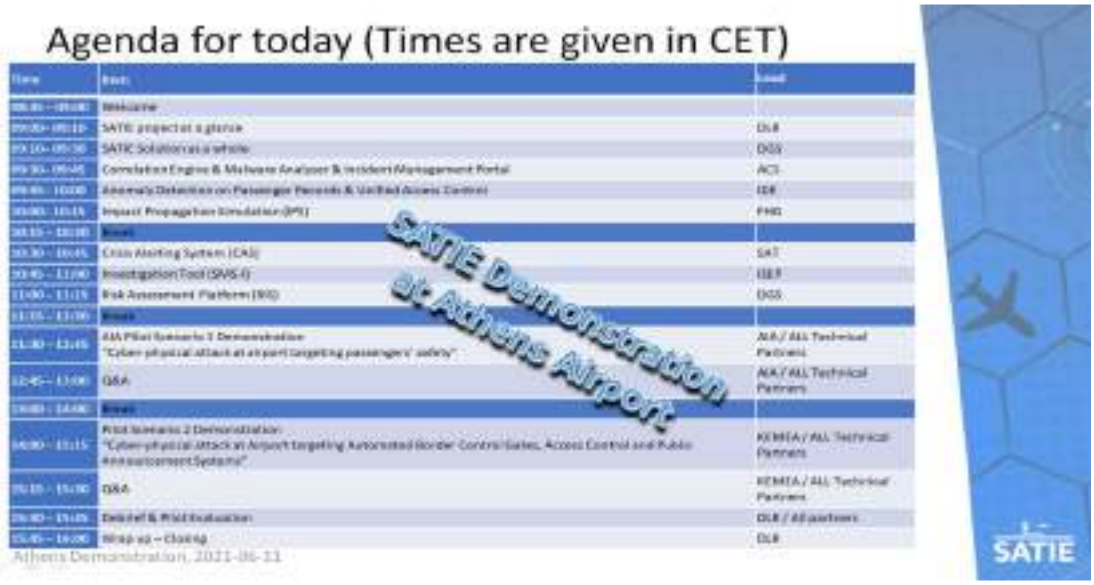
More specifically, eighty-six (86) persons were invited to the event. They were representatives from different sectors such as EU airports, EC and EU agencies, policy makers, national agencies, physical and cybersecurity professionals, academia and industry of the aviation and cyber physical security domain. The demonstration event was attended by sixty-seven (67) people, twenty-two (22) of whom were external parties. Due to the COVID-19 measures and travel restrictions, the audience attended virtually, the hybrid-based demonstration, taking advantage of the online broadcasting and interactive process.

The main objective of the SATIE demonstration at the Athens Airport was to communicate the SATIE Solution, present its functionalities and illustrate how it is capable of preventing, detecting, responding and mitigating threats in a holistic manner. In doing this, SATIE will help airports to address and undertake effective actions to potential complex cyber and physical attacks and therefore maintain airports' security and safety. This objective was validated through the deployment of two realistic cyber and physical attack scenarios that took place at the Athens International Airport premises:

- Scenario #1: "Cyber- physical attack targeting passengers' security".
- Scenario #2: "Cyber-physical attack at airport targeting Automated Border Control Gates, Access Control and Public Announcement Systems".

The first scenario was coordinated by AIA and the second pilot scenario was coordinated by KEMEA with the support of AIA. The SATIE demonstration at Athens Airport was a full day event and lasted approximately 7 hours. The agenda of the event is depicted in Figure 2.2.

Figure 2.1: The Athens Airport premises



Agenda for today (Times are given in CET)

Time	Item	Lead
08:45 – 09:00	Welcome	
09:00– 09:10	SATIE project at a glance	DLR
09:10– 09:30	SATIE Solution as a whole	DGS
09:30– 09:45	Correlation Engine & Malware Analyser & Incident Management Portal	ACS
09:45 – 10:00	Anomaly Detection on Passenger Records & Unified Access Control	IDE
10:00 – 10:15	Impact Propagation Simulation (IPS)	FHG
10:15 – 10:30	Break	
10:30 – 10:45	Crisis Alerting System (CAS)	SAT
10:45 – 11:00	Investigation Tool (SMS-I)	ISEP
11:00 – 11:15	Risk Assessment Platform (RIS)	DGS
11:15 – 11:30	Break	
11:30 – 12:45	AIA Pilot Scenario 1 Demonstration "Cyber-physical attack at airport targeting passengers' safety"	AIA / ALL Technical Partners
12:45 – 13:00	Q&A	AIA / ALL Technical Partners
13:00 – 14:00	Break	
14:00 – 15:15	Pilot Scenario 2 Demonstration "Cyber-physical attack at Airport targeting Automated Border Control Gates, Access Control and Public Announcement Systems"	KEMEA / ALL Technical Partners
15:15 – 15:30	Q&A	KEMEA / ALL Technical Partners
15:30 – 15:45	Debrief & Pilot Evaluation	DLR / All partners
15:45 – 16:00	Wrap up – Closing	DLR

SATIE Demonstration at Athens Airport

Athens Demonstration, 2021-06-11

Figure 2.2: The agenda of the SATIE demonstration event at the Athens 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 Athens's demonstration scenarios (see section 2.5), namely Malware Analyser, Incident Management Portal (IMP), Anomaly Detection on Passenger Records (ADPR), Unified Access Control (UAC), Impact Propagation Simulation (IPS), Crisis Alerting System (CAS), Investigation Tool (SMS-I) and Risk Assessment Platform (RIS). Afterwards, the demonstration was executed following a hybrid approach for each demonstration scenario, as described in more detail in section 0.

The Athens' demonstration event closed with Questions and Answers (Q&As), debrief and pilot evaluation session, during which an online evaluation questionnaire was disposed to the audience for their feedback. At the end of the event valuable comments were collected and fruitful discussions took place between the pilot attendees and the project representatives. In addition, at the end of the event, interviews were provided by (a) the employed SOC operators to testify their overall experience of the SATIE Solution during the pilot and (b) the project technical partners to illustrate the added value of the SATIE Solution towards airport's security operations.

For the needs of the scenario's deployment cyber and physical infrastructure of the Athens Airport was engaged and audio-visual material was produced, as further analysed in sections 0 and 0 respectively.

In the following, some indicative pictures of the SATIE Athens Airport demonstration event are displayed (Figure 2.3, Figure 2.4, Figure 2.5, Figure 2.6 and Figure 2.7).

Figure 2.3: The Security Operations Centre (SOC) activities during the Athens Airport demonstration event

Figure 2.4: Technical partners' works during the Athens Airport demonstration event

Any questions?

Figure 2.5: Screenshot from the web performance of the Athens Airport demonstration event during technical partners' presentations

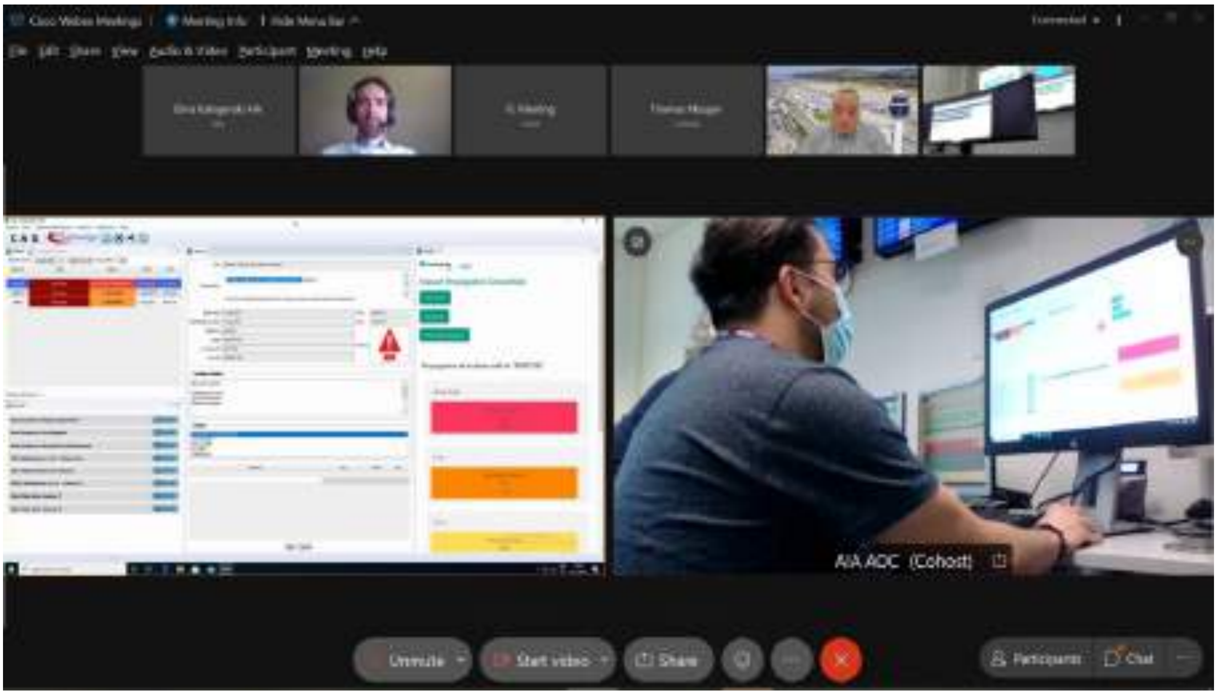


Figure 2.6: Screenshot from the web performance of the Athens Airport demonstration event during the scenario’s execution, showing the AOC activities

Figure 2.7: SATIE project partners’ representatives in the Athens Airport demonstration event

2.2 AIA cyber and physical infrastructure and systems integration with the SATIE Solution

The current section presents the cyber and physical infrastructure utilized for the SATIE Athens demonstration.

2.2.1 Localisation and logistics

As described in section 2.1., the SATIE Athens Airport demonstration event was held in AIA premises in Greece on the 11th of June, 2021. For the demonstration performance the Administration Building - B17, Technical Services/backup AOC - B11, Gate 3 and Automated Border Control (ABC) gates of the Athens Airport were utilized.

The Athens Airport sites and supply engaged to run the Athens Airport demonstration event were the following:

- **Two conference rooms** at the 2nd floor of the Athens Airport Administration Building (B17) for the performance of the combined physical and web demonstration event.
- The **Network Operations Centre/Security Operations Centre** (**NOC/SOC room)** of the Athens Airport for the pilot operations allocating two working positions for the SOC operators trained users giving access to the SATIE functionalities and graphical user interfaces of the engaged SATIE Tools that are relevant to SOC operations, as presented in sections 0 and 0.
- The **Airport Operations Centre** (**AOC) room** of the Athens 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 giving access to the SATIE functionalities and graphical user interfaces of the engaged SATIE Tools that are relevant to AOC operations, as presented in sections 0 and 0.
- The **ABC officer working position** giving access to the relevant SATIE functionalities and graphical user interfaces of the engaged SATIE Tools as described in section 0.
- A **muster station** of the Athens Airport for the demonstration scenarios execution, as described in section 0.
- The **border control area** and the **Automated Border Control (ABC) gates** of the Athens Airport operated by the Hellenic Police, as described in section 0.
- The **Public Announcement (PA) room** of the Athens Airport for the demonstration scenarios execution, as described in section 0.
- **Airport authorized security area** that leads to the PA room for the demonstration scenarios execution, as described in section 0.
- **Networking and audio-visual equipment, technical support for the real-time video transmission** to run the demonstration operations and perform the virtual event.

Figure 2.8 illustrates a map of the Athens International Airport indicating the Airport sites, where the demonstration was performed.

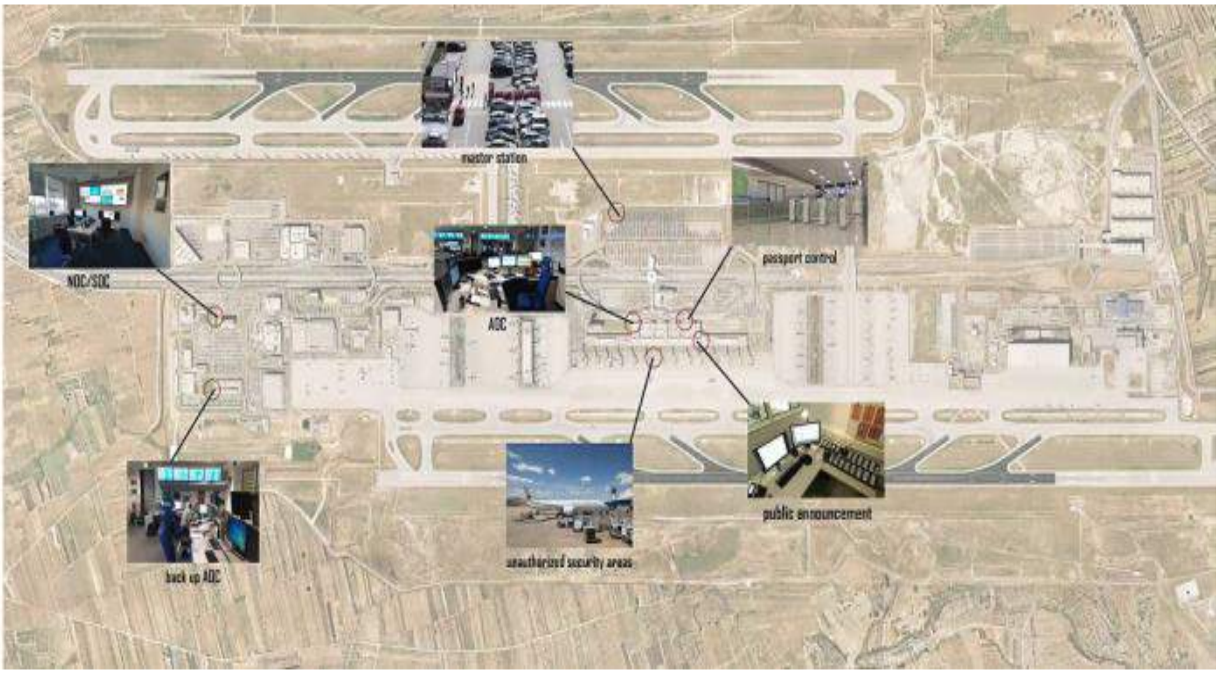


Figure 2.8: Athens International Airport map depicting the sites used in the SATIE Athens demonstration

In the following, indicative images of the Athens Airport demonstration sites are shown (Figure 2.9, Figure 2.10, Figure 2.11, Figure 2.12, Figure 2.13).

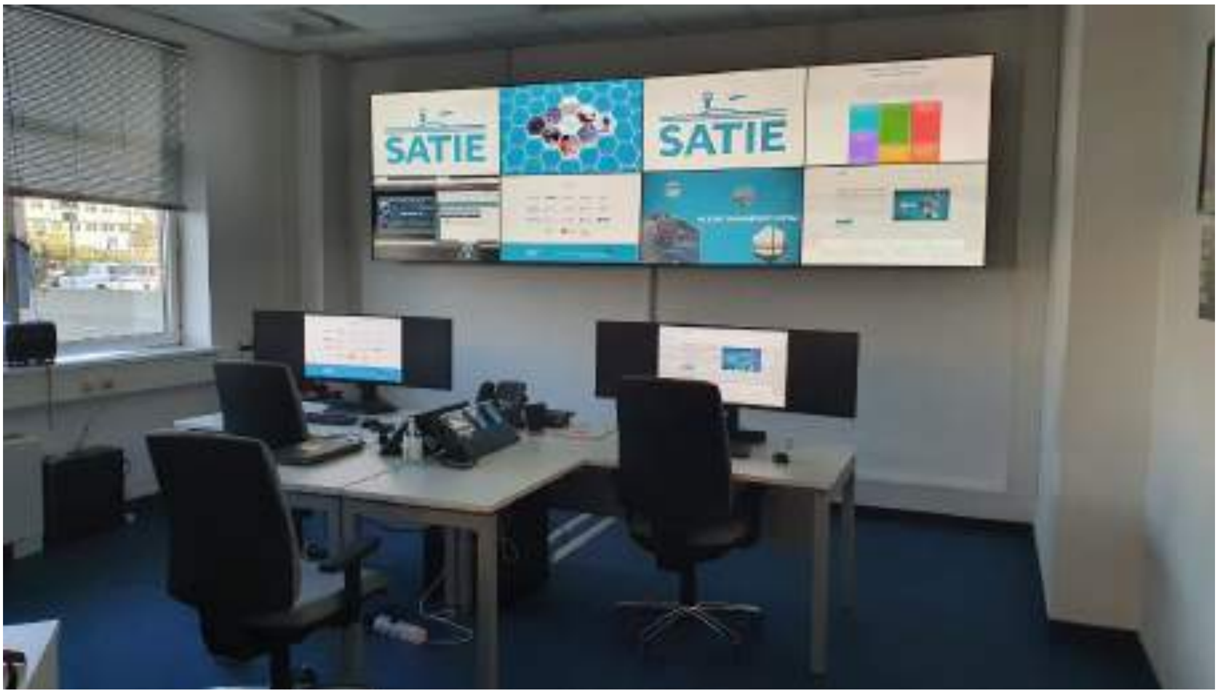


Figure 2.9: The Athens Airport SOC room used for the demonstration event

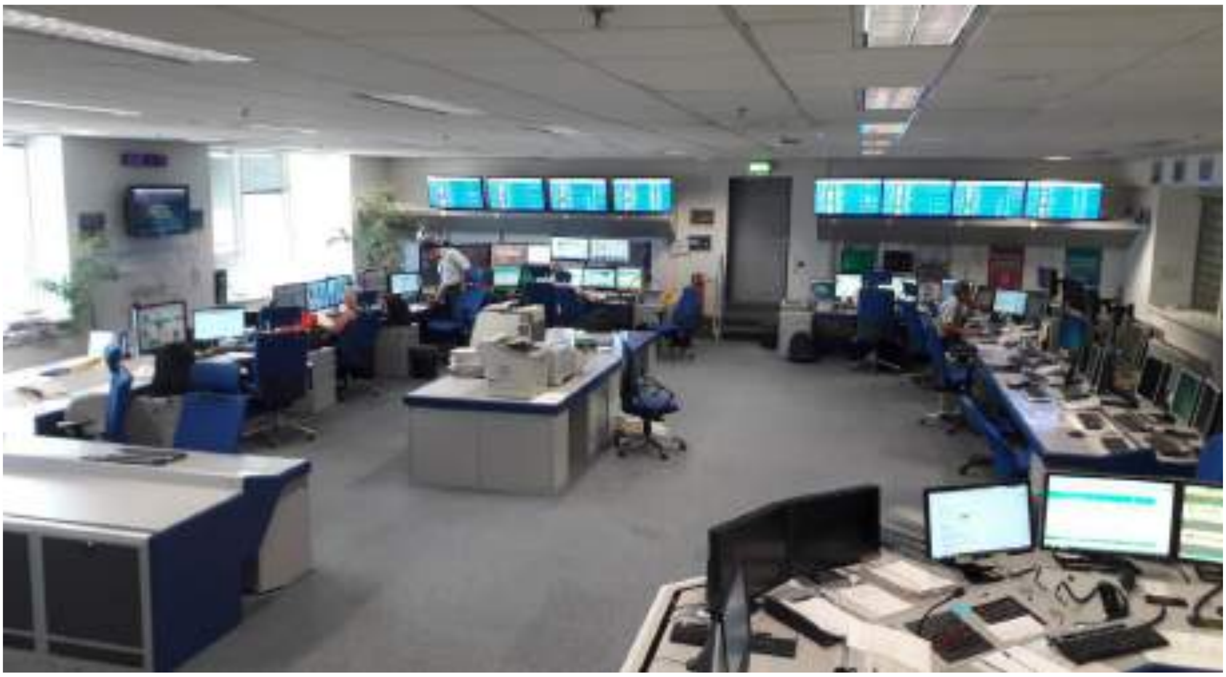


Figure 2.10: The AOC room used for the demonstration event of the Athens Airport

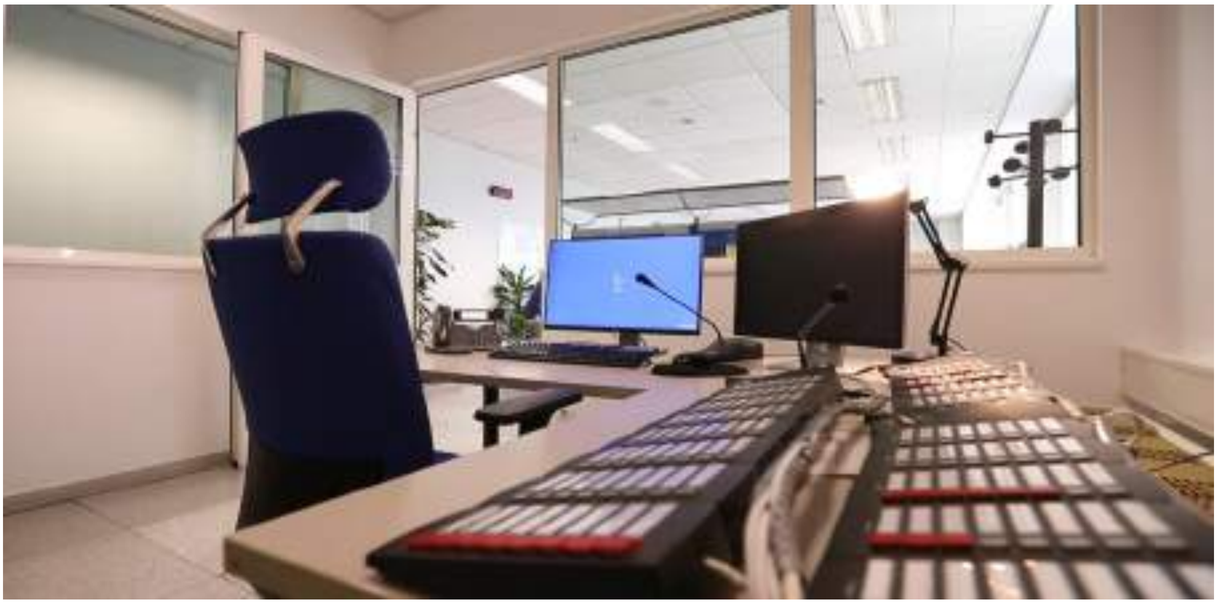


Figure 2.11: The Athens Airport Public Announcement (PA) room utilized for the demonstration scenarios execution

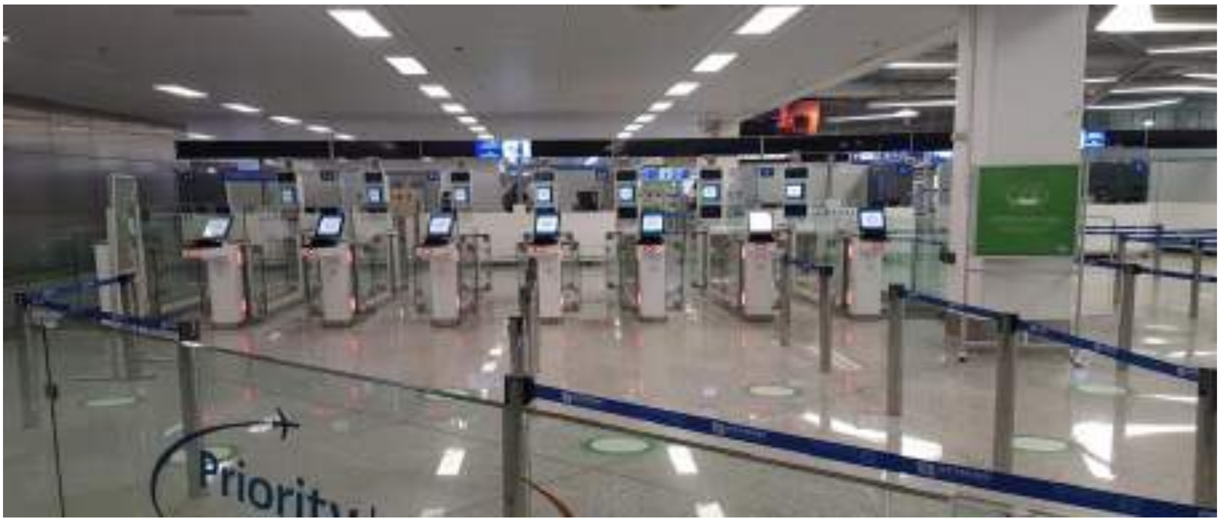


Figure 2.12: The border control area and the Automated Border Control (ABC) gates of the Athens Airport utilized for the demonstration scenarios execution

Figure 2.13: The conference room used for the partners' participants

2.2.2 Cyber and physical infrastructure integration for the Athens Airport demonstration

To validate the SATIE Solution under real circumstances and demonstrate that it is capable of responding to complex attacks, two realistic attack scenarios were set during the Athens demonstration event bridging the cyber and physical worlds, involving Athens Airport critical systems. The Athens Airport cyber and physical infrastructure utilized to execute the AIA demonstration scenarios are provided herein:

- The **Airport Operational Database (AODB)/Flight Information Display system (FIDS)**, which is a critical system for the AIA airport as it is responsible of displaying such information to passengers on screens around in the airport.
- The **Public Announcement (PA) system** which supports the announcements services to passengers and thus it is of great importance for the airport.

- The **cyber and physical systems, e.g. Access Control (AC) and security doors, Closed-Circuit Television (CCTV),** which are considered of high criticality to maintain people's safety and prevent unauthorised access to airport's restricted areas.
- A **muster station** of the Athens Airport for the demonstration scenarios execution, as described in section 0.
- The **Automated Border Control (ABC) system,** operated by the Hellenic Police, authenticates the passenger's electronic machine-readable travel document or token, and establishes that the passenger is the rightful holder of the document or token by querying border control records. The system determines the eligibility of border crossing, according to the pre-defined rules. The ABC system consists of the following main components: (a) a document reader, (b) biometric capture devices (i.e. camera and/or fingerprint reader), (c) one or two physical barriers (ABC-gates), which may have swinging or sliding doors opened by electronic means, and (d) device to provide instructions, which guide the passenger through the border control (monitors, LED signals, audio devices), (e) cameras/sensors for surveillance (f) monitoring and control stations for the operators (ABC computer or Police passport computer).

To run the demonstration scenarios, the following Athens Airport environment was replicated on the CyberRange simulation environment and thereby connected to the SATIE Solution:

- For the demonstration Scenario #1 a CCTV camera, the AC system, the PA system and the AODB.
- For the demonstration Scenario #2 the PA system.

Figure 2.14 displays the Athens Airport environment that was replicated on the SATIE Cyber Range platform.

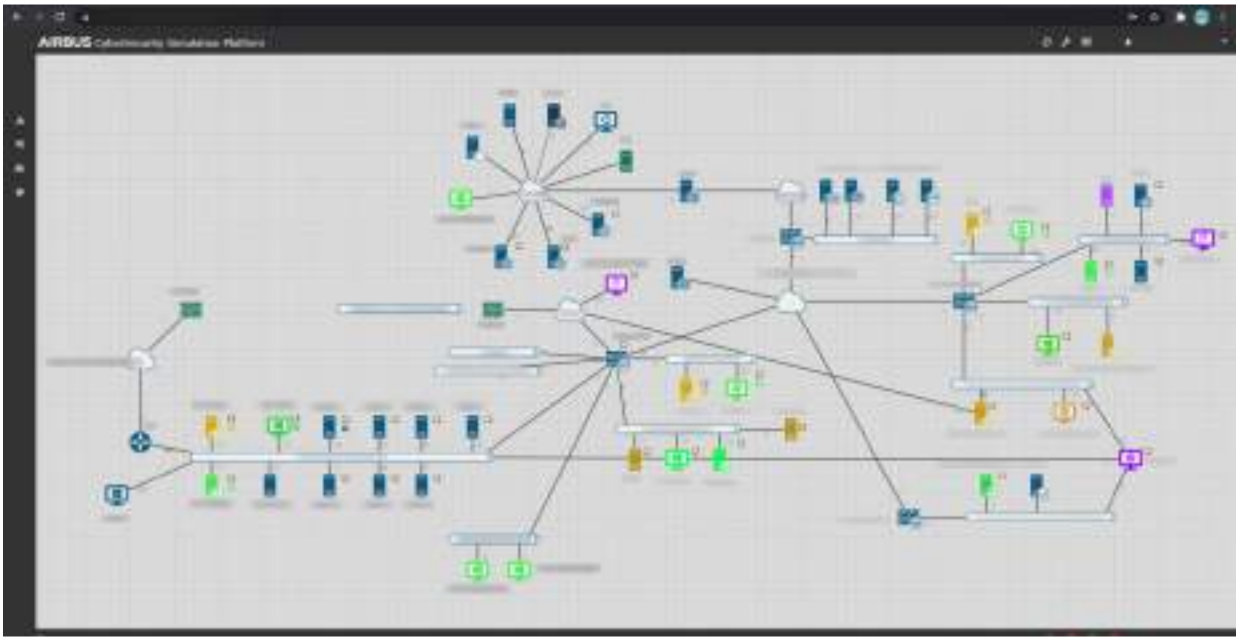


Figure 2.14: The SATIE Cyber Range platform addressing the Athens Airport critical environment

2.3 Operations during the AIA demonstration event

A set of coordinated activities took place, during the AIA demonstration event. These activities were undertaken by AIA and KEMEA and the SATIE technical partners that actively participated in the event. During the demonstration event, two SOC operators (one from AIA and one from the Hellenic Police) and two AOC operators (from AIA), already trained through the SATIE training workshops as mentioned in section 2.1, have participated.

During the demonstration, the scenarios were introduced to the attendees by the business moderators from either AIA for Scenario #1 or KEMEA for Scenario #2, who were responsible for the narration of the scenario and the explanation of the business aspects per each scenario step. The technical moderator (DLR) coordinated and explained the technical aspects of each scenario step, while the SOC and AOC operators interacted in real time with the SATIE Tools (further details are presented in section 0). In order to operate in near real conditions, limited information was provided to the involved SOC and AOC operators, regarding the scenarios, ensuring that they cannot foresee the attacks, as they wouldn't be able during a real incident occurring at the airport. On the other hand, the audience was aware of the detailed scenario steps in order to have the capacity to evaluate the detection of the attacks by the SATIE Solution and the operators' reactions.

The Athens demonstration event was set up as a hybrid event. As such, for each scenario some of the steps that could not be demonstrated live were pre-recorded and presented through video, while the other steps were demonstrated live from AIA premises. In more detail for the needs of Scenarios #1 and #2, IDEMIA demonstrated the functionality of the Unified Access Control (UAC) and the Passenger Anomaly Detection (ADPR) live at AIA premises. For both scenarios the attacks were simulated and the SOC and AOC operators could manage real-time alerts and incidents through the IMP and the CAS respectively at real time, while sharing their screens with the attendees.

At the beginning of each scenario a sharp and detailed video was presented to the attendees. The video presented per each scenario step the attack and the SATIE means of detection as well as the relevant SATIE operations. Then, during the demonstration of each scenario short videos were presented to the audience, mostly highlighting the attacks. The short videos highlighted critical parts of the scenarios and how the SATIE Tools were utilised in order to detect the attacks and mitigate the consequences. At the same time the attack was simulated and the participating SOC operators were notified for the alerts through the Incident Management Portal (IMP) and were able to further investigate them by using the SATIE Tools. In addition, the SOC operators were able to create incident reports, and retrieve additional information for the incidents through the relevant network graphs, the statistics and the impact propagation simulation results. In this sense, they took appropriate actions to encounter or mitigate the threats (e.g. create manual alerts to communicate the detected threats to the AOC operators to undertake proper actions) when needed. The AOC operators were monitoring the Crisis Alerting System (CAS) and used CAS to manage incidents and implement the necessary and standard operational procedures to mitigate the incident. The AOC operators could see the incident details and feeds of CCTV cameras, and send an SMS or email notification to the First Responders e.g. Hellenic Police. The SOC and AOC operators shared their screens with the attendees while performing the aforementioned activities.

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

- Incident Management Portal (IMP).
- Risk Integrated Service (RIS).
- Vulnerability Intelligence Platform (VIP).
- Malware Analyser (MA).

- Correlation Engine.
- Investigation Tool (SMS-I).
- Impact Propagation Simulation (IPS).

The participating AOC operators were notified for the alerts raised by the SATIE Incident Management Portal (IMP) through the Crisis Alerting System (CAS). In addition, they had access to the produced incident reports, 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 encounter or 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).

For the needs of Scenario #2, IDEMIA demonstrated the functionality of the Passenger Anomaly Detection (ADPR) system live at AIA premises. As indicated by Scenario #2, at specific steps during the demonstration, a Hellenic Police (HP) officer had access and used the ADPR, on site at the airport as further described in Table 2.2.

As previously mentioned, to better comprehend the scenario demonstration, two videos were produced for each scenario; a detailed (15 minutes) video and a short (5 minutes) video. The following Figures (Figure 2.15 and Figure 2.16) show some video footages of the produced audio-visual material of the two demonstration scenarios.

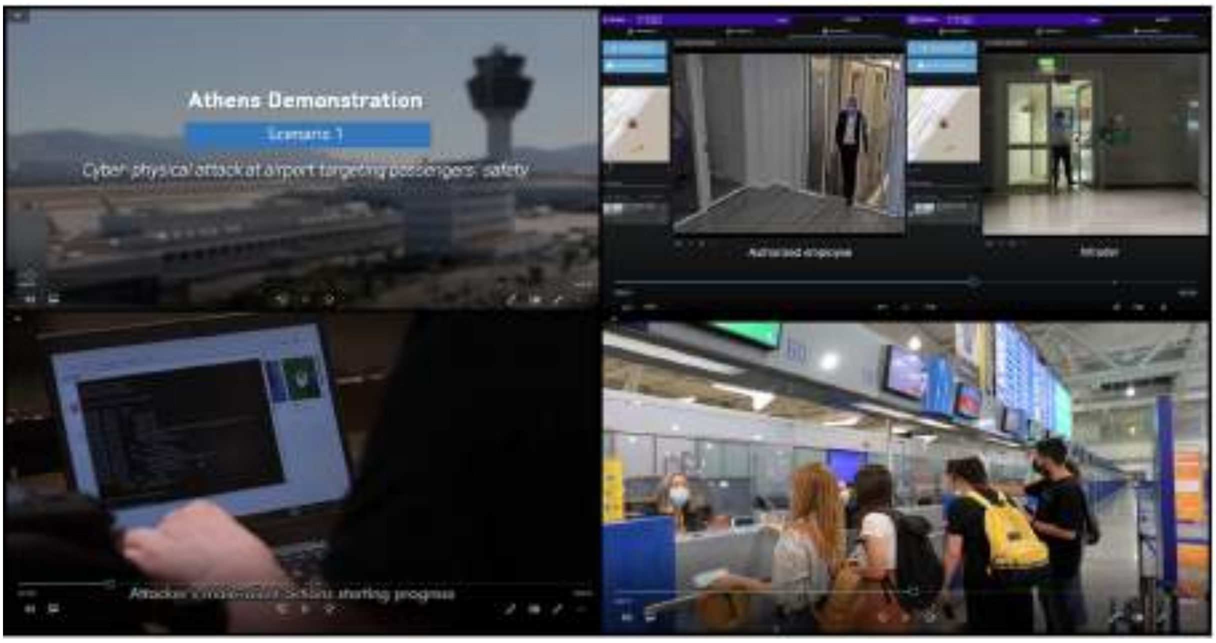

Athens Demonstration
Scenario 1
Cyber physical attack at airport targeting passengers' safety
Authorised employee
Intruder
Attacker [illegible] Scenario starting progress

Figure 2.15: Footages of the Athens demonstration Scenario #1 videos

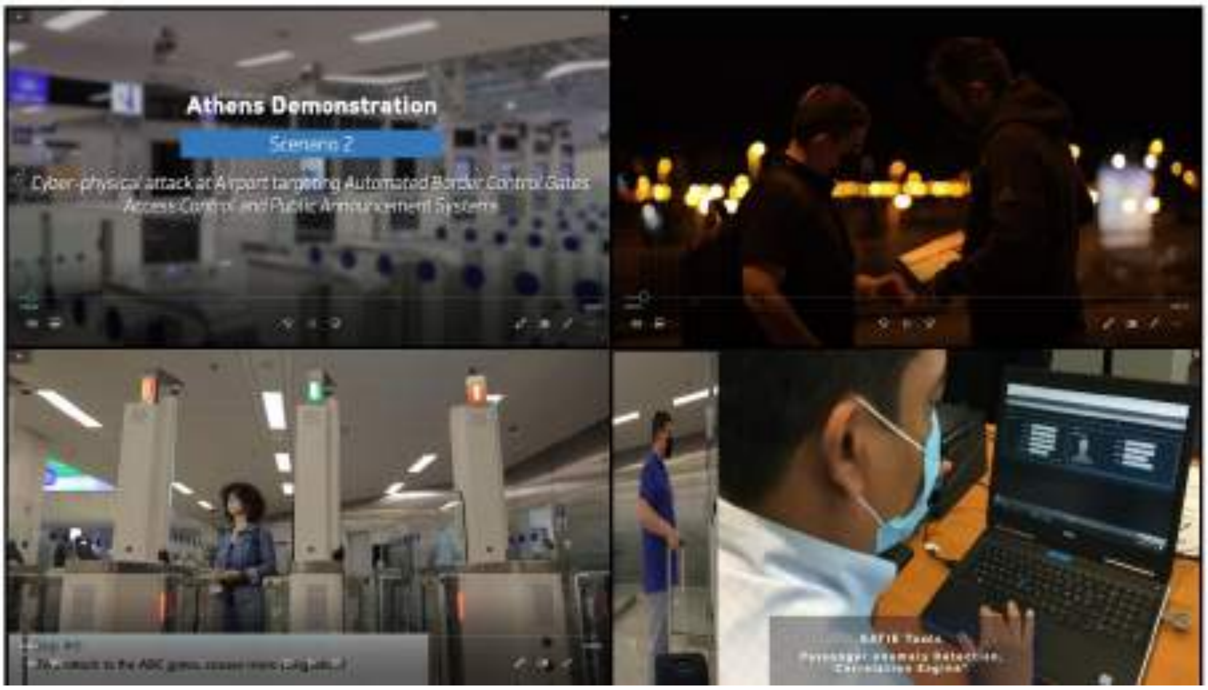

Athens Demonstration
Scenario 2
Cyber-physical attack at Airport targeting Automated Border Control Gates Access Control and Public Announcement Systems
SATIE Tools
Passenger anomaly detection, Correlation Engine

Figure 2.16: Footages of the Athens demonstration Scenario #2 videos

The following figures (Figure 2.17 to Figure 2.19) depict operations from the Athens Airport demonstration scenarios execution.

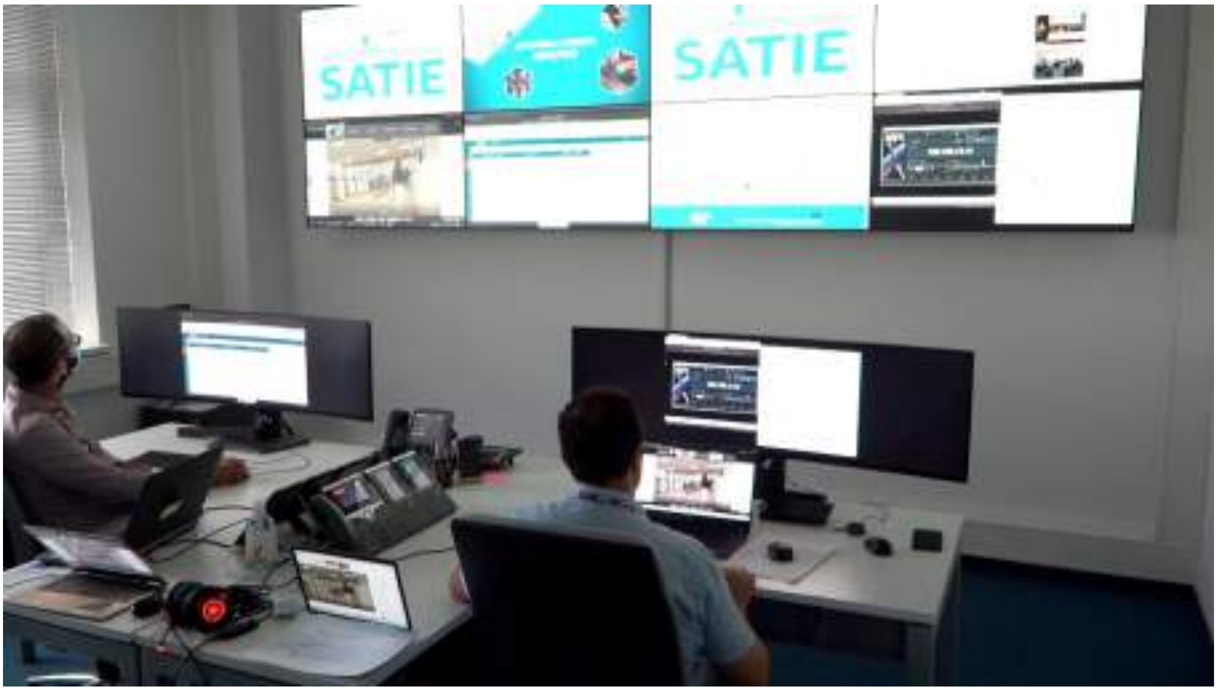


Figure 2.17: SOC operations during the Athens Airport demonstration scenarios execution

Figure 2.18: AOC operations during the Athens Airport demonstration scenario´s execution

Figure 2.19: Technical operations during the Athens demonstration event regarding the Anomaly Detection on Passenger Records (ADPR)

2.4 Demonstration scenarios

Athens Airport demonstration incorporated two sophisticated, coordinated scenarios, engaging both cyber and physical threats. The scenarios are the following:

- Demonstration Scenario #1: “Cyber physical attack at airport targeting passengers’ security” (coordinated by AIA).
- Demonstration Scenario #2: “Cyber-physical attack at airport targeting Automated Border Control Gates, Access Control and Public Announcement Systems” (coordinated by KEMEA and AIA).

2.4.1 Demonstration Scenario #1 “Cyber- physical attack targeting passengers’ security”

The current scenario refers to a potential coordinated attack at the airport premises primarily targeting at passengers’ safety by disrupting the provision of Flight Information, physical Access Control and public announcement services leading to massive passengers’ evacuation at the airport terminal.

The SATIE Solution adopts a holistic approach towards threat prevention, detection, response, and mitigation which can help airports to address such attacks to the protection of critical systems and people's safety.

The objective of this attack scenario performance is to demonstrate the SATIE Solution towards a real airport environment under real conditions. In addition, it aims to illustrate how SATIE can detect complex cyber and physical attacks and how its integrated components operate with each other 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 the airport security and people’s safety.

The roles considered in the specific scenario are as follows:

Cyber attacker: An AIA employee imitating the cyber attacker.
Physical attacker: An AIA employee imitating the physical attacker.
Employee: Meaning a member of the CyberRange operating personnel, acting as an AIA employee in the simulation and an AIA employee in the demonstration.
SOC operator: Employee of the AIA’s Security Operation Centre (SOC) who has access to the Incident Management Portal (IMP) of SATIE.
AOC operator: Employee of the AIA’s Airport Operation Centre (AOC) who has access to the Crisis Alerting System (CAS) of SATIE.

Table 2.1: Scenario #1: “Cyber-physical attack at airport targeting passengers’ security”

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
1. Cyber-attack on FIDS to display incorrect information to passengers.	1.1 A spear-phishing email is sent to an email address accessed on a FIDS workstation. An employee opens an attached word file which activates a macro and grants the attacker access	Malware Analyser Correlation Engine Incident Management Portal (IMP)	The cyber attacker sends the spear-phishing email. The Malware Analyser triggers the alert of FIDS workstation compromisation. The SOC operator reviews the alert	The cyber attacker sends the spear-phishing email. The Employee downloads and opens the attachment (video). Implemented at airport site: the SOC operator reviews the alert for

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	to the Remote Administration Tool (RAT).		from the IMP. The SOC operator sends the alert to the IPS and CAS.	FIDS workstation compromisation from the IMP screen, detected by the Malware Analyser. The SOC operator sends the alert to the IPS and CAS.
	1.2 The cyber attacker performs information gathering to better understand the network and proxy, and finds an incorrect configuration on a local service on the workstation.		The cyber attacker performs the described actions. The Correlation Engine triggers a recurring alert which is viewed by the SOC operator from the IMP. The SOC operator sends the alert to the IPS and CAS.	The cyber attacker performs the described actions. Implemented at airport site: the Correlation Engine triggers a recurring alert which is viewed by the SOC operator from the IMP. The SOC operator sends the alert to the IPS and CAS.
	1.3 The cyber attacker uploads a manipulated RAT and modifies the service with the incorrect configuration to execute it. This allows him to exploit the wrong configuration of the service and get local account access of the system.		The cyber attacker performs the described cyber-attack. The Correlation Engine triggers alerts which are viewed by the SOC operator from the IMP. The SOC operator sends the alerts to the IPS and CAS.	The cyber attacker performs the described cyber-attack. Implemented at airport site: the Correlation Engine triggers alerts which are viewed by the SOC operator from the IMP. The SOC operator sends the alerts to the IPS and CAS.
	1.4 The cyber attacker uploads the exploit “SharGPOAbuse” which allows the modification of the Group Policy		The cyber attacker performs the described cyber-attack. The Correlation Engine triggers the alert of Domain	The cyber attacker performs the described cyber-attack. Implemented at airport site: the Correlation

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	Object (GPO).		Controller compromisation which is reviewed by the SOC operator from the IMP. The SOC operator sends the alert to the IPS and CAS.	Engine triggers the alert of Domain Controller compromisation which is reviewed by the SOC operator from the IMP. The SOC operator sends the alert to the IPS and CAS.
	1.5 A scheduled task is created on the domain controller policy (which holds a group policy for FIDS and AC systems).		The cyber attacker performs the described cyber-attack. The Correlation Engine triggers an alert which is reviewed by the SOC operator from the IMP. The SOC operator sends the alert to the IPS and CAS.	The cyber attacker performs the described cyber-attack. Implemented at airport site: the Correlation Engine triggers an alert which is reviewed by the SOC operator from the IMP. The SOC operator sends the alert to the IPS and CAS.
	1.6 The GPO domain controller policy executes that task to compromise the domain controller to allow access to the entire domain.		The cyber attacker performs the described cyber-attack. The Correlation Engine triggers alerts involving FIDS, and AC compromisation which is reviewed by the SOC operator from the IMP. The SOC operator sends the alert to the IPS and CAS.	The cyber attacker performs the described cyber-attack. Implemented at airport site: the Correlation Engine triggers alerts involving FIDS, and AC compromisation which is reviewed by the SOC operator from the IMP. The SOC operator aggregates all the alerts received from step 1.1 to step 1.6 into a unified incident and sends it to the IPS and CAS.
	1.7 The cyber attacker accesses		The cyber attacker performs the	The cyber attacker performs the

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	the FIDS with credentials stolen from the clipboard of the compromised workstation.		described cyber-attack.	described cyber-attack.
	1.8 The cyber attacker runs a script to change data in the FIDS database by searching for all flights for that day and shifting them ahead or behind by an hour or two.		The cyber attacker performs the described cyber-attack.	The cyber attacker performs the described cyber-attack.
2. The FIDS monitor shows the changing of flight times. Passengers cannot locate their flights.	Passengers cannot locate their flights as they arrive at gates at the wrong times.	-	-	The FIDS monitor visually shows the changing of flight times (video).
3. Passengers' request assistance from Employee.	Passengers turn to airport personnel for assistance and overburden the staff.	-	-	-
4. Airport operations degrade.	Airport operations degrade and the airport comes to a standstill.	-	-	-
5. Cyber-attack to gain access to the airport's Access Control (AC) workstation.	5.1 The cyber attacker compromises the legitimate information system of a maintenance contractor.	-	-	The cyber attacker compromises the legitimate information system of a maintenance contractor (video).
	5.2 Cyber attacker sends a seemingly legitimate email requesting to activate the VPN connection	-	-	The cyber attacker sends an email requesting to activate the VPN (video).

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	between their remote PC and the maintenance workstation.			
	5.3 AIA grants access.	-	-	The Employee grants access (video).
	5.4 The cyber attacker accesses the maintenance workstation that monitors the status of the AC system.	-	-	The cyber attacker accesses the maintenance workstation that monitors the status of the AC system (video).
	5.5 The cyber attacker connects to the access control application and unlocks all AC doors.	-	-	The cyber attacker connects to the access control application and unlocks all AC doors. The door at AIA's premises opens (video).
6. The physical attacker passes the security doors to move to the PA room.	6.1 Doors are not secured, allowing unauthorized people to enter security restricted areas, halting airport operations, delaying flights and possibly allowing a physical attack.		-	Doors are not secured, allowing unauthorized people to enter security restricted areas, halting airport operations, delaying flights and possibly allowing a physical attack (video).
	6.2 In this situation, physical attacker enters into a restricted area which leads to the PA room without raising any suspicion.	Unified Access Control (UAC) Correlation Engine Incident Management Portal (IMP)	Triggers the alert of unauthorized access which is reviewed by the SOC operator and was sent to the IPS and CAS.	Implemented at airport site, the Correlation Engine raised an alert for unauthorised access and displayed to SOC operators at the airport site through the IMP and passed to the IPS and CAS: the physical attacker passes the security doors which lead to security restricted

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
				areas. Demonstration of the Unified Access Control tool while authorised and non-authorised people were passing the security doors.
7. The physical attacker enters the PA room and presses the evacuation button to activate an evacuation message.	7.1 The physical attacker approaches the PA room, and gains access to the PA server.	-	-	The physical attacker accesses the PA server (video).
	7.2 The physical attacker pushes the evacuation button of the PA system and activates the pre-recorded evacuation message urging passengers and staff to evacuate the terminal building and move to the muster stations.	Correlation Engine Impact Propagation Simulation (IPS) Incident Management Portal (IMP) Crisis Alerting System (CAS)	An evacuation request alert was displayed indicating "evacuation" of the area and move to the "Muster Station". The SOC operator reviewed the alert and passed it to the IPS and CAS. The AOC received and reviewed the alert along with the accompanying information.	The physical attacker presses the evacuation button and plays the pre-recorded message. Implemented at airport site: the correlation Engine displayed an evacuation message alert indicating "evacuation" of the area and move to the "Muster Station" reviewed by the SOC operator from the IMP screen and forwarded to the IPS and CAS. The IPS produced a passengers' evacuation simulation results. The SOC operator reviewed from the IMP the respective simulation report and the evacuation request alert produced by the Correlation Engine and aggregated the alerts received from steps 6

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
				(unauthorised access) and 7 (evacuation request) to register a unified incident (which is passed again to the IPS and CAS). The AOC operator received and reviewed the alert and the content of the unified incident.
8. Terminal evacuation.	PA messages indicate to evacuate the terminal, causing passengers and staff to move to muster stations near the parking areas.	Incident Management Portal (IMP) Crisis Alerting System (CAS)	The SOC operator aggregated the alerts produced from step 1, step 6 and step 7 and registered a unified incident through the IMP. The AOC operator received the incident and reviewed it.	Passengers evacuate the terminal moving towards to the muster stations (video). Implemented at airport site: the SOC operator reviewed all results from the IMP, aggregated all the corresponding alerts received from step 1, step 6 and step 7 to register a unified incident. The AOC operator received and reviewed the alert and the incident sent to CAS.
9. Passengers are gathered at the muster stations.	While passengers are gathered at the muster stations, a terrorist attack is possible as cars and people in the parking area do not go through security screening.	Crisis Alerting System (CAS)	-	The AOC communicated with security personnel via the CAS to handle the incident and undertake proper actions to the people's safety.

2.4.2 Demonstration Scenario #2 "Cyber-physical attack at airport targeting Automated Border Control Gates, Access Control and Public Announcement Systems"

Using social engineering, the attacker achieves to identify an ABC maintenance worker willing to accept bribe to perform an attack to the ABC gates. During a regular maintenance visit by the bribed maintenance worker, the on-duty ABC operator enables the USB port usage on the ABC computer, as requested by the maintenance worker in order to install the most recent security patches. The bribed worker inserts a USB stick with the malware created by them. The malware gets installed automatically as soon as the USB stick is plugged-in, making a MITM attack between the ABC gate and the ABC database possible, in which, when the ABC gate queries the database for the person attempting to cross the ABC gate and enter or exit EU soil, the malware sends back a falsified response regarding whether a background check is needed.

During this first attack, as a result of the falsified responses due to the malware execution, all passengers, including an attacker, are allowed to cross without further background checks. Due to the fact that the normal rate of necessary background checks is relatively low, the aforementioned abnormality, considering its short duration, does not raise suspicion to the ABC officers.

After 15 minutes, the attack progresses to its next phase whereby the malware alters its behaviour and manipulates the background check requirements randomly. The result of this second attack is the increased rate of travellers having unsuccessful authentications by the ABC system, signalling the need to be manually checked by the on-duty ABC officers. As a consequence, a light congestion starts being created and for addressing the situation the ABC officers manually open the ABC gates and perform manual checks to travellers using SATIE's Anomaly Detection on Passenger Records (ADPR) Tool.

In parallel, a cybercriminal managed to compromise the Access Control system of the airport. Thus, he is able to connect to the access control application and unlock the security doors that lead to airport security areas, where the Public Announcement system is located. Thereby, another attacker enters the PA room, gains unauthorized access to the PA server, and plays a pre-recorded message asking travellers to move to the passport control area (ABC-gates). For addressing the situation, the ABC officers are forced to continuously use the ADPR, which triggers a medium severity alert, generated and managed accordingly through the SATIE Solution by the ABC officer and the SOC operators. Together, all of SATIE Tools enable the SOC operator to recognize the attack in time and inform law enforcement through the Crisis Alerting System taking in consideration numerous aspects of the situation in comparison to the expected normality of daily operations. More specifically, the Correlation Engine as core part of the SATIE Solution enables the security personnel to unveil the attack path behind the raised alerts.

The roles considered in the specific scenario are as follows:

Attacker 0: A KEMEA employee compromising the external maintenance worker.
Compromised Maintenance Worker: A KEMEA employee imitating the compromised external ABC maintenance worker.
Operator: A member of the CyberRange operating personnel.
ABC Officers: ABC officers on duty at the ABC gates.
Police Duty Officer: Police Duty Officer at the ABC gates.
Travellers: Multiple people recruited by AIA, KEMEA who act as passengers, on a volunteering basis. It is assumed that some of them require background checks before passing the ABC-gates.
Attacker 1: A KEMEA employee imitating the cyber – criminal.
Attacker 2: A KEMEA employee imitating the second attacker. He is assumed to be a person of interest for whom background check is required.
Attacker 3: An AIA employee imitating the third attacker. He is assumed to be a member of the airport cleaning services team.
SOC operator (L1): ABC officer who has access to the Incident Management Portal (IMP) of SATIE.

SOC operator (L2): Employee of the AIA's Security Operation Centre (SOC) who has access to the Incident Management Portal (IMP) of SATIE.
AOC operator: Employee of the AIA's Airport Operation Centre (AOC) who has access to the Crisis Alerting System (CAS) of SATIE.

Table 2.2: Scenario #2: "Cyber-physical attack at airport targeting Automated Border Control Gates, Access Control and Public Announcement Systems"

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
0. Preparation	0.1 Attacker 0 compromises through bribery the external Maintenance Worker.		**-**	Attacker 0 compromises the external **Maintenance Worker** through bribery. The latter develops the malware and saves it on the USB (video).
	0.2 The compromised Maintenance Worker creates and installs the malware to the USB.		-	
1. Malware installation in ABC system	1.1 The Compromised Maintenance Worker arrives at the airport to perform maintenance procedures.		-	The **Compromised maintenance Worker** arrives at the airport. An **ABC officer** on duty accompanies him to the ABC administration office. (video).
	1.2 The ABC officer goes to its desk, logins on the computer and enables the USB port.		-	The **ABC Officer** on duty logs into the ABC computer with admin credentials and enables the USB port (video).
	1.3 The Compromised Maintenance Worker, while performing maintenance procedures, mounts the USB device.	Correlation Engine Incident Management Portal (IMP)	A low severity alert is sent to the Correlation Engine. The **SOC operator (L1)** is notified for the alert through the IMP and further investigates it. As there is nothing out of the ordinary (maintenance procedures), there is no need to assign the alert to another operator for a deeper investigation and he writes the	The **Compromised Maintenance Worker** inserts the USB stick with the malware. As soon as the USB is mounted, a low severity alert is raised for the insertion of the USB stick. The **SOC operator (L1)** is notified for the alert through the IMP and further investigates it. As there is nothing out of the ordinary (maintenance procedures), there is

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
			relevant report.	no need to assign the alert to another operator for a deeper investigation and he writes the relevant report.
	1.4 The malware gets installed automatically as soon as the USB stick is plugged in**.**		The **Operator** remotely installs to the ABC computer the malware, which malforms all responses about the background check requests.	The **Compromised Maintenance Worker** installs the malware to the ABC computer (video).
	1.5 The Compromised Maintenance Worker informs the ABC officer on duty that the system is updated and leaves the airport.			The **Compromised Maintenance Worker** informs the **ABC officer** on duty about the finalization of the update and leaves the airport (video).
2. First attack to ABC system.	2.1 While travellers scan their passports, the ABC system displays "No Hit" for every passenger's check. As a result, all travellers manage to cross the border.		The ABC system (simulated on the Cyber Range) displays "No Hit" next to the field indicating whether a background check is required.	**Travellers** at the airport scan their passports and are always allowed to cross the ABC gates. The ABC system displays "No Hit" next to the field indicating whether a background check is required for each person crossing the gate.
3. Attacker crosses the border	3.1 Attacker 2 succeeds in crossing the ABC gates.			**Attacker 2** scans his passport and crosses the ABC gates (video).
4. Second attack to ABC system.	4.1 While travellers still scan their passports, the malware changes its functionality and produces random positive deceiving-hits.		This automatically occurs.	This automatically occurs.
	4.2 The travellers blocked in the ABC gates refer to the ABC officers. The ABC			**Travellers** scan their passports at the airport and are blocked at the ABC

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	Officers manually open the gates and perform manual checks.			gates. The **ABC officers on duty** perform manual checks (video).
	4.3 The ABC officer uses a lot the Passenger Anomaly Detection (PAD) during the manual checks. Every time the ABC officers use the PAD, an alert is sent automatically by the PAD to the correlation engine (Right).	Passenger Anomaly Detection (PAD) Correlation engine Incident Management Portal (IMP)	An alert is sent automatically by the PAD to the correlation engine.	The **ABC officer** has access to the PAD on site at the airport and makes an additional check. Every time the ABC officers use the PAD, a low severity alert is sent automatically by the PAD to the correlation engine.
	4.4 As the ABC officers use the PAD for 8-12 times in 10 minutes, an alert will be sent automatically by the correlation engine to the IMP. This alert will be marked as having low severity. The incident will be then forwarded to the Impact Propagation Simulation (IPS) and to the Crisis Alerting System (CAS).	Passenger Anomaly Detection (PAD) Correlation engine Incident Management Portal (IMP) Impact Propagation Simulation (IPS) Investigation tool (SMS-I)	The abnormal use of the PAD results in a low severity alert. The **SOC operator (L1)** is notified for the low severity alert and further investigates it. The analysis confirms that it is an incident and the operator marks it as such. The low severity incident is then sent by the SOC operator to the IPS and the CAS. The **AOC operator** is notified for the incident through the CAS and handles the incident by also using the material from the camera that confirms the light congestion. At the moment the incident is considered as low severity and no further escalation is needed.	The **ABC officers** use the PAD on site excessively and makes an additional check. The abnormal use of the PAD results in a low severity alert. The **SOC operator (L1)** is notified for the low severity alert and further investigates it. The analysis confirms that it is an incident and the operator marks it as such. The low severity incident is then sent by the SOC operator to the IPS and the CAS. The SOC operator further explored information reported from the SMS-I. The **AOC operator** is notified for the incident through the CAS and handles the incident by also using the material from the camera that confirms the light congestion. At

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
				the moment, the incident is considered as low severity and no further escalation is needed.
	4.5 The overall control-time for each Traveller (passenger) increases, and this consequently produces congestion to and near the passport control area.	Correlation engine Incident Management Portal (IMP) Impact Propagation Simulation (IPS)	Through the IPS the **SOC operator (L1)** can understand how the congestion at the border control affects the other assets at the airport which is represented in the network model. Also, the light congestion is visualised through the Agent Based Model (ABM).	Through the IPS the **SOC operator (L1)** can understand how the congestion at the border control affects the other assets at the airport which is represented in the network model. Also, the light congestion is visualised through the Agent Based Model (ABM).
5. Attack to AC and PA systems	5.1 Attacker 1 compromises the legitimate information system of a maintenance contractor.		-	**Attacker 1** compromises the legitimate information system of a maintenance contractor (video).
	5.2 Attacker 1 sends a seemingly legitimate email to activate the VPN connection between his remote PC and the maintenance workstation; AIA grants access		-	**Attacker 1** sends a seemingly legitimate email to activate the VPN connection between his remote PC and the maintenance workstation; AIA grants access (video).
	5.3 Attacker 1 accesses the maintenance workstation that monitors the status of the Access Control (AC) system.		-	**Attacker 1** accesses the maintenance workstation that monitors the status of the Access Control (AC) system (video).
	5.4 Attacker 1 connects to the AC application and grants himself access to secured areas.		-	**Attacker 1** connects to the AC application and grants himself access to secured areas (video).

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	5.5 Attacker 3 (camouflaged as cleaning service provider) enters the PA room as the doors have been successfully unlocked by Attacker 1; accesses the PA server; and broadcasts messages via the PA system.	Unified Access Control (UAC) Correlation Engine Incident Management Portal (IMP) Crisis Alerting System (CAS) Investigation Tool (SMS-I)	The Correlation Engine triggered the alert related to unauthorised access. **The SOC operator** reviewed the alert and forwarded it to the IPS and the CAS. The Correlation Engine triggered the alert related to the PA message receipt. The **SOC operator** reviewed the alert and forwarded it to the IPS and the CAS. The **AOC operator** is notified for the incident through the CAS to handle the incident.	The physical attacker enters the PA room as the doors have been successfully unlocked by Attacker 1; accesses the PA server; and broadcasts messages via the PA system (video). Implemented at Airport site: The **SOC operator** reviewed from the IMP screen the alert raised by the Correlation Engine for unauthorised access and the alert related to the PA message and passed it to the IPS and CAS. The IPS processed the information and produced simulation results. The **SOC operator** reviewed the simulation report from the IMP and aggregated the alerts of unauthorised access and related to the PA message to register a unified incident. The SOC operator further explored information reported from the SMS-I. The **AOC operator** received the incident and reviewed it to undertake proper actions.
6. Third attack to ABC system	6.1 While travellers still scan their passports, the malware (changes its			**All travellers** scanning their passports at the ABC gates are blocked from crossing the

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	functionality) and the checks are always positive (“Hit”) This means that the passport and the travellers’ authentication are always rejected. The ABC-gates block all crossings, requiring that each person passes a background check. This essentially blocks all entries and exits			border control (video).
	6.2 The travellers blocked in the e-gates lanes refer to the ABC officers. To do that, the ABC Officers manually open the gates and perform manual checks.			As the **travellers** at the blocked ABC gates refer to the **ABC officers**, the latter manually open the ABC gates and perform manual checks (video).
	6.3 The ABC officer uses continuously the PAD. Every time the ABC officers use the PAD, an alert is sent automatically by the PAD to the correlation engine.	Passenger Anomaly Detection (PAD) Correlation engine	A low severity alert is sent automatically by the PAD to the correlation engine.	The **ABC officer on duty** performs manual checks using the PAD (video). Every time the ABC officer uses the PAD, a low severity alert is sent automatically by the PAD to the correlation engine.
	6.4 As the ABC officers use the PAD for more than 12 times in 10 minutes, an alert will be sent automatically by the correlation engine to IMP. This alert will be marked as having MEDIUM severity. The incident will be then forwarded to the Impact Propagation	Passenger Anomaly Detection (PAD) Correlation engine Incident Management Portal (IMP)	A medium severity alert is sent automatically by the correlation engine to the IMP. **The SOC operator (L1)** is notified for the medium severity alert though the IMP. The incident will be then forwarded to the Impact	As the **ABC officers** at the airport use the PAD for more than 12 times in 10 minutes, an alert is sent automatically by the correlation engine to the IMP. This alert is marked as medium severity. **The SOC operator (L1)** is notified for the medium severity alert though the IMP.

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
	Simulation and to the CAS.		Propagation Simulation and to the CAS. The SOC operator through the IPS can understand how the congestion at the border control affects the other assets at the airport which is represented in the network model. Also, the congestion is visualised through the Agent Based Model (ABM).	The incident is then forwarded to the Impact Propagation Simulation and to the CAS. The SOC operator through the IPS can understand how the congestion at the border control affects the other assets at the airport which is represented in the network model. Also, the congestion is visualised through the Agent Based Model (ABM).
	6.5 Additionally, the malware disables the button that enables a manual opening of the ABC-gates' doors. Hence, the ABC-officers are unable to free the travellers trapped inside the ABC-gates and let anyone pass, causing panic to the travellers.			**Travellers** at the airport are trapped between the ABC gates. The **ABC officers on duty** are unable to free the **travellers** as the button is disabled (video).
7. Alerts aggregation	7.1 The SOC operator aggregates the alerts received from steps 4, 5 and 6 and this will be forwarded to the CAS and to the Impact Propagation Simulation	Correlation engine Incident Management Portal (IMP) Crisis Alerting System (CAS)	The **SOC operator (L2)** aggregates the alerts relevant to the PAD (steps 4,6), the PA and the AC (step 5), into a medium severity incident. The incident is forwarded to the CAS. The **AOC operator** is notified for the incident through the CAS. The material from the camera is used and the	The **SOC operator (L2)** aggregates the alerts relevant to the PAD (steps 4,6), the PA and the AC (step 5), into a medium severity incident. The incident is forwarded to the CAS. The **AOC operator** is notified for the incident through the CAS. The material from the camera is used and the congestion at the ABC gates is confirmed.

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
			congestion at the ABC gates is confirmed. The AOC operator escalates the incident to the Police for further investigation through email and SMS. The Hellenic Police immediately sends a patrol car at the airport for further investigation.	The AOC operator escalates the incident to the Police for further investigation through email and SMS. The Hellenic Police immediately sends a patrol car at the airport for further investigation.

3 SATIE response

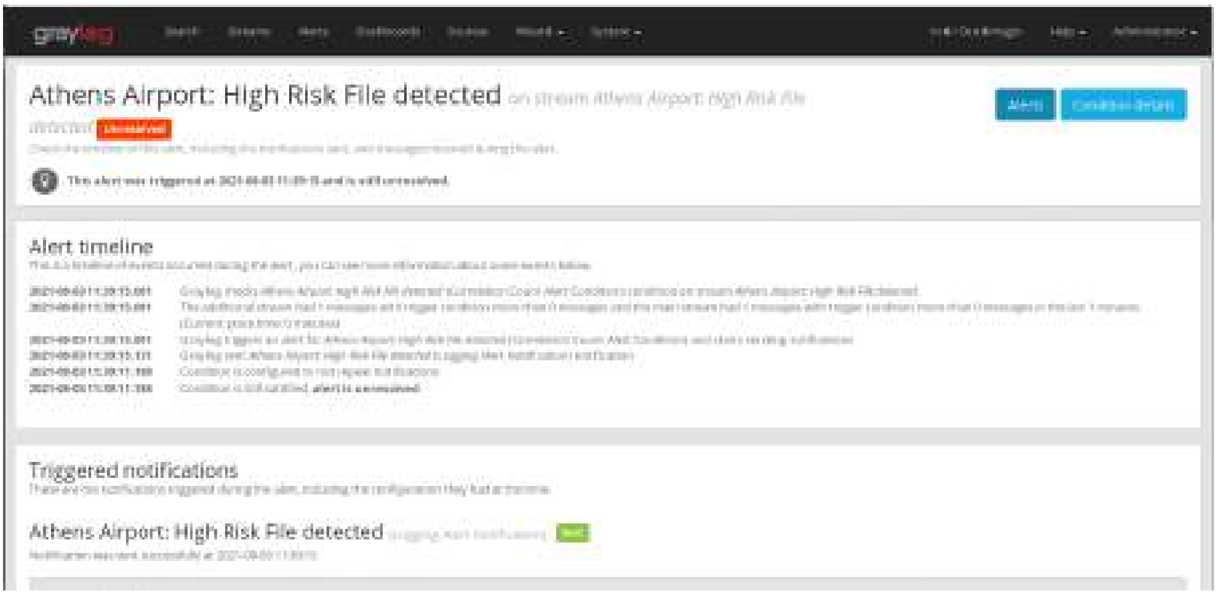
This chapter presents how the SATIE Solution and the accompanying components have been used to detect the cyber, physical and hybrid threats of the attack scenarios described in sections 2.4.1 and 0.

3.1 Correlation Engine

The Correlation Engine (CE) was used in Scenario #1 and #2. It received events from the physical and cyber SATIE threat detection systems, and also directly from the Operating Systems (OS) and network on the airport (Figure 3.1).

Figure 3.1: Correlation Engine events

With different rules defined, alerts were raised to the Incident Management Portal. The Figure 3.2 below, shows an example of an alert. Table 3.1 shows the alerts raised in Scenario #1, and the Table 3.2 displays the alerts raised in Scenario #2.



Athens Airport: High Risk File detected [illegible]

[illegible]

Alert timeline

[illegible]

Triggered notifications

[illegible]

Athens Airport: High Risk File detected [illegible]

Figure 3.2: Example of a Correlation Engine alert

Table 3.1: Alerts raised in Scenario #1

Time	Title	Detection systems	Affected Assets
00:03	High risk file detected	Malware Analyser	FIDS Workstation
00:05	Suspicious PowerShell Command detected	OS events	FIDS Workstation
00:08	Suspicious file uploaded	OS events	FIDS Workstation
00:15	Suspicious PowerShell Command detected	OS events	Domain Controller
00:18	High risk file detected	Malware Analyser	Domain Controller
00:26	Suspicious PowerShell Command detected	OS events	FIDS
00:27	Suspicious PowerShell Command detected	OS events	Access Control
00:35	Unauthorized access to the PA room	UAC	PA room
00:40	Evacuation request	Airport event	Muster station

Table 3.2: Alerts raised in Scenario #2

Time	Title	Detection systems	Affected Assets
00:01	USB Connection	OS events	ABC computer
00:15	Abnormal use of PAD possible congestion at the border control	ADPR	Border control
00:18	Unauthorized access to the Public Announcement area	UAC	Public Announcement
00:21	Possible unauthorized PA message broadcasted	PA events	Passport control area
00:22	Abnormal use of PAD congestion at the border control	ADPR	Border control

3.2 Malware Analyser

For Scenario #1, the Malware Analyser has to detect the first step when a corrupt word document is downloaded on the computer as visualized in Figure 3.3 below.

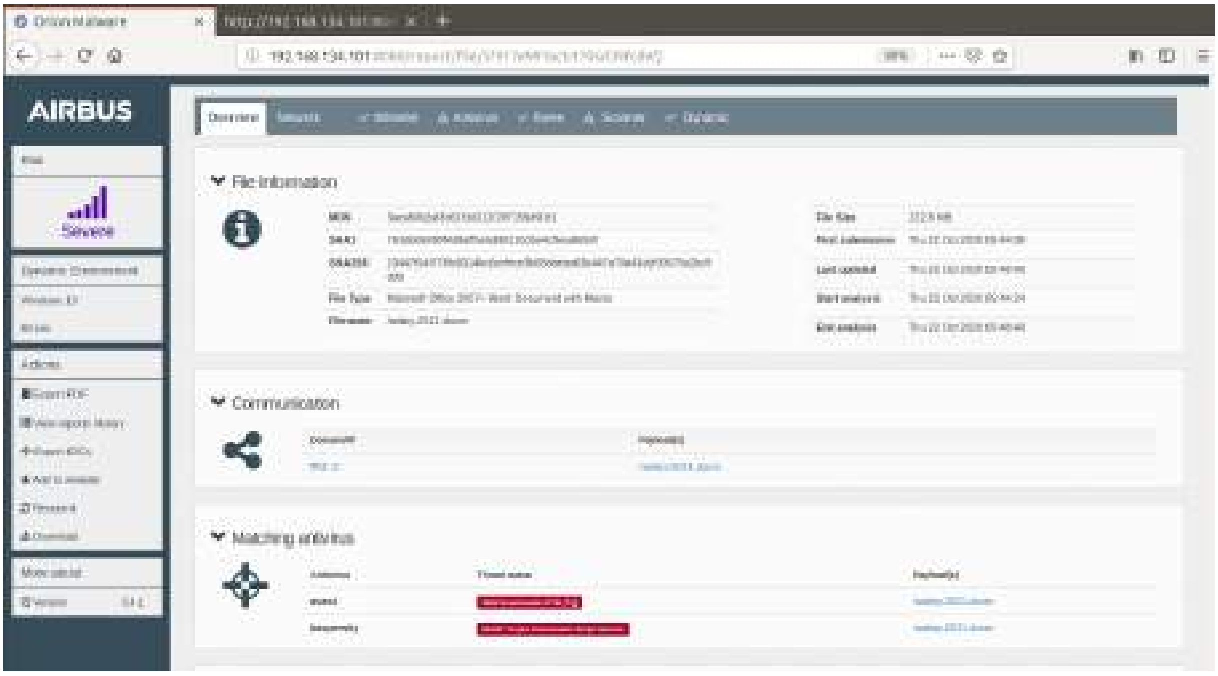


Figure 3.3: Malware Analyser report about corrupt word document

The file was detected as a severe risk, due to the suspicious macro. The antivirus detects the threat, but also the dynamic analysis shows suspicious file activity, and network activity.

A second step was detected by the Malware Analyser, when a schedule task is created on the domain controller. The malware analyser detects that the eXtensible Markup Language (XML) file is actually a payload, as show in Figure 3.4.

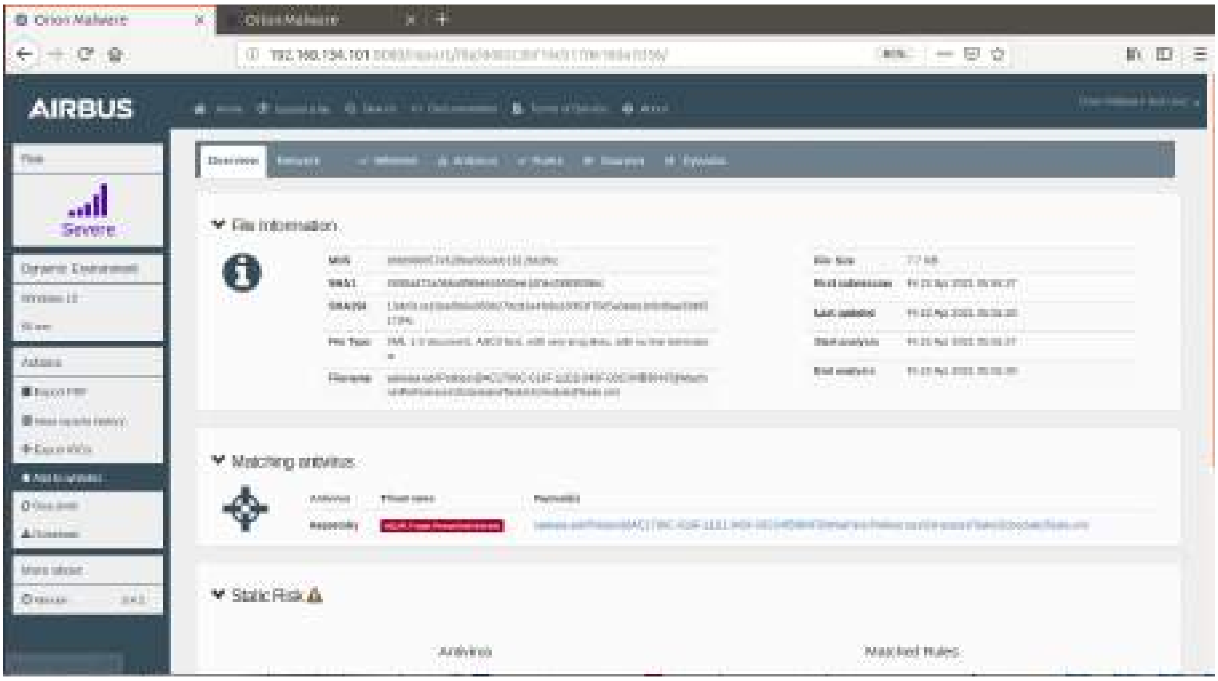


Figure 3.4: Malware Analyser report about corrupt XML file

The file was detected as a severe risk, the antivirus detects that the file contains a suspicious PowerShell command.

3.3 Incident Management Portal

The Incident Management Portal received alerts from the Correlation Engine. An operator checks each alert, and assign it to another operator that 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, the alert will be sent to the Impact Propagation Simulation (IPS) and Crisis Alerting System (CAS). Table 3.3 depicts the alerts and incidents raised in Scenario #1. Table 3.4 shows the alerts and incidents raised in Scenario #2.

Table 3.3: Alerts and incidents raised in Scenario #1

Time	Title	Severity	Affected Assets	Operator actions
00:03	High risk file detected	High	FIDS Workstation	Raised an incident and send to IPS and CAS
00:05	Suspicious PowerShell Command detected	Medium	FIDS Workstation	
00:08	Suspicious file uploaded	Low	FIDS Workstation	Aggregate the first 3 alerts
00:15	Suspicious PowerShell Command detected	Medium	Domain Controller	Aggregate the 4 alerts, convert to incident and send the incident to IPS and CAS
00:18	High risk file detected		Domain Controller	
00:26	Suspicious PowerShell Command detected	Medium	FIDS	
00:27	Suspicious PowerShell Command detected	Medium	Access Control	
00:35	Unauthorized access to the PA room	Medium	PA room	Aggregate and raised an incident, and send to IPS and CAS
00:40	Evacuation request	Medium	Muster station	

Table 3.4: Alerts and incidents raised in Scenario #2

Time	Title	Severity	Affected Assets	Operator actions
00:01	USB Connection	Low	ABC computer	No action
00:15	Abnormal use of PAD possible congestion at the border control	Low	Border control	Raised an incident and send to IPS and CAS
00:18	Unauthorized access to the Public Announcement area	Medium	Public Announcement	Aggregate and raised an incident, and send to IPS and CAS
00:21	Possible unauthorized PA message broadcasted	Medium	Passport control area	

Time	Title	Severity	Affected Assets	Operator actions
00:22	Abnormal use of PAD congestion at the border control	High	Border control	Raised an incident and send to IPS and CAS

The Figure 3.5: shows the alert raised in the Incident Management Portal for Scenario #2.

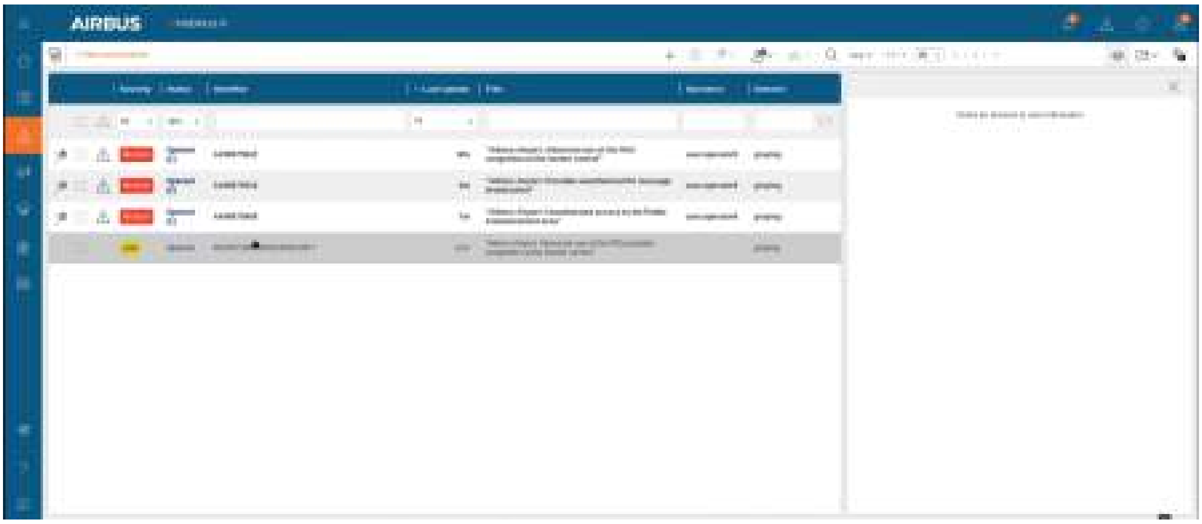
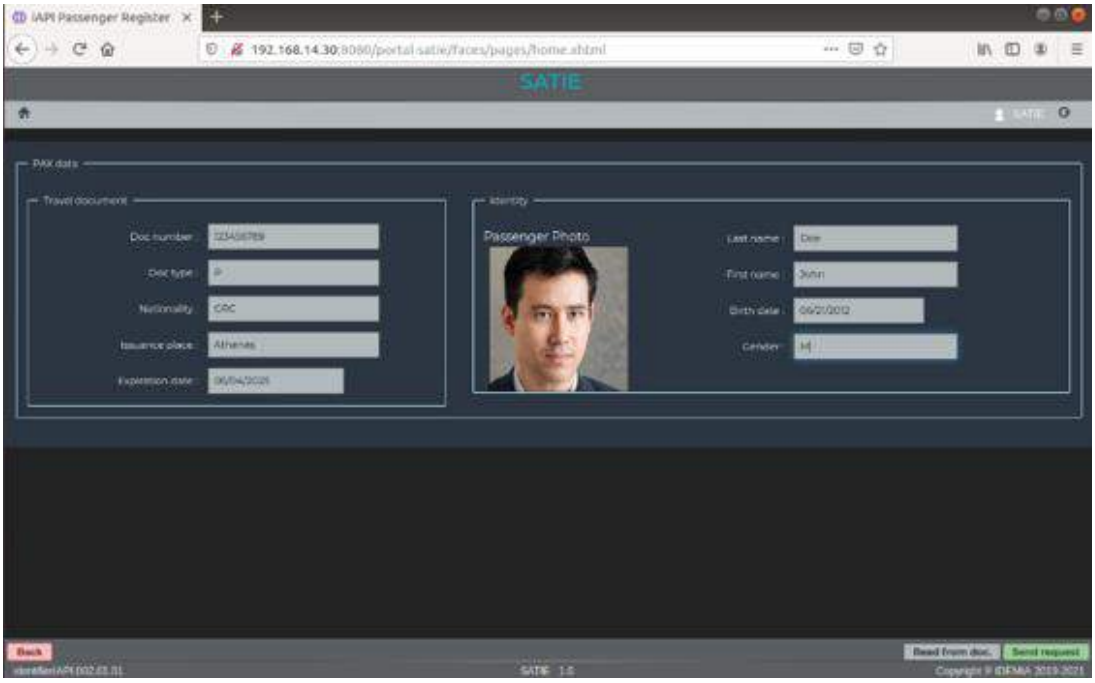


Figure 3.5: Alerts of Scenario #2

3.4 Anomaly Detection on Passenger Records

For scenario #2, the Anomaly Detection on Passenger Record was used to offer a second source of verification of the threat of passenger at the Automated Border Control. By using a passport reader and an intuitive graphical interface, as shown in Figure 3.6, the Police Duty Officer can simply check the passenger information against a database of known threat to help him took a decision. With real time response about the potential threat of a passenger, the Police Duty Officer can ensure to still manage the passenger flow in an efficient way while keeping the security of the border crossing process.

In addition, ADPR system is part of the SATIE solution and sends alert and events for the SOC agents to take decision and react about threat detected or dysfunction of a system as presented in this scenario.



iAPI Passenger Register
192.168.14.30:8080/portal-satie/faces/pages/home.xhtml
SATIE
SATIE
Back
Read from doc.
Send request
SATIE 1.0
Copyright © IDEMIA 2019-2021

PAX data

Travel document

Doc number : 123456789

Doc type : P

Nationality : CRC

Issuance place : Athenes

Expiration date : 06/04/2026

Identity

Passenger Photo

Last name : Doe

First name : John

Birth date : 06/21/2012

Gender : M

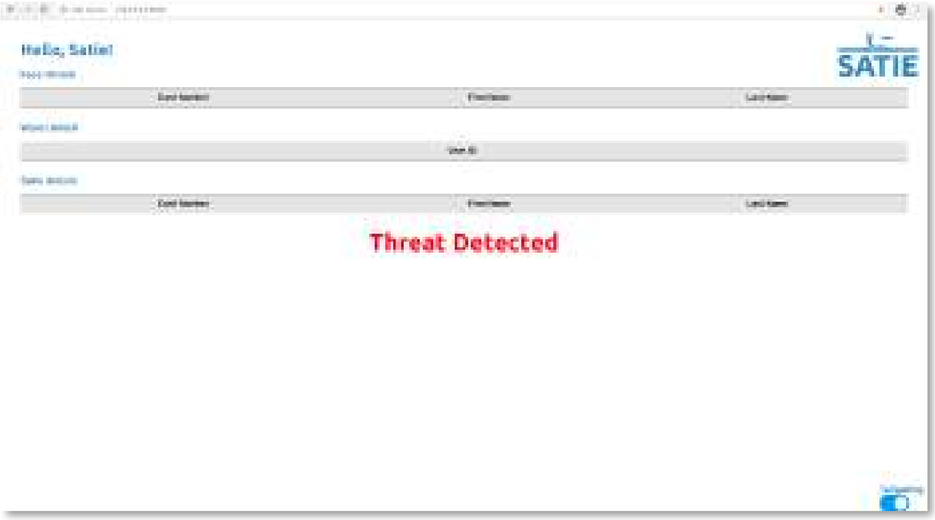
Figure 3.6: Screen capture of ADPR graphical interface

3.5 Unified Access Control

For Scenario #1 and #2, the Unified Access Control was used to trigger an alert based on the face identification of somebody listed in a watchlist of threat. Placed behind the door of the PA room, the camera and Augmented Vision detect a face, identify this individual according to reference image in the threat watchlist.

Once identification is completed, the Unified Access Control send an automated alert to the SATIE Correlation Engine signalling there is a threat detected at the entrance of the PA room. The Correlation Engine interpret this alert with high risk and immediately escalate it to the Incident Management Portal. Once received by the IMP, SOC operators can react accordingly based on the level of the threat.

Figure 3.7 and Figure 3.8 show the administration interface and the nominal process of the Unified Access Control system.



Threat Detected

Figure 3.7: Screen capture of internal Unified Access Control tool to retrieve results from face identification. Threat detected capture similar to demo in AIA

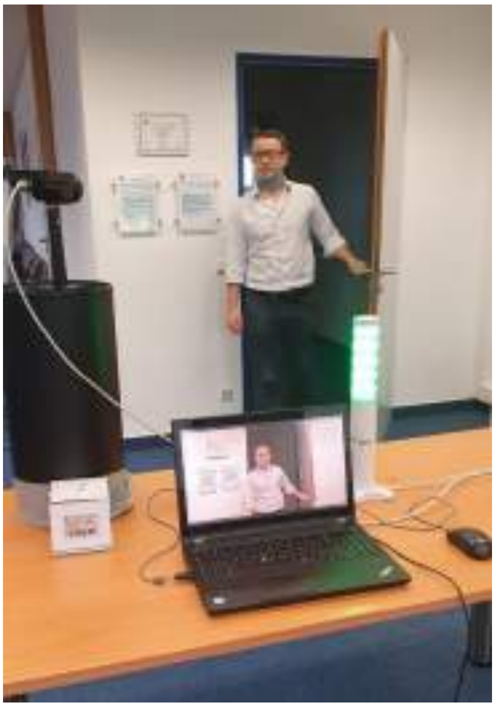


Figure 3.8: Photo of the Unified Access Control system deployed for the demo at AIA with camera, LED tower feedback and Augmented Vision computer

3.6 Impact Propagation Simulation (IPS)

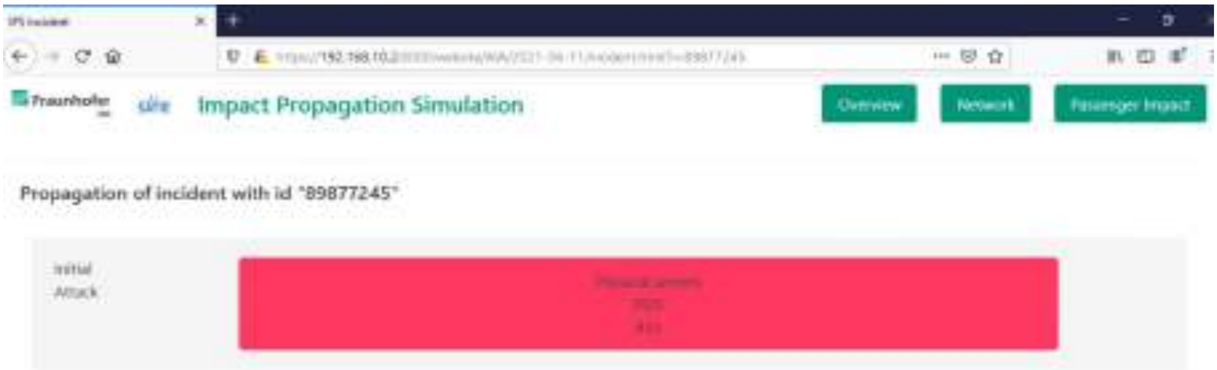
The IPS received single and aggregated incidents during the demonstration on June 11. The incidents are listed in Table 3.5. These incidents are forwarded by the SOC operator who uses the Incident Management Portal (IMP). The SOC operator can choose alerts which he classifies as incident and forwards them either as single or aggregated incident to 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. From Table 3.5, it can be observed that the SOC operator sent some incidents twice and that aggregated alerts contain some information that has been sent before as single incident.

Table 3.5: Incidents received during scenario 1 and 2.

Scenario	Time (CEST)	Incident ID	# of unique alerts	Systems/assets impacted	ABM trigger
1	11:57	89877245	1	FIDS	-
	12:10	89877296	3	AC, Muster stations	Evacuation
	12:20	89877263	7	FIDS, AC, Muster stations, Domain controller	Evacuation
	12:21	89877263	7	FIDS, AC, Muster stations, Domain controller	Evacuation
2	14:29	89877323	1	ABC	50% rejection
	14:42	89877330	3	AC, PA	-

Scenario	Time (CEST)	Incident ID	# of unique alerts	Systems/assets impacted	ABM trigger
	14:52	89877342	2	ABC	50% and 100% rejection
	14:54	89877323	5	ABC, PA	50% rejection
	14:59	89877323	5	ABC, PA	50% rejection

The very first incident that has been received with the ID “89877245” was an attack on the physical server of the Flight Information Display System (FIDS) which is presented in Figure 3.9.



Propagation of incident with id "89877245"

Figure 3.9: First incident received from IMP

In this incidents-view, only one impacted asset can be presented. However, the network-view enables to present all received incidents in specific graphs. Figure 3.10 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 3.11 but here the number of undisturbed assets is presented as a function of time. This graph view enables to capture both sets of attacks, one around lunch time and the other in the afternoon, at a glance. As given in Table 3.5, some incidents have triggered the Agent-Based Model (ABM) where two main scenes have been simulated and saved as video files, i.e. (1) the evacuation of the terminal and (2) the rejection of passengers are the e-gates. These two scenes are presented as screenshots in Figure 3.12 and Figure 3.13.

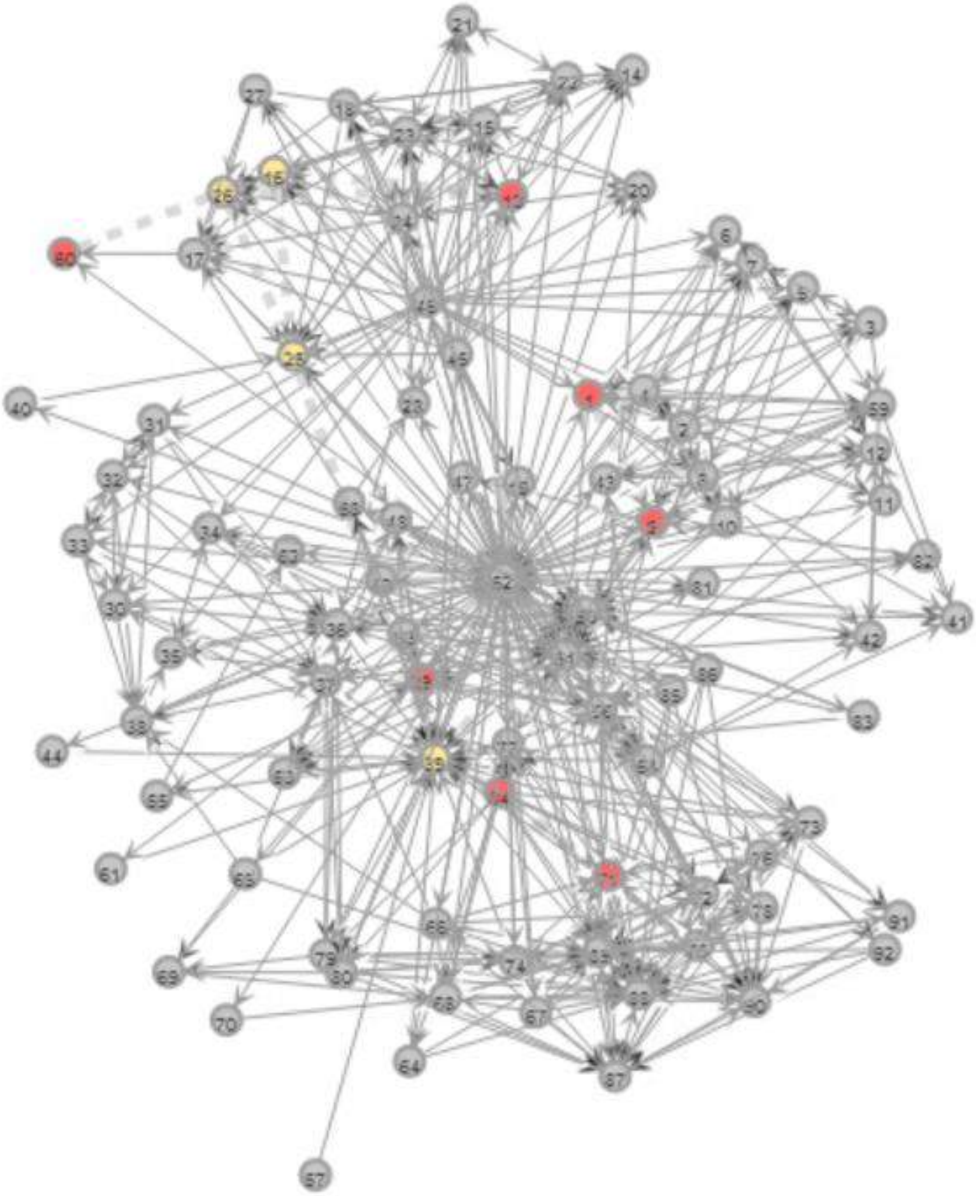


Figure 3.10:All nodes that have been attacked (red) on June 11

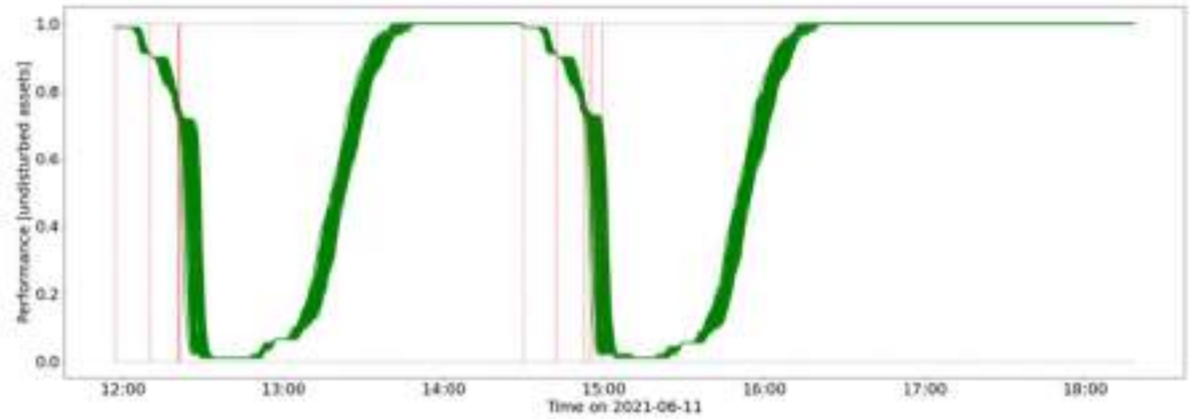


Figure 3.11: All nine incidents (red vertical lines) received on June 11. The number of nodes of the network which is undisturbed is given as green lines for repeated simulations

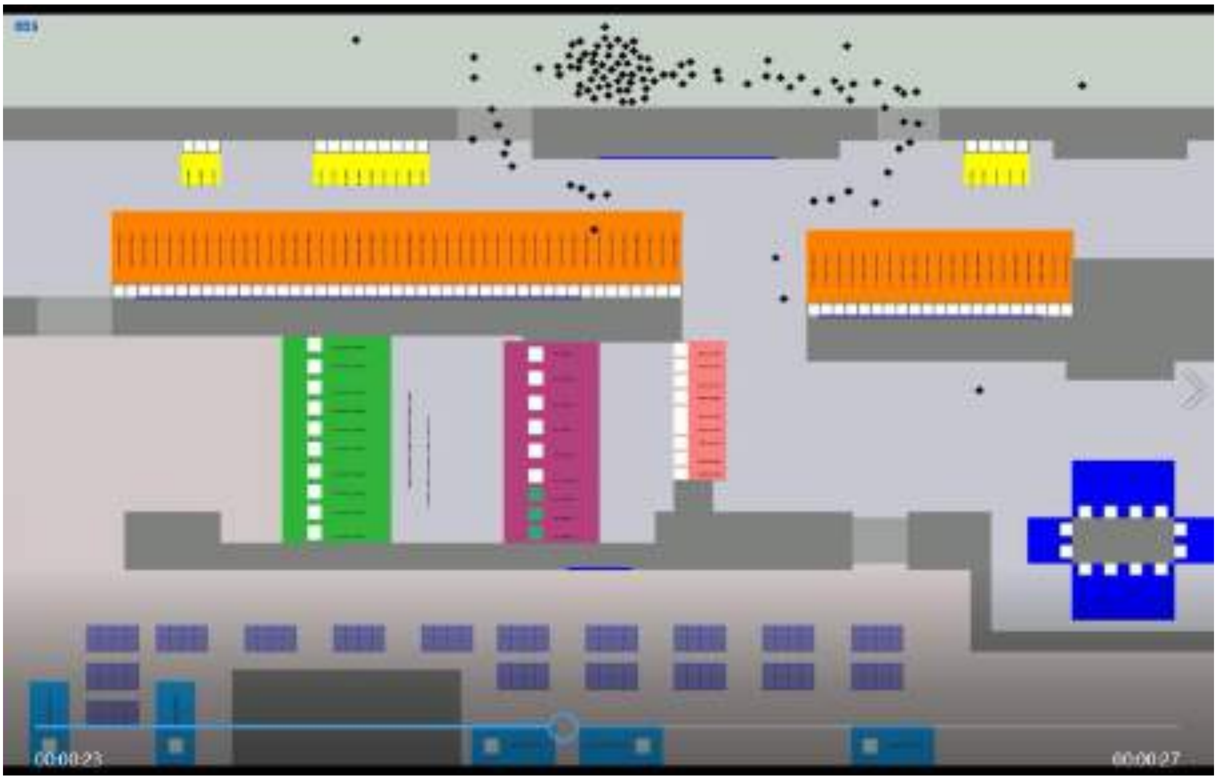


Figure 3.12: Screenshot of the ABM evacuation video which has been shown similarly on June 11 triggered by Incident ID 89877296

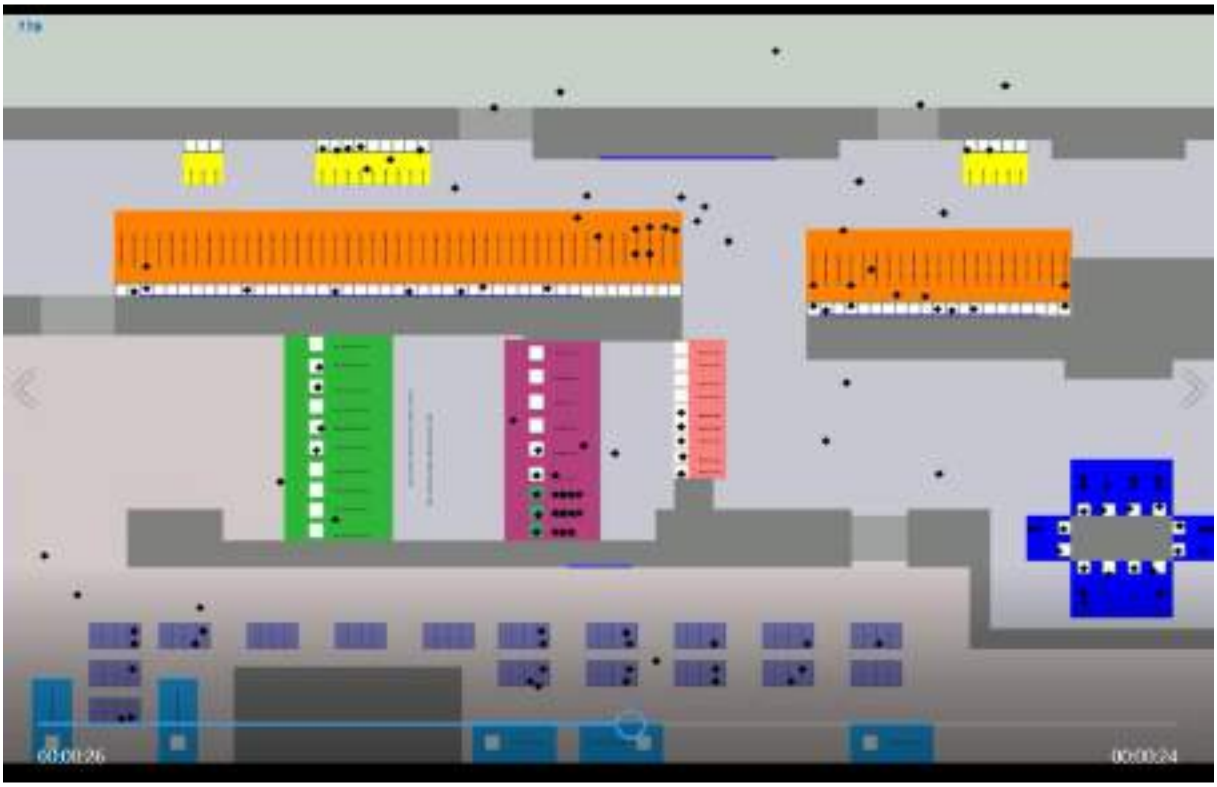


Figure 3.13: Screenshot of the ABM rejection video which has been shown similarly on June 11 triggered by Incident ID 89877342

All this information, is also visible to the AOC operator. During the demonstration, the AOC operator had to react quite fast to incoming incidents and communicate to the respective agencies such as the police. In 'down-times', when the AOC operator was waiting for some incidents to be received, the IPS results were studied and provided some insights on the severity of the incident and the impact on specific assets or the passengers. More information on the IPS can be found in (3), (1) and (4).

3.7 Crisis Alerting System (CAS)

The Crisis Alerting System (CAS) has been deployed at the AOC, providing to the operators' alarm management, notification and collaboration functionalities that were useful to their activities that had to execute during the two scenarios.

The role of CAS was twofold:

1. To collect the operational information produced by multiple sources, such as the SOC (incident management and impact assessment) and the airport's safety systems (e.g. CCTV). This information was combined and presented to the AOC operators creating a common operational picture.
2. To provide a smart notification and collaboration mechanism, enabling the notification of the first responders and the safety agencies that had to be involved in the situation. The collaboration among the AOC operators and the involved actors/responders was supported.

During the execution of the two scenarios, a number of events were forwarded from SOC to AOC operators as displayed in Table 3.6.

Table 3.6: Events forwarded to the AOC operators (CAS).

Scenario	Time (CEST)	Incident ID
1	11:57	89877245
	12:10	89877296
	12:20	89877263
	12:21	89877263
2	14:29	89877323
	14:42	89877330
	14:52	89877342
	14:54	89877323
	14:59	89877323

AOC operators, through the "Alarm Management" perspective of CAS, were able to be informed about the list of the active events and the related information produced by the IPS as depicted in Figure 3.14. Considering this information, they were able to organize their actions and take decisions.

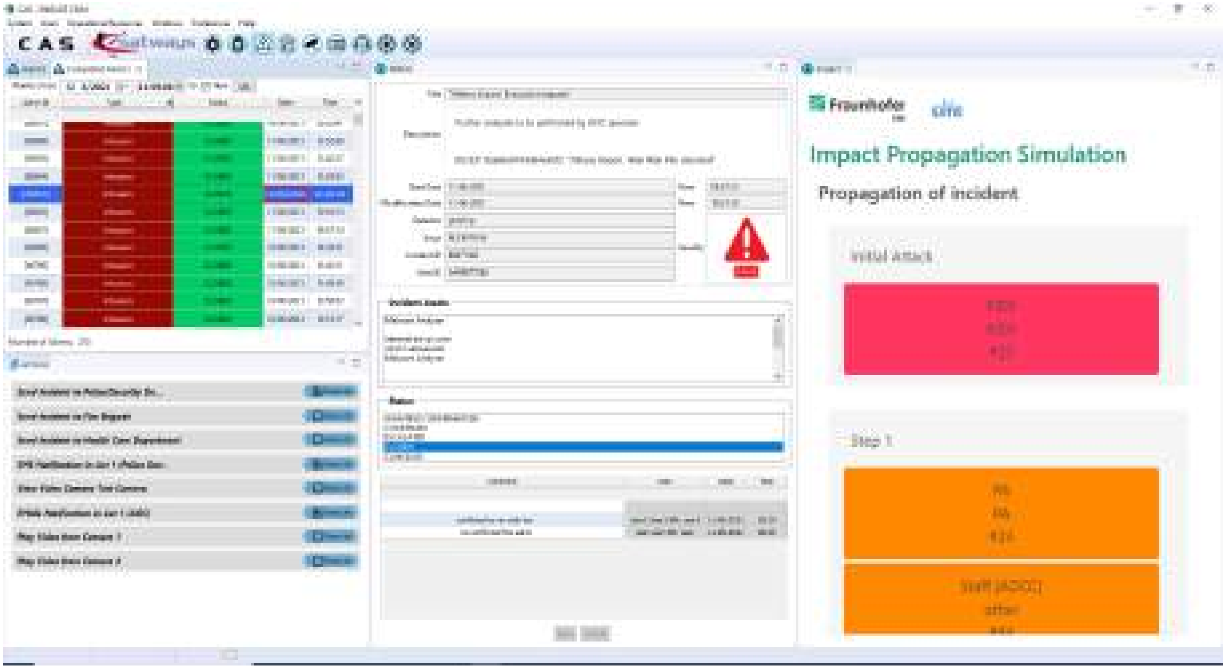


Figure 3.14: CAS – Alarm Management perspective.

Additionally, through the Collaboration perspective, AOC operators were able to notify the public safety agencies and responders that had to be involved in the situations, which is indicatively shown in Figure 3.15. During the two scenarios, a number of notifications (emails and SMSs) were produced and forwarded from the CAS to the related public safety agencies (e.g. Police). Additionally, all actors were able to communicate and collaborate through the collaboration perspective.

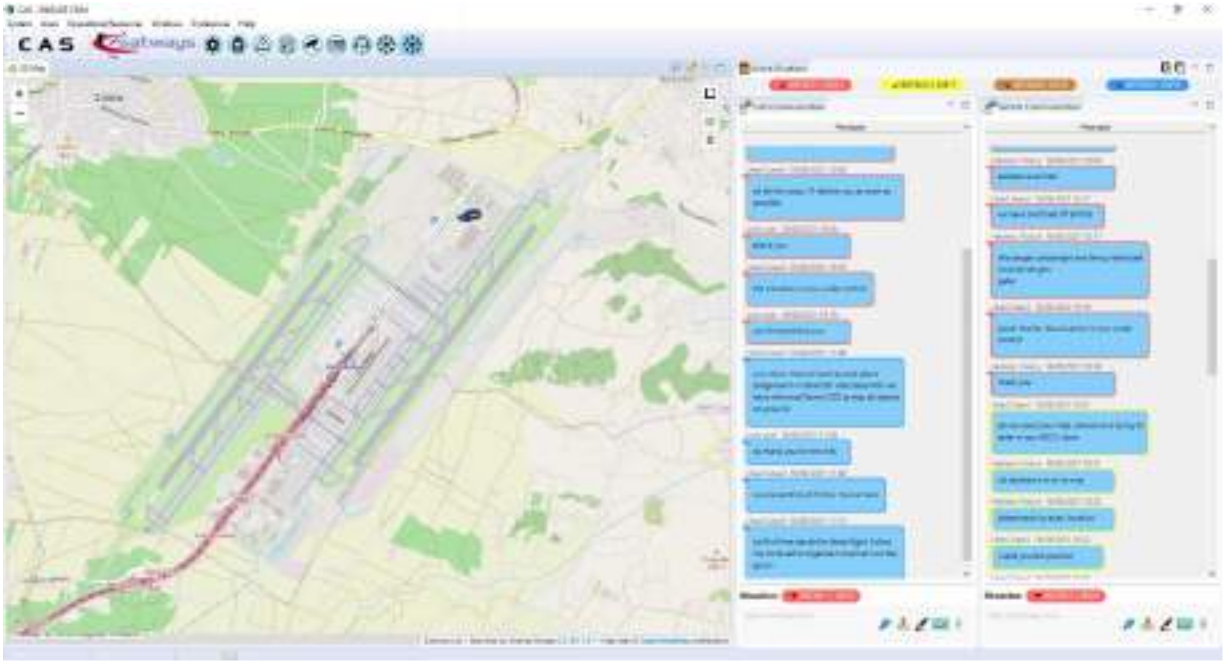


Figure 3.15: CAS – Collaboration perspective.

3.8 Investigation Tool (SMS-I)

SMS-I, as a decision support tool, analyses the data generated by the different SATIE Tools, over different time frames, and 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.

Therefore, 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's time-lines. Figure 3.16 shows a representation of all alerts and incidents that occur during the execution of Scenario #2. This view is interesting since the SOC operator can see the events in chronological order.

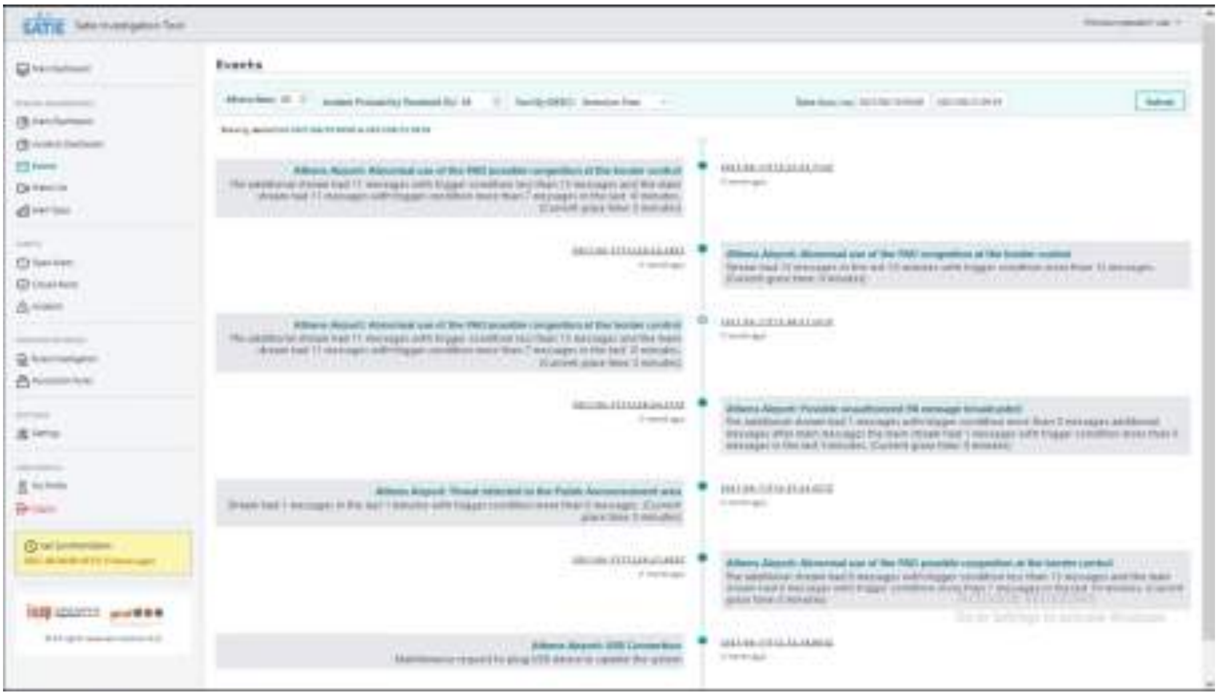


Figure 3.16: Alerts and Incidents of Scenario #2 displayed in SMS-I

The SOC operator can get all the information of each event clicking on it (see Figure 3.17), which can help him in the investigation of the attack.

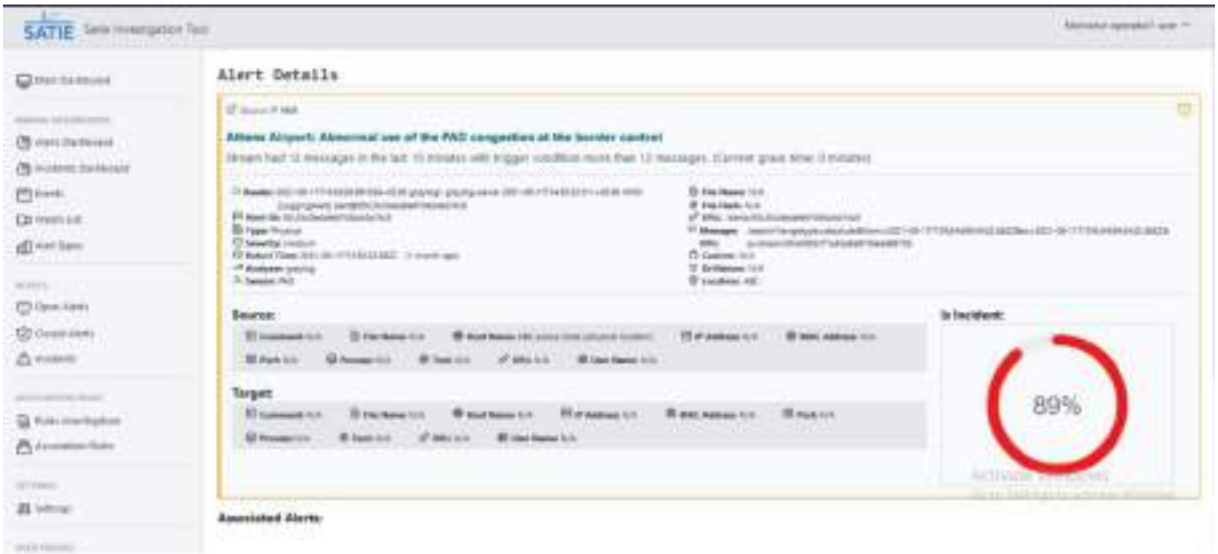

SATIE
Alert Details
Athens Airport: Abnormal use of the PAD congestion at the border control
Source:
Target:
Is Incident:
89%
Associated Alerts:

Figure 3.17: Alert details displayed in SMS-I

Note that several details are provided in this window, namely the sensor that raised the alert, the severity and the type of the sensor. The probability of this alert be an incident is also provided.

The SOC operator can also see all the incidents raised by IMP (Figure 3.18).

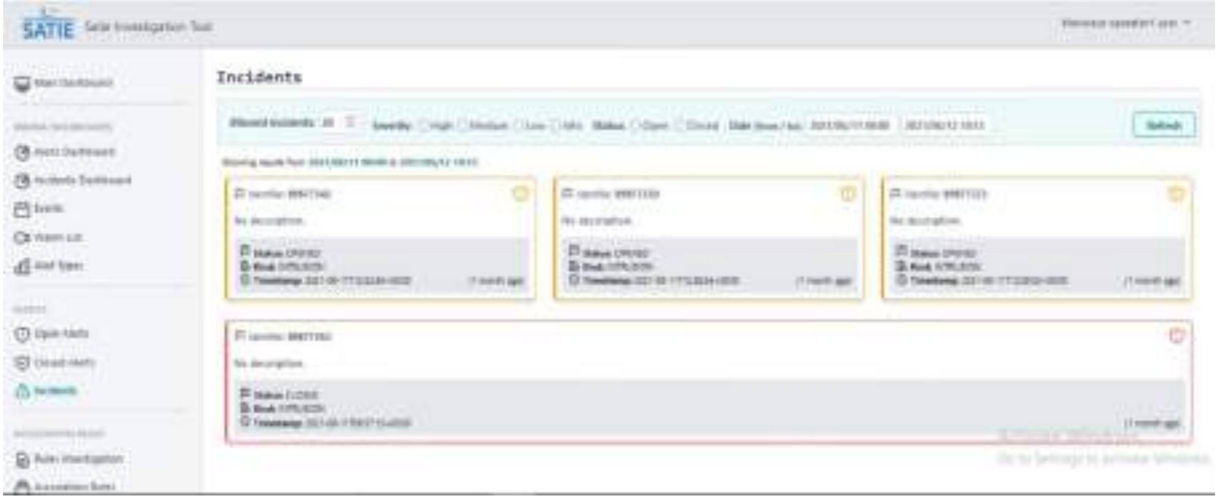
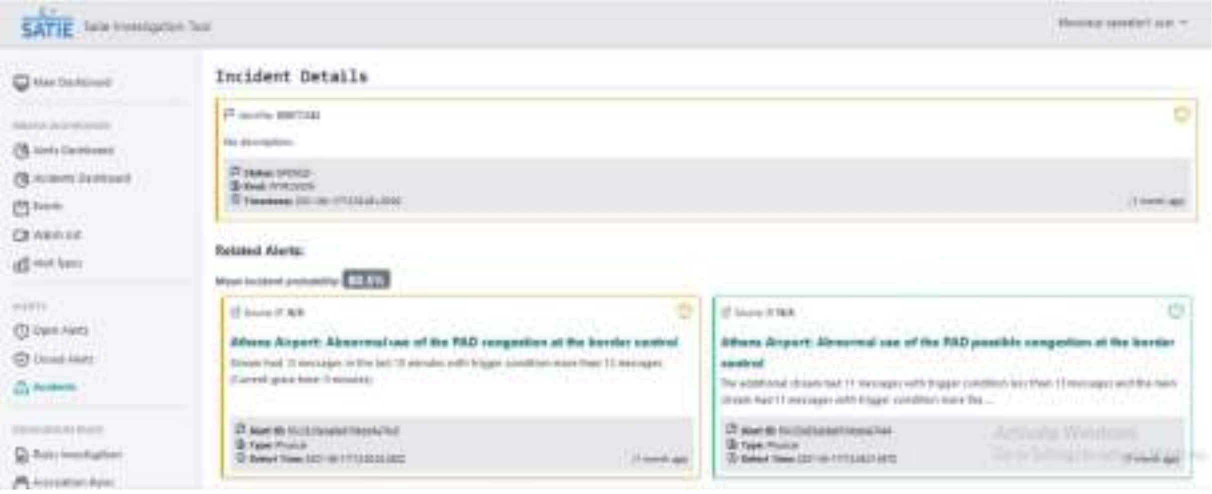


Figure 3.18: SMS-I’s Incidents List

For each incident, the SOC operator can see its details and understand which alerts originate the incident (Figure 3.19). For example, if two alerts were aggregated to generate an incident, as happened in Scenario #2, both alerts can be seen in the incident details.



Athens Airport: Abnormal use of the PAD congestion at the border control

Athens Airport: Abnormal use of the PAD possible congestion at the border control

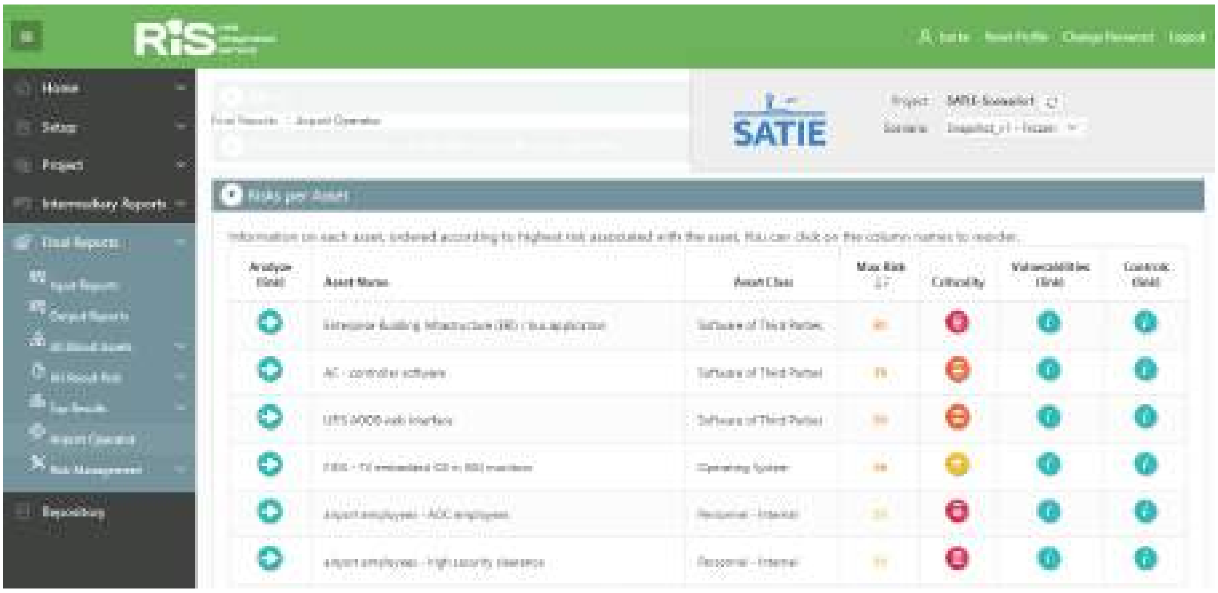
Figure 3.19: Incident details displayed in SMS-I

It also shown in this incident details the mean of incident probability. 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 is the probability of intelligent system 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 in this document are just some of the views available in the SMS-I intelligent dashboard. The SOC operator can use the view 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, as well as updating exactly how well each control is in place per airport operation.



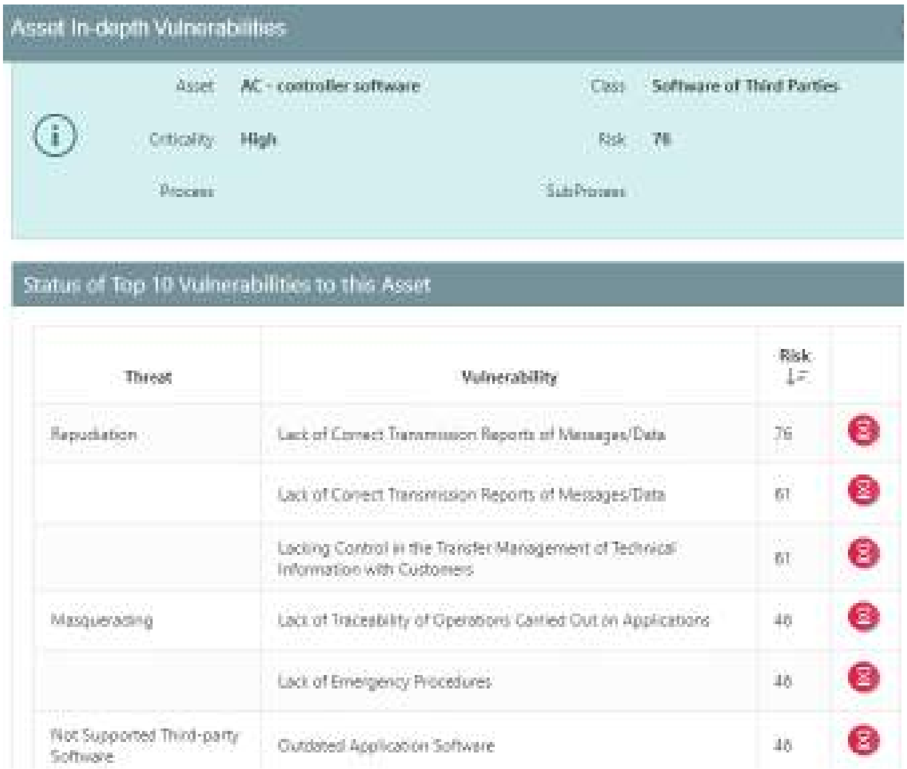
Risks per Asset

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

Analyze (link)	Asset Name	Asset Class	Max Risk	Criticality	Vulnerabilities (link)	Controls (link)
	Enterprise Building Infrastructure (EBI) - bus application	Software of Third Parties	[illegible]			
	AC - controller software	Software of Third Parties	76			
	UPS 9000 web interface	Software of Third Parties	[illegible]			
	EBIS - T? embedded OS in EBI machines	Operating System	[illegible]			
	Airport employees - AOC employees	Personnel - Internal	[illegible]			
	Airport employees - high security clearance	Personnel - Internal	[illegible]			

Figure 3.20: The Airport Operator page of RIS showing the assets with the highest risks

The results of the first scenario taking place at AIA demonstrate that the asset with the second highest risk was one related to Access Control, specifically the controller software (see Figure 3.20), and the threats contributing the most to that high risk value were masquerading and unauthorized use of the software (see Figure 3.21). These results highlight that the airport should address countermeasure efforts to reduce these risks. And in fact, the scenario demonstrated that an attacker masqueraded and used the access control software without authorization to modify credentials and allow another attacker to gain access to security restricted areas.



Asset In-depth Vulnerabilities

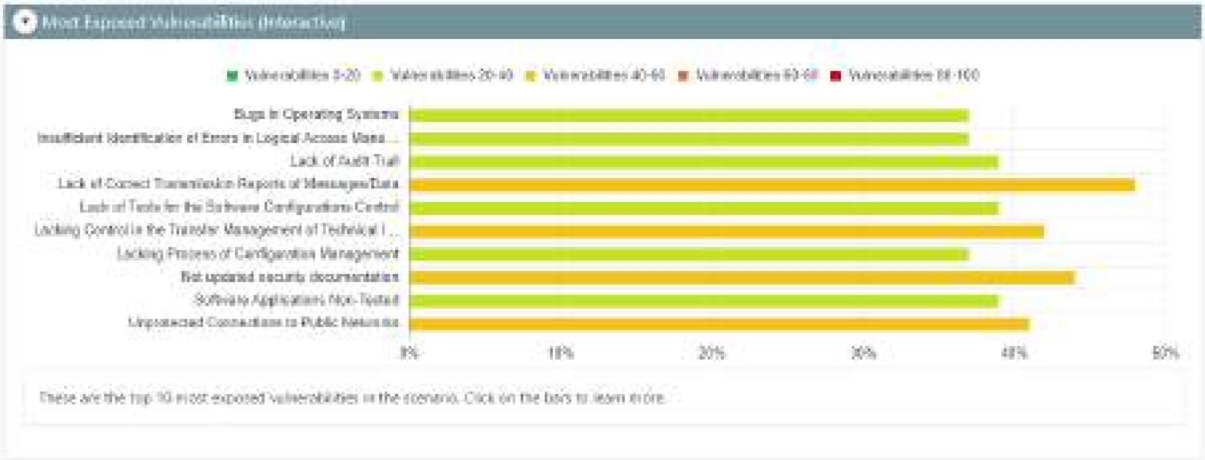
Asset: AC - controller software
Class: Software of Third Parties
Criticality: High
Risk: 76
Process:
SubProcess:

Status of Top 10 Vulnerabilities to this Asset

Threat	Vulnerability	Risk	
Repudiation	Lack of Correct Transmission Reports of Messages/Data	76	
	Lack of Correct Transmission Reports of Messages/Data	61	
	Lacking Control in the Transfer Management of Technical Information with Customers	61	
Masquerading	Lack of Traceability of Operations Carried Out on Applications	46	
	Lack of Emergency Procedures	46	
Not Supported Third-party Software	Outdated Application Software	46	

Figure 3.21: The threats and vulnerabilities most contributing to the high risk of the AC controller software

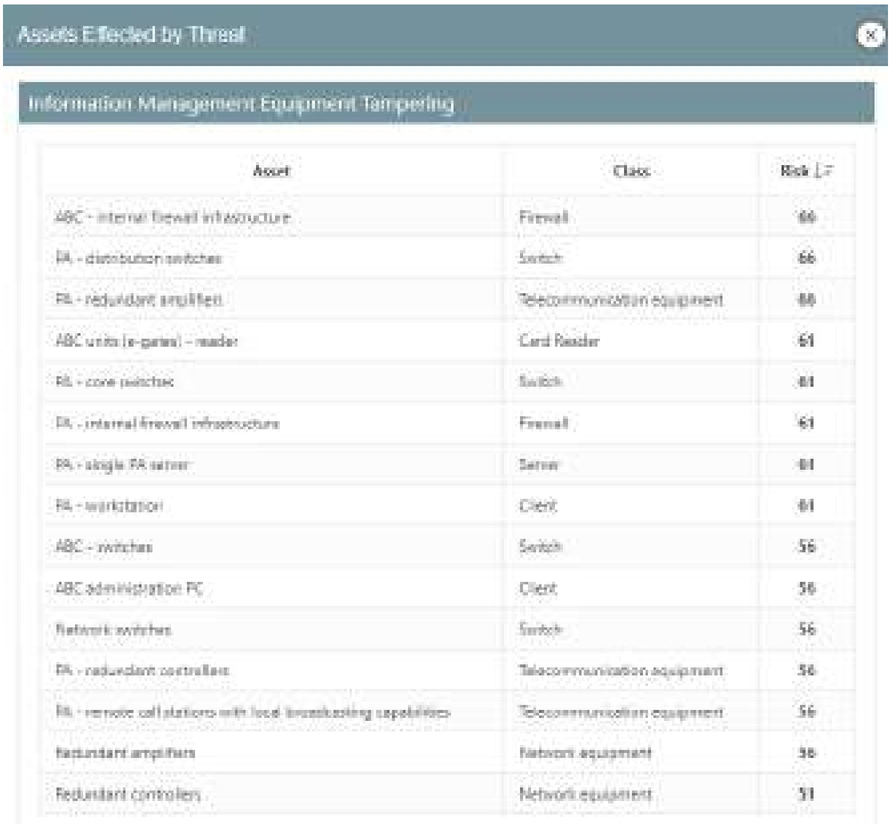
For the second scenario taking place at AIA, the asset with the highest risk is the Automatic Boarding Control (ABC) system. The vulnerabilities contributing the most to this risk are software-related: bugs in operating systems, lack of procedures for change management and configuration management. Looking at the most exposed vulnerabilities in general for this scenario, there are the many of the same ones (see Figure 3.22), including bugs in operating systems, change management and configuration management. This indicates that the ABC system is not unique in being affected by these vulnerabilities because they are risky for this scenario as a whole, and thus create real weaknesses for software in general.



These are the top 10 most exposed vulnerabilities in the scenario. Click on the bars to learn more.

Figure 3.22: The most exposed vulnerabilities in Athens Scenario #2

The threat with the highest associated risk in general for this scenario is considered one of terrorism and sabotage, specifically information management equipment tampering, which can impact 15 assets (see Figure 3.23). Within these assets are some related to ABC assets, which highlights that the ABC system in general is at a high risk, as well as apparently the PA system.


Assets Effected by Threat
Information Management Equipment Tampering

Asset	Class	Risk
ABC - internal firewall infrastructure	Firewall	66
PA - distribution switches	Switch	66
PA - redundant amplifiers	Telecommunication equipment	66
ABC units (e-gates) – reader	Card Reader	61
PA - core switches	Switch	61
PA - internal firewall infrastructure	Firewall	61
PA - single PA server	Server	61
PA - workstation	Client	61
ABC - switches	Switch	56
ABC administration PC	Client	56
Network switches	Switch	56
PA - redundant controllers	Telecommunication equipment	56
PA - remote call stations with local broadcasting capabilities	Telecommunication equipment	56
Redundant amplifiers	Network equipment	56
Redundant controllers	Network equipment	51

Figure 3.23: The assets affected by the threat with the highest risk in Scenario #2

Overall these results have highlighted that the ABC system is highly at risk for someone to maliciously tamper with the information in the system, which is exactly what occurred in the scenario. These kinds of results can be used by the risk manager to understand where the largest weaknesses are in their security measures, and thus where to best address time and effort to reduce risks.

For use during the SATIE demonstrations, the risk assessment results were not based on any real situation neither at the Athens Airport, nor any other airport, but they represent realistic results. Similarly, the scenarios represented realistic, potential attack paths of malicious persons. 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 (5).

4 Evaluation Results

This section presents the evaluation results of the Athens 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 Athens 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 “Annex 1 - Evaluation questionnaire”.

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

- Calculate the final value for each KPI Related to the Athens 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 Athens 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 Athens Airport demonstration and presented in Moreover, the following table displays the KPIs which are relevant to the Athens 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 Athens 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. In the current document, only the cyber and physical attacks implemented during the two demonstration scenarios of Athens Airport are considered.

Regarding the demonstration scenario #1 eight cyber-attacks were committed:

- The cyber attacker sends a spear-phishing email (malware included).
- FIDS workstation compromisation. The cyber attacker uploads a manipulated Remote Administration Tool (RAT) and modifies the service with the incorrect configuration to execute it.
- FIDS workstation compromisation. The cyber attacker exploits the wrong configuration of the service and gets local system account of the FIDS workstation.
- The cyber attacker uploads the exploit “SharGPOAbuse” which allows the modification of the Group Policy Object (GPO) to get access to the domain controller.

- A scheduled task is created on the domain controller policy (which holds a group policy for FIDS and AC systems). The GPO domain controller policy executes that task to compromise the entire domain.
- FIDS compromisation. FIDS credentials are stolen from the clipboard of the compromised workstation. The cyber attacker runs a script to change data in the FIDS database by searching for all flights for that day and shifting them ahead or behind by an hour or two.
- The Access Control system has been compromised.
- The PA system has been compromised.

and the following two physical attacks:

- Unauthorised access to the PA room. The physical attacker enters into a restricted area which leads to the PA room without raising any suspicion.
- Evacuation request message. The physical attacker pushes the evacuation button of the PA system and activates a pre-recorded evacuation message urging passengers and staff to evacuate the terminal building and move to the muster stations.

As a result, Scenario #1 contains ten attacks.

Regarding the demonstration Scenario #2 six cyber-attacks were committed:

- The malware gets installed automatically as soon as the USB stick is plugged in the ABC computer by a compromised Maintenance Worker.
- Abnormal use of ADPR. ABC system displays "No Hit" for scanned passports (All travellers cross the gates).
- Abnormal use of ADPR. ABC system displays ”Random positive deceiving-hits” (Passengers congestion to the Border Control).
- Abnormal use of ADPR. ABC system displays positive “’Hit” (Passengers congestion to the Border Control). The malware disables the button enabling a manual opening of the ABC-gates’ doors.
- Compromisation of the Access Control System.
- Compromisation of the PA system.

and the following two physical attacks:

- The physical attacker obtains unauthorized access to the Public Announcement area.
- Unauthorized PA message provided.

As a result, Scenario #2 entailed eight attacks.

Eventually, eighteen cyber and physical attacks were committed under the scope of the Athens Airport demonstration.

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

For the current KPI estimation, all Innovation Elements (IEs) that were illustrated during the two scenarios execution of the Athens Airport demonstration event are enlisted below:

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

IE4: Unified access control (UAC) system combined with video analytics.

IE5: Extended passenger identity with baggage tracking and data analysis for anomaly detection.

IE8: Cyber threat detection on critical networks and business processes.

IE9: Correlation engine for cyber-physical threat detection.

IE10: Data analytics for forensics investigation and fast recovery.

IE11: Impact propagation simulation for anticipated impact assessment.

IE12: Cyber-physical incident management portal for enhanced SOC awareness.

IE13: Crisis alerting system for coordinated security and safety responses.

IE14: Emulation platform for improved cyber defence strategies.

As a result, ten capabilities were demonstrated in the Athens Airport event.

The target was to perform nine capabilities. The IE2: Vulnerability management system for ICS and OT systems (GLPI) was initially planned to be illustrated in the Athens Airport demonstration. Eventually, it was not directly demonstrated; the results were considered for the cyber and physical threat analysis of IE1 (RIS) during the risk assessment performance. Nevertheless, two more SATIE IEs were shown within the Athens Airport demonstration utilized in both scenarios that were not considered as targets; IE4: Unified access control system combined with video analytics and the IE14: Emulation platform for improved cyber defence strategies.

SATIE KPI #Number of participants trained.

This KPI value addresses the number of SOC and AOC operators trained and participated in the Athens Airport demonstration event. In particular, two SOC operators and two (AOC) operators were involved both in scenario #1 and scenario #2 (who could be considered as a double individual effort) and thus the final value of KPI did not reach target six.

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

This KPI value was calculated according to the evaluation questionnaire responders, defined in section 4.2.

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

To assess the current value of this KPI, all external demo visitors (physical and online visitors) are considered. Unfortunately, due to COVID-19 security and safety indications and travel restrictions, invitees were unable to join the event physically. Thus, all external demo visitors were thirteen people who attended online.

Table 4.1: enlists the current values of KPIs with respect to the Athens Demonstration event

KPI	Objec-tive	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
Number of different attacks implemented in the demonstration of the final scenarios.	O8	N/A	18	Yes	This calculation includes only the subset of cyber and physical attacks demonstrated in Athens. The target (23) is not applicable, as it is counting all 4 scenarios	All attacks of the two scenarios carried out within the Athens Airport demonstration are counted.

KPI	Objec-tive	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
					demonstrated in the 3 locations (Athens Airport, Milan Airport, Zagreb Airport).	
Number of capabilities demonstrated (Demo AIA)	O8	9	10	Yes	The Athens Demonstration event overpassed successfully the targeted value of the specific KPI with the demonstration of 10 Innovation Elements (IEs). In particular, IE2 considered as target was not demonstrated. Nevertheless, IE4 and IE14 were demonstrated which were not counted in the initial target (see description in the beginning of the section)	Counting how many SATIE Innovation Elements (IEs) were demonstrated during the Athens Airport event.
Number of participants trained (Demo AIA)	O8	6	4	N/A	2 SOC operators and 2 AOC operators were trained for the Athens Airport demonstration. During the demonstration, the same 4 trained people (2 SOC operators and 2 AOC operators) were allocated for both scenarios' execution.	2 roles were trained: AOC and SOC. No observer was trained for the Athens Airport demonstration event.
Number of security practitioners /participants answering a questionnaire (Demo AIA)	O8	6	8	Yes	The Athens Airport demonstration succeeded in increasing the final value of security practitioners answering the evaluation questionnaire.	Security practitioners were counted as individuals and not per organisation.

KPI	Objec-tive	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
Number of project external demo visitors (Demo AIA) online/physical	O8	20 when online 15 when physical	22	Yes	Due to COVID-19 security and safety protocols and to the respective travel restrictions and limitations there were no physical external visitors in the Athens Airport demonstration event.	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 Athens demonstration is presented. A subset of the questions already asked during the simulation validations (described in D6.2 (6) 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). 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. We define the term of “independent external” participant 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. However, the total number of considered questionnaire responses was only *N* = 8. The evaluation of operators was already performed during the simulation validations and is described in D6.3 (2).

Table 4.2 presents an overview over the results of the answers of the participants and Table 4.3 visualizes these results with bar graphs.

Table 4.2: Results of evaluation questionnaire responders

Statement	Average	Median	Minimum	Maximum	Standard Deviation	No. of participants
The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	6.38	7.00	4.00	7.00	1.06	8
The SATIE Solution is an excellent way to monitor and raise security alerts.	6.63	7.00	6.00	7.00	0.52	8
The SATIE Solution provides all relevant information.	6.25	6.00	6.00	7.00	0.46	8

Statement	Average	Median	Minimum	Maximum	Standard Deviation	No. of participants
The SATIE Solution enables a faster detection of cyber threats compared to current systems.	6.00	6.00	4.00	7.00	1.07	8
The SATIE Solution enables a faster detection of physical threats compared to current systems.	5.63	6.00	4.00	7.00	0.92	8
The SATIE Solution enables a faster response to cyber threats compared to current systems.	6.25	6.50	4.00	7.00	1.04	8
The SATIE Solution enables a faster response to physical threats compared to current systems.	5.75	6.00	4.00	7.00	0.89	8
The use of the SATIE Solution increases the efficiency compared to current systems.	5.88	6.00	4.00	7.00	0.99	8
I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	4.75	5.00	3.00	6.00	1.39	8
The SATIE Solution is innovative compared to others on the market.	6.14	7.00	4.00	7.00	1.21	7
I think the SATIE Solution will boost airports' revenues.	5.00	5.00	3.00	7.00	1.41	7
I think airports will like to secure their systems with the SATIE Solution.	6.14	6.00	6.00	7.00	0.38	7
I think that the shown scenario(s) were suitable to illustrate the SATIE Solution's capabilities.	6.14	6.00	5.00	7.00	0.69	7

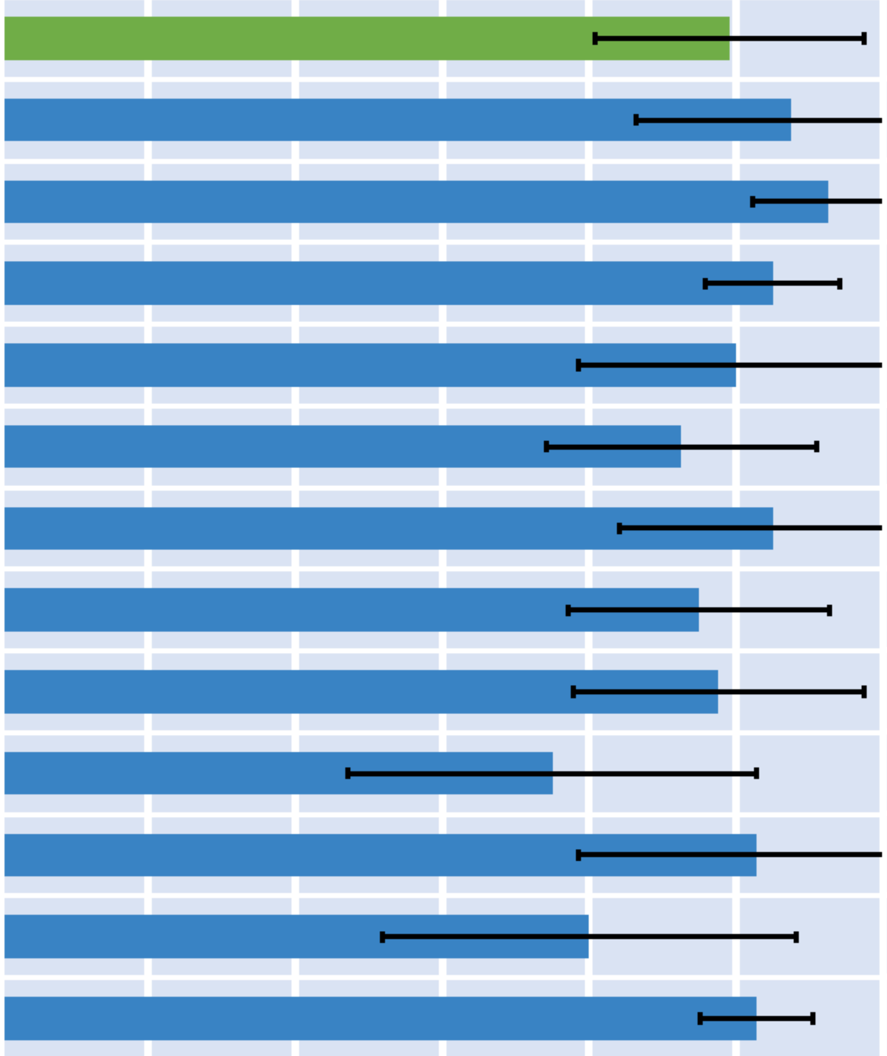
Statement	Average	Median	Minimum	Maximum	Standard Deviation	No. of participants
The SATIE Solution has good usability.	6.43	7.00	5.00	7.00	0.79	7
Summary	5.96	6.18	3.00	7.00	0.92	

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 statements that the SATIE solution will boost revenues for airports and the ease of integrating the SATIE Solution with necessary airport systems. The shown scenarios at Athens 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 questions asked during the demonstration event were an adapted subset of the ones presented to the simulation validation participants. This offered the opportunity to compare the results of the demonstration and simulation validation activities. Even though the participants were different regarding their operational background and experience (see Table 4.5), the responses received were similar. 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 systems, 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 both 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	1 Completely disagree	2	3	4 Neutral	5	6	7 Completely agree	No. of replies
Statements	Overall								
AIA_S01	The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.								8
AIA_S02	The SATIE Solution is an excellent way to monitor and raise security alerts.								8
AIA_S03	The SATIE Solution provides all relevant information.								8
AIA_S04	The SATIE Solution enables a faster detection of cyber threats compared to current systems.								8
AIA_S05	The SATIE Solution enables a faster detection of physical threats compared to current systems.								8
AIA_S06	The SATIE Solution enables a faster response to cyber threats compared to current systems.								8
AIA_S07	The SATIE Solution enables a faster response to physical threats compared to current systems.								8
AIA_S08	The use of the SATIE Solution increases the efficiency compared to current systems.								8
AIA_S09	I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.								8
AIA_S10	The SATIE Solution is innovative compared to others on the market.								7
AIA_S11	I think the SATIE Solution will boost airports' revenues.								7
AIA_S12	I think airports will like to secure their systems with the SATIE Solution.								7



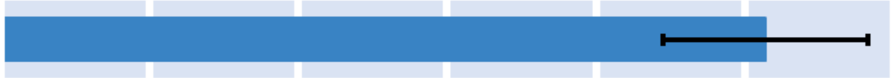
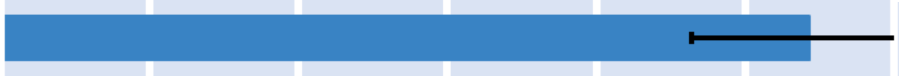
AIA_S13	I think that the shown scenario(s) were suitable to illustrate the SATIE Solution's capabilities.		7
AIA_S14	The SATIE Solution has good usability.		7

Table 4.4: Innovation Elements Feedback

Question	"Which of the Innovation Elements (IE) stood out for you, and why?"	
Innovation Element	**Frequency**	**Reasons**
Crisis Alerting System (CAS)	3	
Risk Integrated Service (RIS)	2	Analytical, Very useful
Unified Access Control (UAC)	2	Targeted, Standardisation needed
Passenger Anomaly Detection (PAD)	2	Targeted, Standardisation needed
Incident Management Portal (IMP)	2	
Vulnerability Intelligence Platform (VIP)	1	Good step into right direction
Malware Analyser (MA)	1	Securing threats, Very useful
Application Layer Cyber Attack Detection (ALCAD)	1	
Correlation Engine	1	Really important, Need for constant validation
SMS-I	1	Useful
CyberRange	1	

Table 4.5: Affiliation of participants

Question	“Please choose the type of organization you work in.”
Types of organisation	**Number of participants**
Research/Academic	3
Law Enforcement	1
Airport	1
Business Development Consultant	1
Cybersecurity Consultant	1
Large Enterprise	1
Total	**8**

5 Conclusion

After the presentation of the test and verification plan and the validation plan in deliverable D6.2 (6) and the report on the test and validation results on the simulation platform in D6.3 (2) as part of T6.2, the current deliverable presents the Athens Airport demonstration and the results gained in the last phase of the SATIE project. The deliverable presents the outcome of T6.4, the cyber-physical threat scenarios execution towards testing the SATIE tools at the Athens Airport environment under real conditions, which is a fundamental step to communicate the project's feasibility and figure out the value of the SATIE solution to the aviation and airport critical infrastructure security.

The current report presents the main objective of the Athens' Airport demonstration, the overview of the event, including localization and logistics information, the cyber and physical infrastructure deployed, the integration with the SATIE Solution, a detailed step-by-step description of the two dedicated scenarios, containing an extended analysis of the embedded cyber and physical attacks, the corresponding technical operations and the SATIE involved Tools response.

The SATIE Solution was demonstrated under different airport critical infrastructures, such as the Flight Information Display System (FIDS), the Access Control (AC) system, the Public Announcement (PA) system, the Automated Border Control (ABC) system to detect and report malicious activity (i.e. anomalies and abnormal use of the systems, suspicious movement, high risk files identification, unauthorized access to airport areas and airport systems) and create alerts and incidents (see Correlation Engine (CE) description in section 3.1) to classify and communicate the results to the end users, namely to the SOC and AOC operators (see Incident Management Portal description in section 3.3). Moreover, the SATIE Solution received events from the threat detection system (see section 3.2) and also directly from the connected airport OS and from the airport network as described in sections 2.2.2 and 3.1. Events and alerts were further analysed through the Investigation Tool (SMS-I) (see section 0). The Anomaly Detection on Passengers Records (ADPR) of SATIE succeeded in detecting the potential threat of a passenger in real-time response, as presented in section 3.4. The Unified Access Control (UAC) Tool of SATIE achieved in detecting unauthorised entrance in airport security areas through face recognition procedures (see section 3.5). The Impact Propagation Simulation (IPS) produced reports and simulation results regarding the impacted assets and their interrelations with the undisturbed assets within the network topology (see section 3.6). Risk results were sent to the end-users produced from the Risk Integrated Service (RIS) Tool. The Crisis Alerting System (CAS) (see section 3.7) successfully communicated immediately the information to internal and external parties, proving that it can be used to facilitate the collaboration within the AOC internally and externally with Law Enforcement Agencies (LEAs) in view of an emergency.

The SATIE Solution performance during the demonstration scenarios execution was evaluated by external web attendees through an online evaluation questionnaire and valuable feedback was received from stakeholders and security practitioners with different background and experience. In particular, according to the evaluation results from the responders the SATIE Solution proved in general that:

- It can contribute significantly to improve the current security-monitoring systems.
- It is an innovative and trustworthy solution to monitor and raise security alerts.
- It enables fast detection and response towards cyber and physical threats.
- It accelerates the efficiency compared to other relevant existing systems.
- It is a cost-benefit solution to be utilized by airports.

The Athens demonstrated scenarios were evaluated as suitable to promote the SATIE Solution´s capabilities.

The evaluation participants pointed out that a window of improvement could be kept open regarding the SATIE Tools integration with existing airport systems.

Comparing the results delivered from the evaluation participants of the demonstration event derived from the current deliverable and the evaluation participants of the simulation event described in D6.3 (2), there are some similarities of the answers given and a positive feedback was provided in the overall coming from groups of different expertise which reinforces the SATIE Solution benefits.

Eventually, the final values of KPIs related to the Athens Airport demonstration were assessed and the initial target was either reached or overcome. In some particular cases where it was not applicable to be reached, relevant justification is provided.

6 References

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

2. **SATIE project.** *D6.3 Test and validation results on the simulation platform.* 2021.

3. —. *D5.1 Anticipated impact assessment.* 2021.

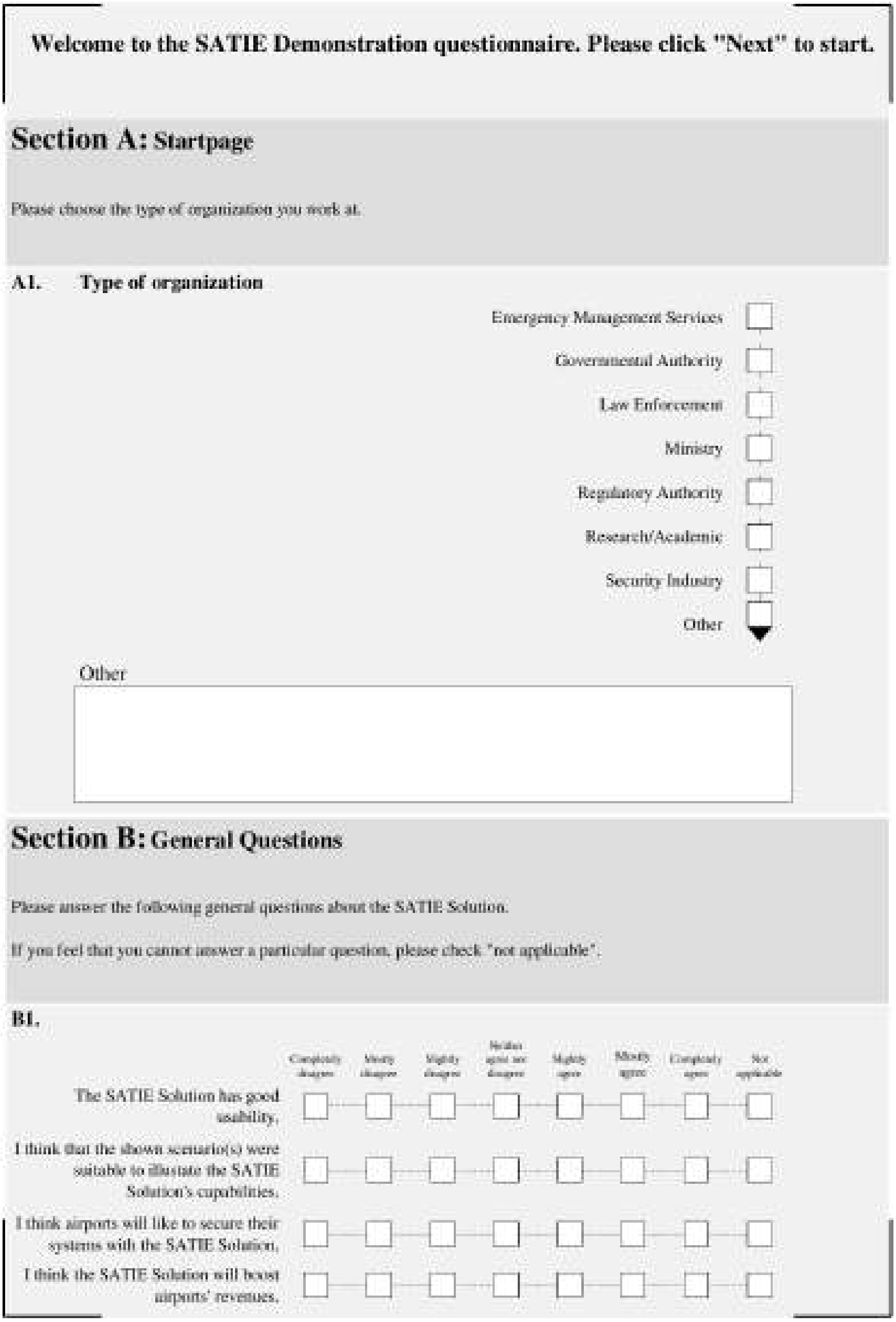
4. **Köpke, C., et al.** Impact Propagation in Airport Systems. *CPS4CIP 2020, LNCS 12618, 1-16.* 2021.

5. **SATIE project.** *D2.3 Cyber-physical risk analysis.* 2020.

6. —. *D6.2 Test, validation and demonstration scenarios.* 2020.

Annexes

Annex 1 - 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

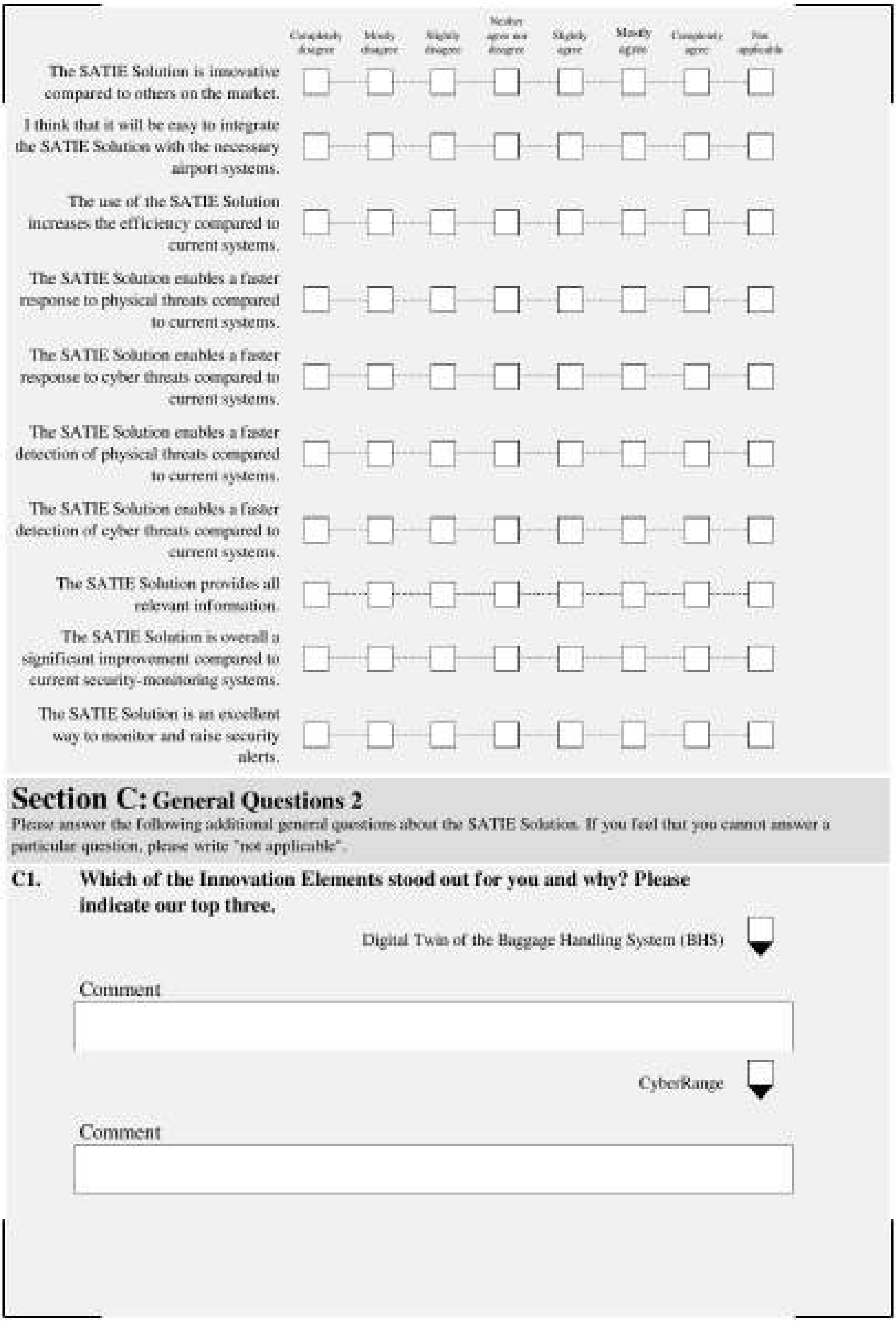
Section B: General Questions

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".

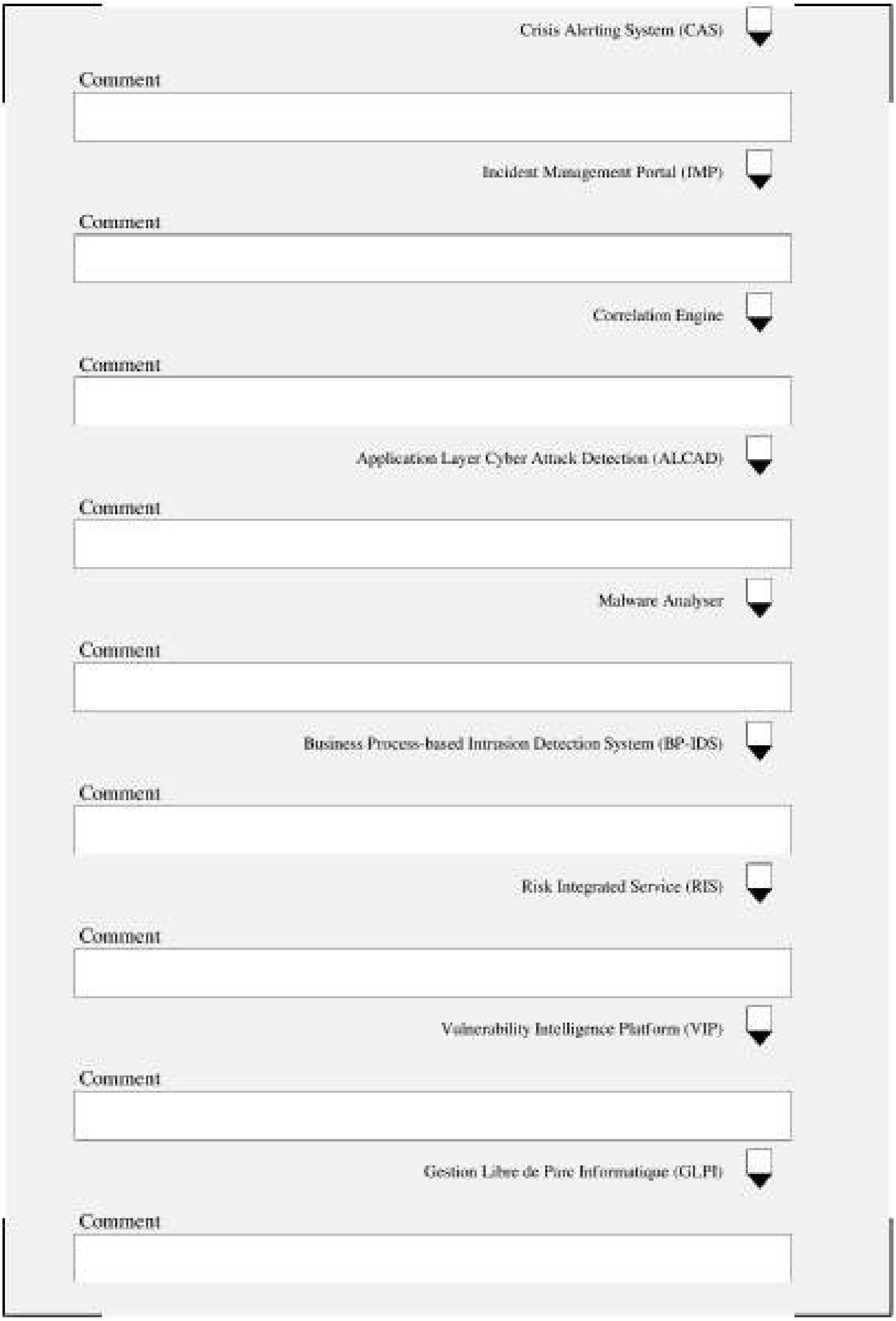
C1. Which of the Innovation Elements stood out for you and why? Please indicate our top three.

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)

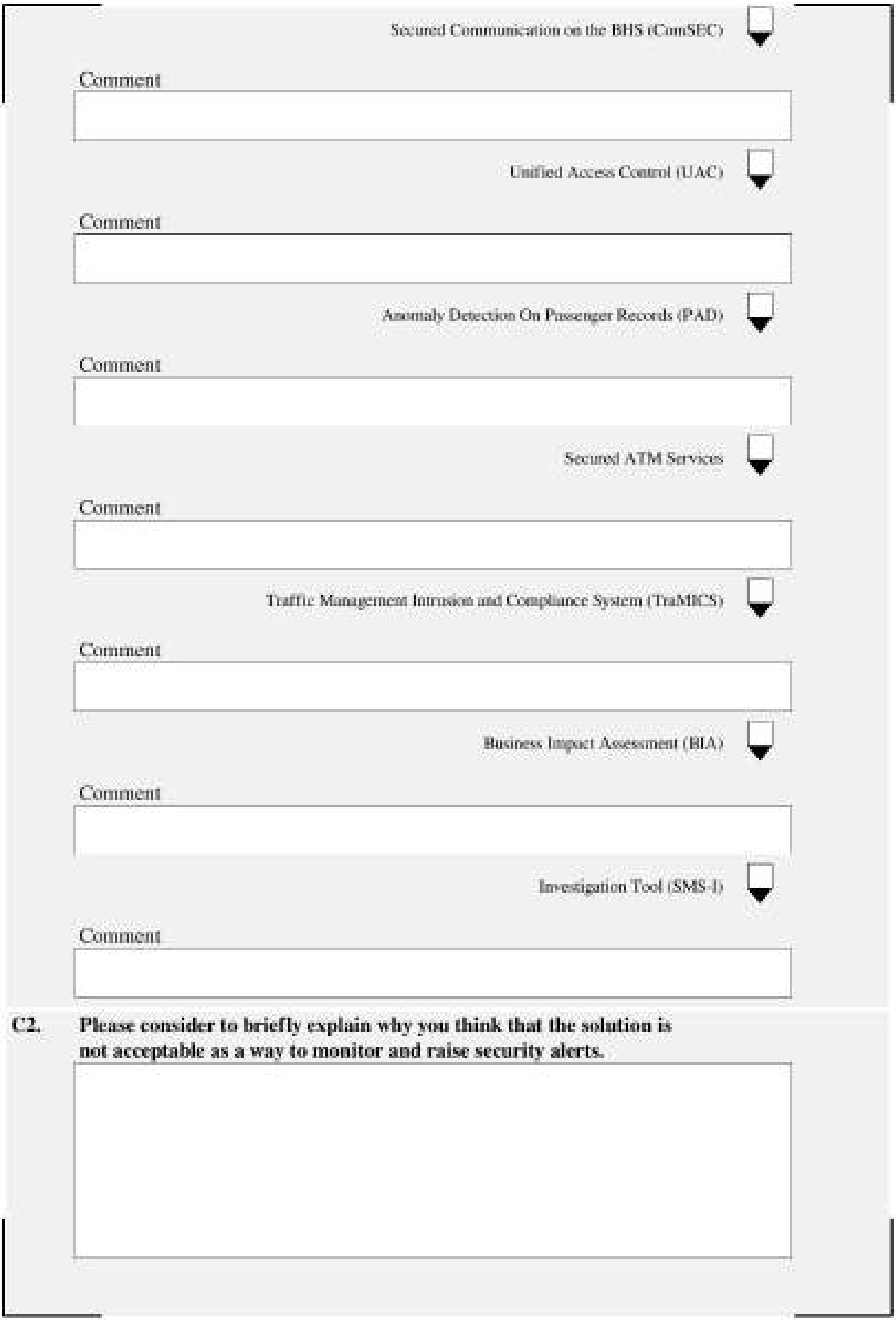
Comment

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

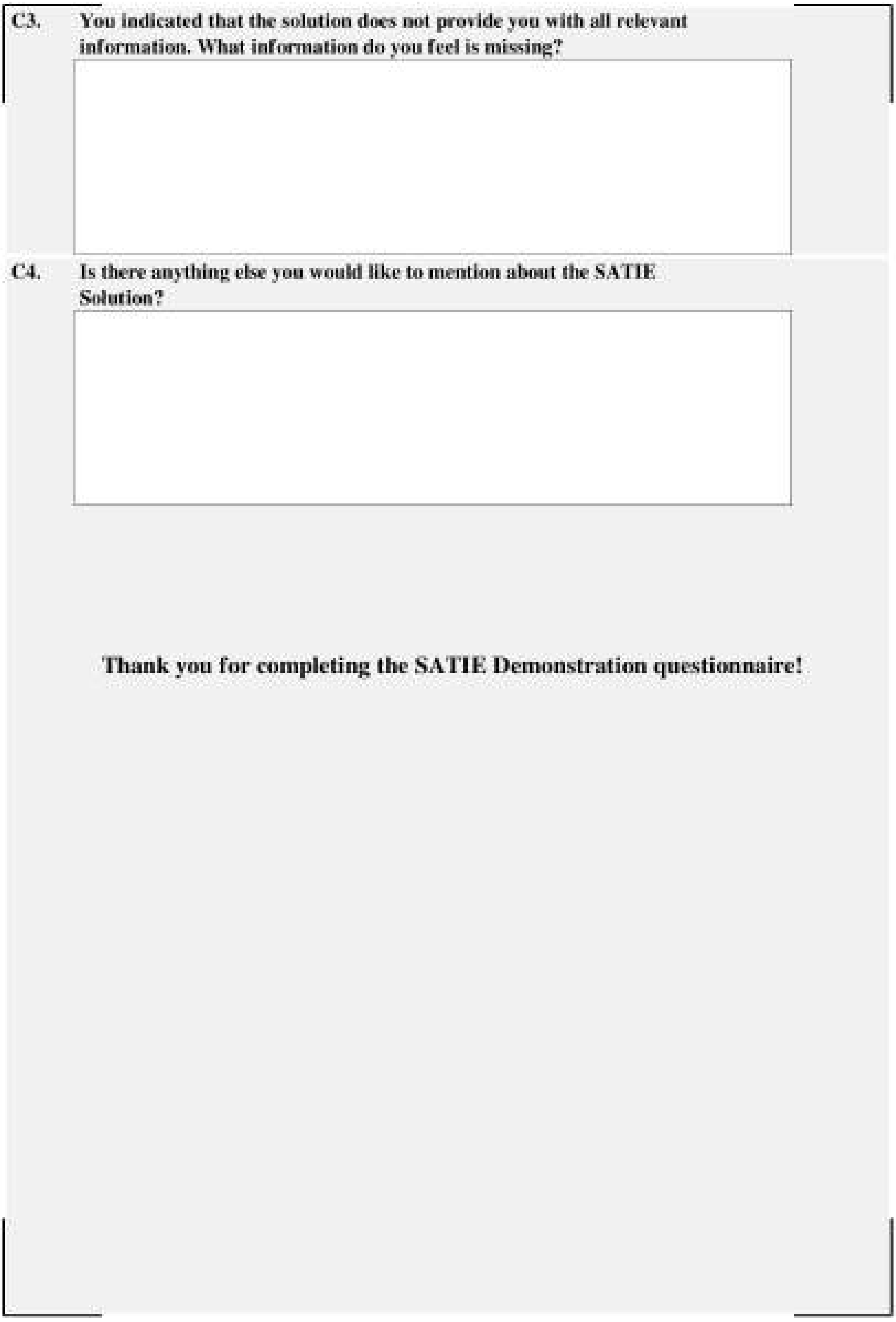
Business Impact Assessment (BIA) ▼

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!