SATIE

Security of Air Transport Infrastructures of Europe

D6.4 – Report about demonstration and results in Zagreb Airport

Deliverable Number	D6.4
Author(s)	ZAG, ALS, ACS, IDEMIA, INOV, TLB, DGS, DLR
Due/delivered Date	M29/2021-10-15
Reviewed by	DLR, KEM
Dissemination Level	PU
Version of template	0.1

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	Sven Hrastnik (ZAG)	Content contributor
2	Thomas Oudin (ACS)	Content contributor
3	Meilin Schaper (DLR)	Reviewer
4	Samoogabalan Kantharuban (IDEMIA)	Content contributor
5	François Déchelle (TLB)	Content contributor
6	Andrei-Vlad Predescu (DLR)	Content contributor
7	Eric HERVE (ALS)	Content contributor
8	Nils Carstengerdes (DLR)	Content contributor
9	Vasileios Kazoukas (KEMEA)	Reviewer
10	Kelly Burke (DGS)	Content contributor
11	Filipe Apolinário (INOV)	Content contributor

Document revisions

Revision	Date	Comment	Author
V0.1	2021-08-08	Initial draft	Sven Hrastnik
V0.2	2021-08-11	Content add to section 3.1 and 3.2	Thomas Oudin
V0.3	2021-08-30	Added contribution to chapter 3	Kelly Burke, Filipe Apolinário, François Déchelle
V0.4	2021-09-01	Added contribution to chapter 4	Nils Carstengerdes, Andrei-Vlad Predescu
V0.5	2021-09-06	Initial quality check and format adjustments	Meilin Schaper
V0.6	2021-09-17	Content added to chapters 1, 2 and 3	Sven Hrastnik
V0.7	2021-09-21	Content added to chapters 2 and 3	Kantharuban Samoogabalan
V0.8	2021-09-28	Content added to sections 2 and 3	Eric Herve
V0.9	2021-10-08	Review the sections 2 to add more steps in scenario	Eric Herve
V0.9	2021-10-15	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V1.0	2021-10-15	Final quality check and approval for submission	Meilin Schaper, Quality Manager

Executive summary

The main objective of this deliverable is the report on the performance of Zagreb Airport demonstration which included four different scenarios aiming disruption of Baggage Handling System (BHS) and passenger and baggage handling processes. These scenarios incorporate a considerable number of potential cyber-attacks that may become physical and could cause a devastating impact to airports operations and people's safety, defined in T6.2.

Furthermore, the current deliverable is the outcome of T6.3 which refers to demonstration in operational conditions in order to show that SATIE Toolkit recognizes threats in avoiding any trouble on the BHS. All four scenarios were performed at night after the last flight departed from Zagreb airport and they consisted of previously recorded videos, live presentations and attack simulations.

SATIE Tools were demonstrated and evaluated through the execution of the four threat scenarios, followed by related Q&A, interviews and questionnaires from external attendees and end-users in order to refine the risk analysis.

List of Content

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
ACS	Airbus Cyber Security
ADPR	Anomaly Detection on Passenger Records
ALCAD	Application Layer Cyber Attack Detection
AOC	Airport Operations Centre
API	Application Programming Interface
BHS	Baggage Handling System
BIA	Business Impact Assessment
BP-IDS	Business Process-based Intrusion Detection System
CAS	Crisis Alerting System
CCTV	Closed-Circuit Television
CVE	Common Vulnerabilities and Exposures
DDOS	Distributed Denial of Service
EU	European Union
GLPI	Gestion Libre de Parc Informatique
GUI	Graphical User Interface
HMI	Human Machine Interface
IE	Innovation Element
IMP	Incident Management Portal
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
LAD	Luggage Anomaly Detection
MITM	Man-In-The-Middle
PAD	Passenger Anomaly Detection
PLC	Programmable Logic Controller
BHS	Baggage Handling System
Q&A	Questions and Answers

Acronym	Definition
RIS	Risk Integrated Service
SAC	Sort Allocation Computer
SATIE	Security of Air Transport Infrastructures of Europe
SCADA	Supervisory Control And Data Acquisition
SOC	Security Operations Centre
TS	Timestamp
USB	Universal Serial Bus
VIP	Vulnerability Intelligence Platform
VuMS	Vulnerability Management System
ZAG	Zagreb Airport

1 Introduction

The SATIE project, as a part of the European Union’s Horizon 2020 research and innovation programme, aims to revolutionise the approach for securing the airport and prevent disruptions of critical systems that could have an impact on the service provided. The idea of the project is to protect against complex cyber-physical threat scenarios while keeping business continuity and ensuring passengers’ safety.

SATIE adopts a holistic approach about threat prevention, detection, response and mitigation in airports, while guaranteeing the protection of critical systems, sensitive data and passengers. The developed interoperable toolkit improves the relationship between existing systems and enhanced security solutions in order to ensure more efficient threat prevention, forensics investigations and dynamic impact assessment at the airports. Having a shared situational awareness, security agents, operational staff and airport managers collaborate more efficiently to the crisis resolution.

Safety is a key pillar of the airport operations and it represents the highest priority for all employees from all companies and stakeholders working at the airport, regardless of their duties or level in each organization. Goal is to be safe, smoothly-functioning airport which is thoroughly compliant with the international standards, national and EU legislation. This project is an example of ensuring the highest possible level of safety maintained throughout the airport.

Cyber-security is significant part of overall security factors that have an impact on safety at the airports. It is important to take cyber-security seriously because it may take some time to detect malicious attacks and security breaches could come with very high costs. Therefore, airports have established, implemented, maintain and continually improve Information Security Management Systems complied with the statutory and regulatory requirements and international standards. Information Security Policy is defined for the scope which includes critical airport systems, such as Baggage Handling System (BHS) among others.

Figure 1.1: Passenger terminal building at Zagreb Airport

The demonstration at Zagreb Airport (Figure 1.1) aimed to recognize and prevent cyber-physical attacks on the BHS (Figure 1.2), especially because of the use of system for Supervisory Control And Data Acquisition (SCADA). This system allows the centralisation of BHS control, visualisation and display of relevant data. Because of interconnectivity of SCADA with other airport information systems, it becomes exposed to vulnerabilities as computers do. Malware could be uploaded with the collaboration of compromised employee, and an attack on SCADA would represent an attack on physical airport infrastructure. The attacker may send malicious commands or disrupt normal baggage handling operations, or even combine it with loading of prohibited objects into the aircraft. It is easy to imagine what kind of catastrophe can occur if the BHS system finds itself under cyber-attack and does not immediately recognize that kind of threat, and this is where SATIE Solution appears.

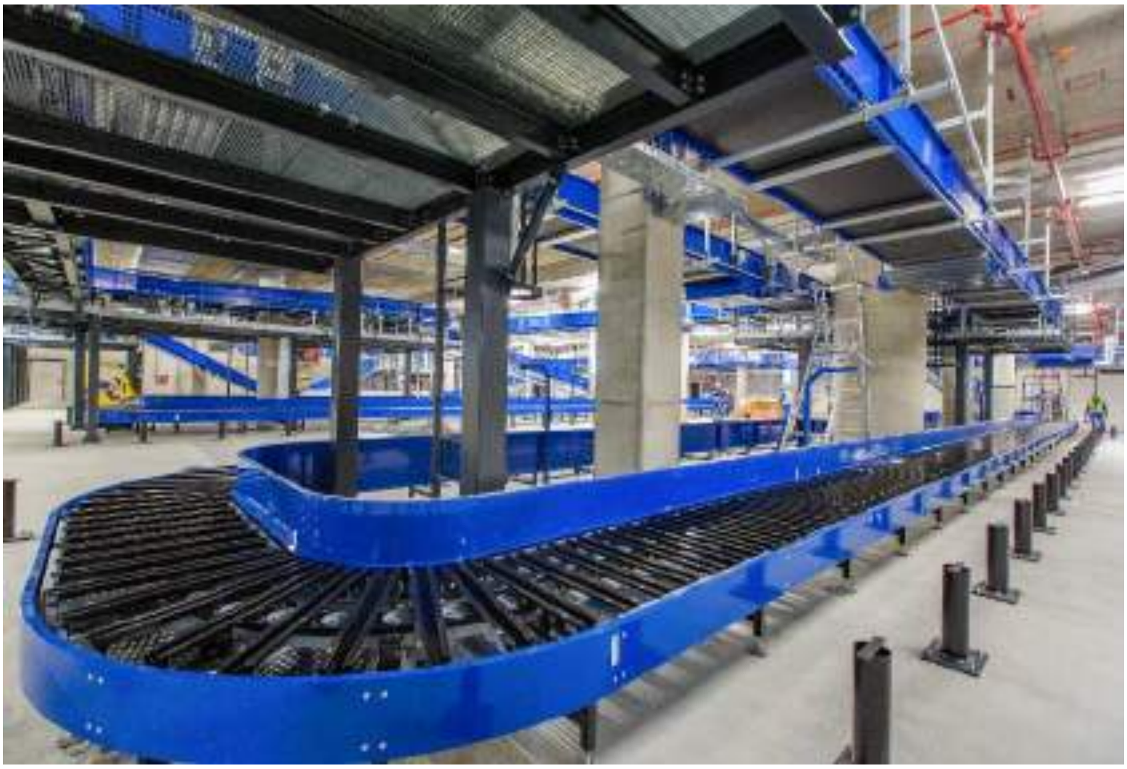


Figure 1.2: Baggage Handling System in construction at Zagreb Airport (around year 2016)

2 International Zagreb Airport demonstration

One of the most critical aspects of the SATIE project is to demonstrate its usefulness and practicality in different airport environments. Zagreb Airport demonstration event was set up to indicate this task and collect feedback from the users and security practitioners involved in relevant business procedures. Several scenarios of threats and cyber-attacks related to the baggage handling system and the process of passenger baggage handling were presented.

Demonstration in Zagreb was organized and coordinated by International Zagreb Airport (ZAG) and ALSTEF (ALS) with the active involvement and technical support of all the partners.

Due to the COVID-19 pandemic and travel limitations, demonstration was carried out as a hybrid event (both cyber and physical). It consisted of a combination of pre-recorded video materials, real-time presentations and live scenario demonstrations which are explained further in the following chapters of this report.

In this context several training seminars and trial workshops were organized with Airport Operations Center (AOC) and Security Operations Center (SOC) operators in order to be trained on the proposed solution. In addition, the demonstration was preceded by several meetings with airport service users and partners to familiarize them with the proposed SATIE Solution. Due to the complexity of the demonstration and coordination of all activities, schedule shown in Figure 2.1 has been developed. Goal of the scheduling was to be prepared for the testing with dates clearly defined one month before the upcoming demonstration. Targeting towards this direction, the following paragraphs describe all important issues that came out from the demonstration performed in Zagreb. These include the identification of potential problems that need to be early solved in order to conclude with a successful implementation of the solution and the achievement of the expected results.

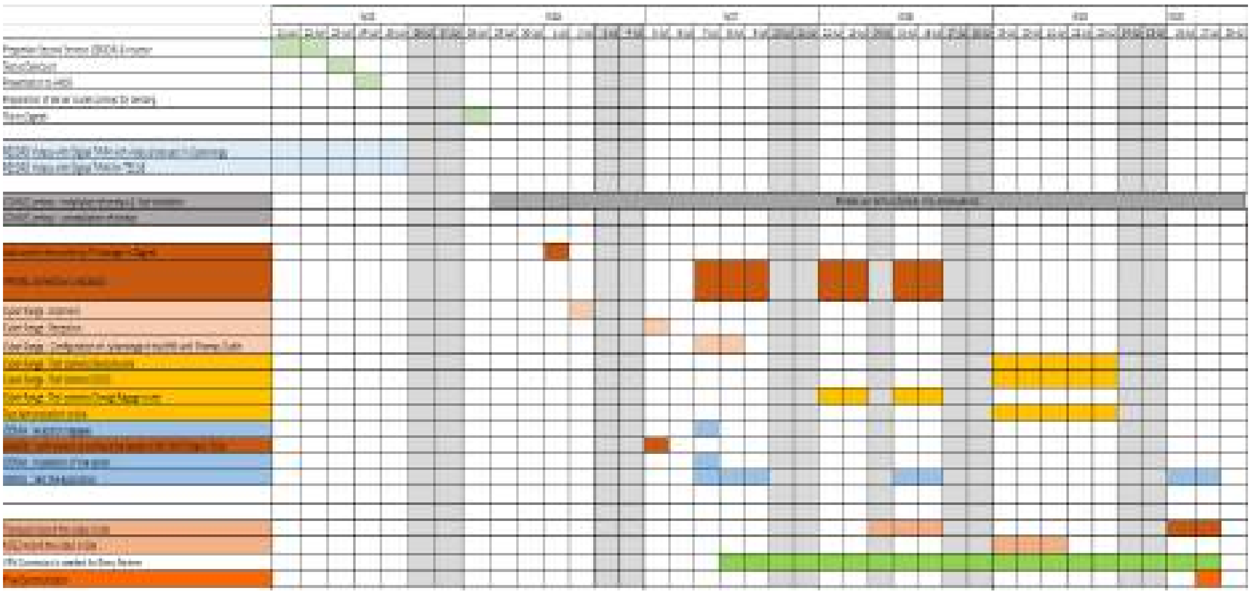


Figure 2.1: Schedule with defined activities for the demonstration

2.1 Demonstration overview

After months of training on the simulation platform, second SATIE online demonstration event took place at Zagreb Airport on the 27th of July, 2021. As well as in the previous Athens case, this too was both virtual and physical event. More than 40 participants were connected through online platform and took part in a demonstration broadcast via video cameras.

The performed scenario was the only one within the SATIE project to involve the Baggage Handling System (BHS) and the baggage registration service. Because of that unique aspect and, thanks to ALSTEF, creation of almost a complete copy of the real BHS connected directly to the SATIE Toolkit, demonstration has been elaborated into four different sub-scenarios with more threats to take advantage of this setup. It was initially conceived that the demonstration consists of three sub-scenarios, but there was an opportunity to include and show the additional one as explained in the next section. Another difference between this and the remaining two events is that Zagreb demonstration took place during the night and after all flights departed due to use of simulated BHS environment.

Demonstration at Zagreb was aimed to revolutionise the approach for securing the airport and prevent disruptions of critical systems such as BHS that could have an impact on the service provided by airports. SATIE Toolkit has shown its purpose against complex cyber-physical threats through prevention, detection, response and mitigation, while guaranteeing the protection of critical systems, sensitive data and passengers.

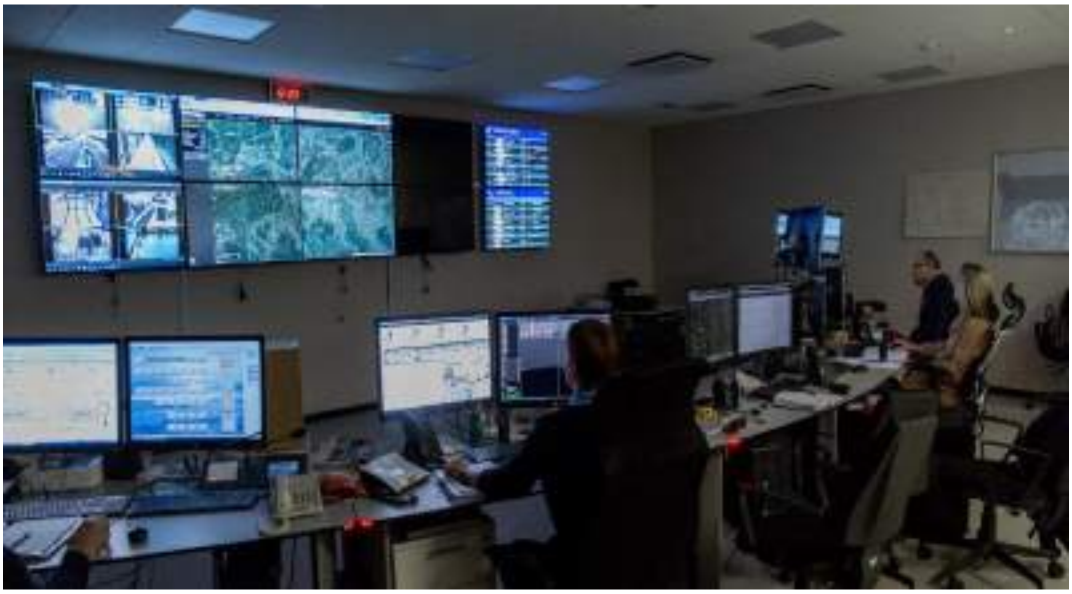
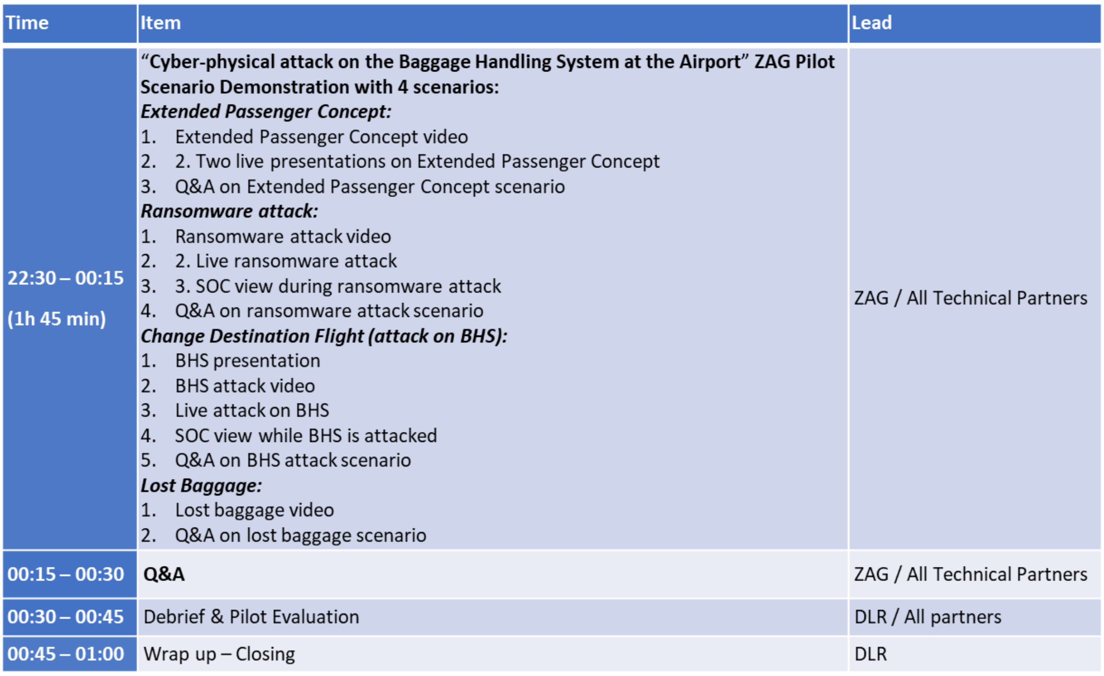


Figure 2.2: Airport Operations Centre (AOC)

Central location intended for use of SATIE Toolkit is Airport Operations Centre (Figure 2.2). AOC is the central link between the landside management (access to the terminal) and the airside management dealing with operational activities in restricted areas. The concept is to master any kind of situation happening in the airport ensuring a safe and secure operation, optimizing critical resources and enhancing the quality of service provided to passengers, users and stakeholders.

AOC integrates the essential functions of the airport – operations, security and maintenance. ZAG airport staff is working 24 hours a day while coordinating various activities throughout the airport, of which the most important are: resources allocation and operations management, maintenance and technical monitoring, safety and security, firefighting services and alerting.

The demonstration agenda (Figure 2.3) was modified several times and depended on the last aircraft departure, which often changes due to accumulated delays of certain flights at the end of the day. Those conditions are accepted as usual in dynamic environment such as airports and all participants adapted to it. That was also the reason why the fourth and last added scenario was shown first, since it was not entirely BHS related.



Time	Item	Lead
22:30 – 00:15 (1h 45 min)	**“Cyber-physical attack on the Baggage Handling System at the Airport” ZAG Pilot Scenario Demonstration with 4 scenarios:** ***Extended Passenger Concept:*** 1. Extended Passenger Concept video 2. 2. Two live presentations on Extended Passenger Concept 3. Q&A on Extended Passenger Concept scenario ***Ransomware attack:*** 1. Ransomware attack video 2. 2. Live ransomware attack 3. 3. SOC view during ransomware attack 4. Q&A on ransomware attack scenario ***Change Destination Flight (attack on BHS):*** 1. BHS presentation 2. BHS attack video 3. Live attack on BHS 4. SOC view while BHS is attacked 5. Q&A on BHS attack scenario ***Lost Baggage:*** 1. Lost baggage video 2. Q&A on lost baggage scenario	ZAG / All Technical Partners
00:15 – 00:30	**Q&A**	ZAG / All Technical Partners
00:30 – 00:45	Debrief & Pilot Evaluation	DLR / All partners
00:45 – 01:00	Wrap up – Closing	DLR

Figure 2.3: Agenda of the SATIE demonstration at Zagreb Airport

2.2 Demonstration scenarios

The four threat sub-scenarios are described below. They were built based on historical information and needs expressed by airport as end-users in this project. The goal is to represent cyber-physical threats that can develop into attacks which are increasingly complex and difficult to predict.

As the SATIE project progressed, so did the scenarios. It was originally conceived that social engineering would be conducted on a member of the BHS team, but it seemed more realistic that the attacker appears in the form of a corrupted employee. Compromised personnel represent major vulnerability because these people have more access and rights than a member of the public and their presence in high-security areas would raise a lot less suspicion.

All threat scenarios used in the SATIE project were already defined and finalized in the deliverable D6.2 (1). However, as progress has been made to prepare for and implement the scenarios, some changes have been made. Looking only at the Zagreb demonstration, three sub-scenarios were originally defined: “The Ransom”, “The Lost Baggage” and “The Bomb”. For the security reasons it was decided that sub-scenario “The Bomb” cannot be demonstrated and shown in public, although the SATIE Toolkit proved its effectiveness in recognizing such an attack. Therefore, an additional sub-scenario called “The Wrong Hold” was created instead, and its preparation can be seen on the Figure 2.4.

In addition to that, a fourth sub-scenario named “The Extended Passenger Concept” was developed and shown first because it was not related to the real time aircraft departures. All sub-scenarios were presented with the help and involvement of all SATIE partners:

- Sub-scenario 1 “The Extended Passenger Concept” (coordinated by IDEMIA)
- Sub-scenario 2 “The Ransom” (coordinated by ALS and ZAG)
- Sub-scenario 3 “The Wrong Hold” (coordinated by ALS and ZAG)

- Sub-scenario 4 “The Lost Baggage” (coordinated by ALS and ZAG, presented only through video)

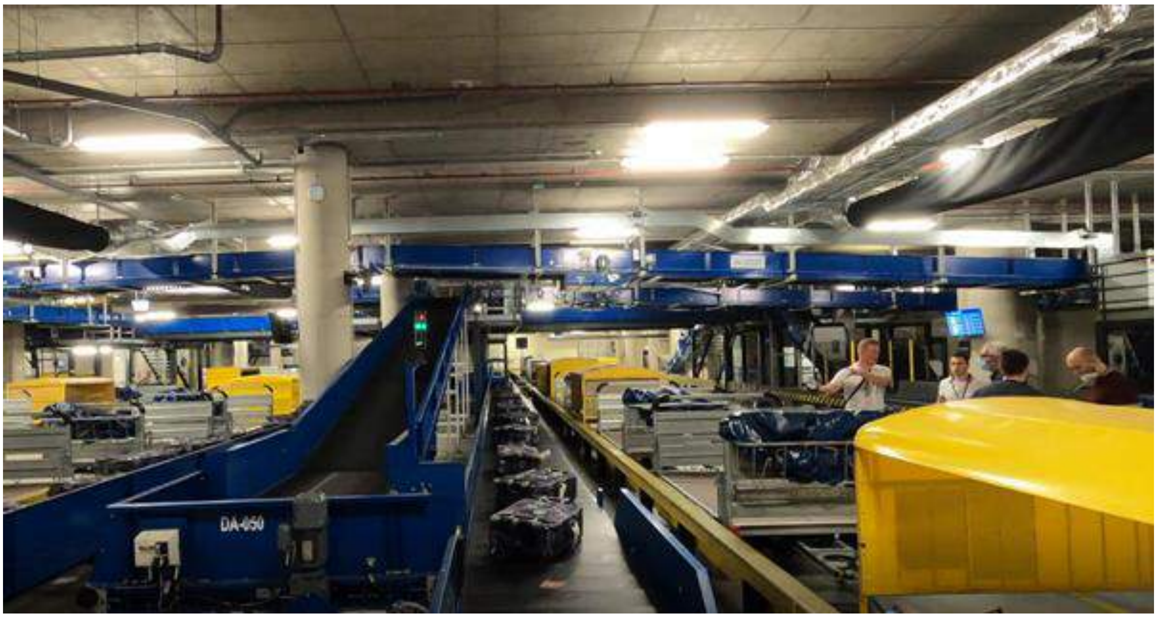


Figure 2.4: Preparation and testing before the start of the demonstration

Demonstration of all four sub-scenarios included previously recorded videos, live presentations and attack simulations, response of the SATIE Toolkit and related Q&A afterwards. SATIE Tools involved at the Zagreb demonstration scenarios are shown on the Figure 2.5 and highlighted in yellow.

Looking at the Figure 2.4 and as mentioned earlier, SATIE demonstration at Zagreb Airport was oriented on BHS and baggage handling processes. Simulated attacks were recognized by SATIE Tools developed especially for threat prevention and detection such as ComSEC, BP-IDS and Passenger/Baggage anomaly detection systems, and all of that took place in the background of the SATIE Solution. At the same time, supporting systems simultaneously activated were Business Impact Assessment (BIA), Risk Integrated Service (RIS), Vulnerability Management System (VuMS) and Correlation Engine. They all provided useful inputs in knowing the severity of the threat and its consequences monitored by the SOC operator, who saw the alerts displayed in Incident Management Portal (IMP). The Crisis Alerting System (CAS) was not used in this demo although trained AOC operators were at disposal as well. Looking at a SATIE as a whole solution, all tools could find their purpose and usage in recognizing threats and preventing cyber-physical attacks, so that none of them went unnoticed by the SOC operator working on the SATIE’s IMP.

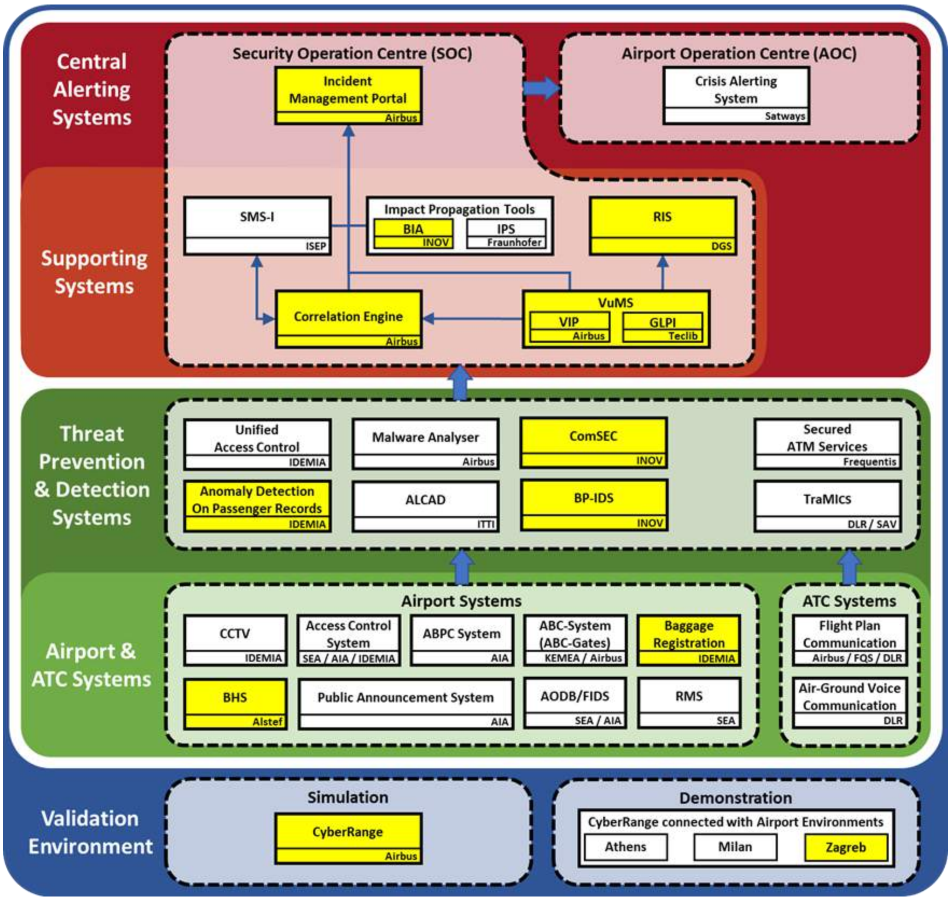


Figure 2.5: SATIE Tools relevant for the demonstration

2.2.1 Sub-scenario #1 “The Extended Passenger Concept”

This sub-scenario (Table 2.1) presents the Extended Passenger Concept using the Passenger Anomaly Detection (PAD) and Luggage Anomaly Detection (LAD) combined together as Anomaly Detection On Passenger Records (ADPR) tool to illustrate the security enhancement around the passenger and its luggage through some uses cases.

Table 2.1: Sub-Scenario #1 “The Extended Passenger Concept”

Scenario Step	Description	Involved Tools	Demonstration Set-Up
1	Control the passenger	Passenger Anomaly Detection (PAD)	At the check-in desk, an agent uses the passport reader to scan the passport and display the passport information on PAD screen. He controls the photo of the person within the chip of the passport, the photo on the document and the person in front the check-in desk. He submits a search to the risk assessment module of

			the PAD and visualizes the boarding directive associated to the person (“OK to Board” or “Further Control Needed”) **<u>Note:</u>** For SATIE illustration purpose the risk assessment module has been limited to check only against a list of wanted persons. This module could indeed be interfaced with other watch lists to verify for example also the authenticity of the travel document (stolen or not)
2	Notify the operators	Correlation Engine	Each time the agent uses the PAD, a notification is sent to the Correlation Engine with the result of the PAD search (“OK to Board” or “Further Control Needed”) to inform the operator on check-in control process and being able to take the appropriate(s) action(s) in case of “Further Control Needed” result.
3	Edit the boarding pass and Luggage tag	No SATIE Tools	As the identity of the passenger is controlled and the boarding directive displayed by the PAD is “OK to Board”, the agent at the check-in desk continues the passenger check-in process by editing the boarding pass and the luggage tags. **<u>Note:</u>** Without SATIE, the agent will control only the photo on the passport page with the person in front of him and assumes also the document is valid.
4	Enroll the Luggage	Luggage Anomaly Detection (LAD)	Once the luggage tag is placed on the luggage, the agent uses the tablet of the LAD to enroll the

			luggage by entering the luggage tag and taking four pictures under different angle of the luggage. **Note:** For SATIE, due to logistic constraints in Zagreb Airport, the enrollment process is illustrated manually using the tablet of the LAD to understand the concept but usually this process is done automatically in the BHS.
5	Enroll hand Luggage	Luggage Anomaly Detection (LAD)	The check-in agent generates also a tag for the hand luggage and enrolls it, too.
6	Create Extented Passenger Record	Luggage Anomaly Detection (LAD)	The extended passenger record is then created by associating the passenger luggage tag and the photos of his luggage. **Note:** The passenger personal information is not collected by the LAD. They remain within the current check-in system of the airport which contains also the tag id of the luggage. During the luggage identification or authentication process, when the passenger information is needed, the LAD will submit a request to the check-in airport system using the tag id of the luggage to retrieve and display them on the tablet.
7	Deliver Travel documents	No SATIE tools	The agent finalizes the check-in process by sticking the luggage tags on the boarding pass and delivers it to the passenger with his passport
8	Control the hand luggage	Luggage Anomaly Detection (LAD)	At the boarding gate the agent in addition of

			checking the passport, boarding pass, uses the tablet of the LAD to scan the hand luggage tag ID to check if the hand luggage belongs or not to the tag and by consequence if the hand luggage belongs to the passenger or not before let him enter into the plane. **Note:** Without SATIE, once one has passed the hand luggage scan area, until the boarding gates, no more control are done. Anything could occur between the duty free, the restaurants and boarding gates. For example, the luggage can be stolen, exchanged, find it alone which could have a serious consequence in the passenger flow, air traffic and passenger security. Within this area, the luggage is not controlled anymore, only the person and his ID are.
9	Authenticate a luggage with creased tag	Luggage Anomaly Detection (LAD)	In the BHS, at the manual coding station, an agent uses the tablet of the LAD to scan the tag and visualize the pictures of the luggage to confirm that the creased was accidental and no one has picked a tag from another luggage to place on this one. **Note:** Without SATIE, the agent does not control if the luggage tag belongs to the luggage or not. As of today, he does not have the means to do so.
10	Identify a luggage without a tag	Luggage Anomaly Detection (LAD)	In the BHS, at the manual coding station, an agent takes a picture of different angles of the luggage and submit for an identification

			search to the system. The system presents a list of potential candidates with pictures to the agent. The agent identifies the luggage and can generate a new tag for the luggage for being processed immediately to its destination. **Note:** Without SATIE, when the agent cannot identify the luggage, he will redirect it for further investigation as he does not know who is the owner and to which destination it should go too. Today, there is no easy way to do that and it takes time. Usually in such situation the luggage will be pushed to lost and found luggage process, sometime being opened to identify any clue on the owner. For sure the luggage will not take the plane with the passenger.
11	Authenticate a luggage	Luggage Anomaly Detection (LAD)	In the BHS, before the agent places a luggage on the cart for being loaded into the plane, he uses the tablet of the LAD to scan the luggage tag and visualize immediately the pictures of the luggage, its owner information and its destination. Confirming by the way the correspondence between the luggage and its tag. **Note:** Without SATIE, the agent does not know if the tag belongs to the luggage or not. He just knows that the tag is a valid one for the destination
12	Identify a luggage	Luggage Anomaly Detection (LAD)	At the plane station, when a luggage needs to be removed from the plane

			because the passenger is not in and the boarding is closed, the agent uses the tablet of the LAD to enter the luggage tag ID and visualize immediately the pictures of the luggage that needs to be removed. **Note:** Without SATIE the identification of the luggage to be removed from the plane takes time because the agent does not have any idea of the shape/colour of the luggage and needs to scan all the luggage one by one to identify the right one. This has an impact on plane schedule and could delay things in cascade. That is why usually there is several calls for the missing passengers by the agent.

2.2.2 Sub-scenario #2 "The Ransom"

The following Table 2.2, Figure 2.6 and Figure 2.7 show details of "The Ransom" sub-scenario.

Table 2.2: Sub-scenario #2 "The Ransom"

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
1	Corrupted Check-in agent enters the airport and go beside check-in counter. He carries a USB stick with the malware and inserts it into a check-in workstation.			
2	Malware is deployed on the workstation.			

	A network scan is initiated by the malware. The malware spreads through the BHS network using the EternalBlue exploit.			
3	The ransomware attacks the Supervisory Control and Data Acquisition (SCADA), cyphering the SCADA files, putting BHS out of service.		This attack has been launched on the BHS Digital Twin to validate the behaviour of the Malware.	The behaviour in demonstration was the same than on the simulation platform.
4	The attacker demands a ransom to give back the access to the BHS operators and ransom note is displayed on BHS workstation screen.			
5	An agent of the SOC, is in front of his computer. It does what is necessary to solve the alert	Ransomware Analyser Correlation Engine Incident Management Portal	This attack has been launched on the BHS Digital Twin to validate the detection through malware analyser, the reception of the log by Correlation Engine and the Alert display in SOC Interface.	Implemented at airport site, raised alerts passed to CyberRange and displayed to SOC operators at airport site. The expected behaviour was the same as with the digital twin.
6	The SOC operator uses BIA to see the propagation paths the attacker can take to compromise	BIA tools	The BIA has been validated on the simulation environment	Same behaviour than on the simulation platform

	the baggage handling system			

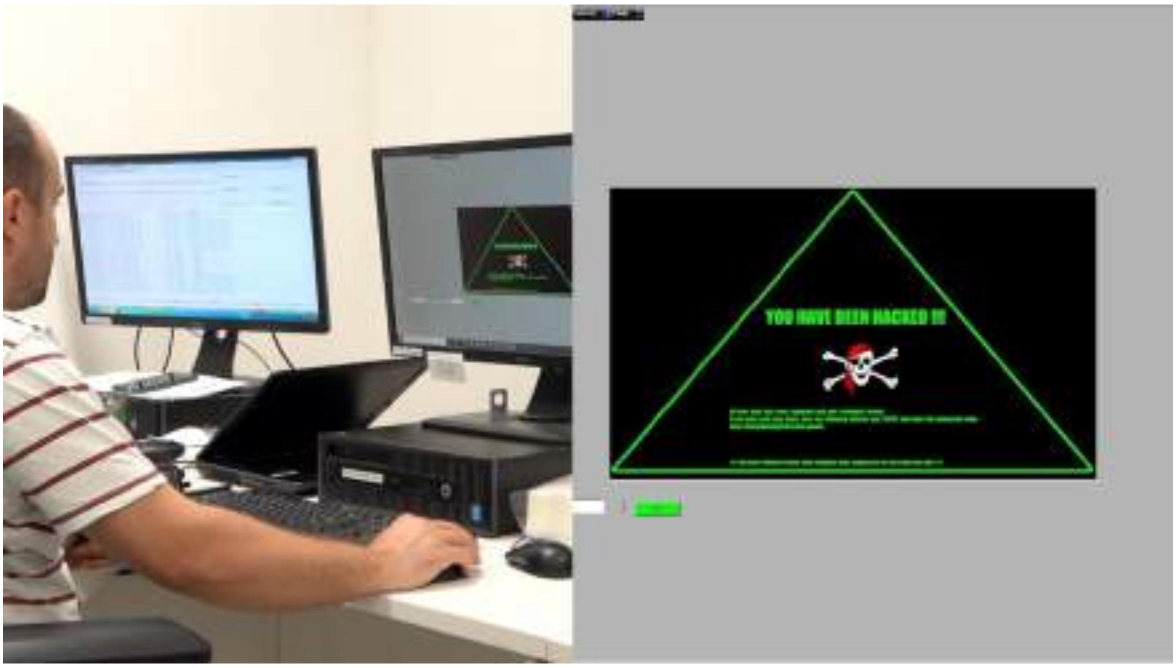


Figure 2.6: Possible outcome of the "The Ransom"

Figure 2.7: SOC operator recognizing an attack with usage of SATIE Toolbox in Airport Operations Centre

2.2.3 Sub-scenario #3 "The Wrong Hold"

The following Table 2.3, Figure 2.8 and Figure 2.9 show details of "The Wrong Hold" sub-scenario.

Table 2.3: Sub-scenario #3 "The Wrong Hold"

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
1	Check the Wifi Endpoint.			
2	A Main In The Middle (MITM) attack on the communication between SAC and ICS PLC is performed and the destination carousel is changed.			
3	The baggage does not go to the Carousel DD and DA go to the chute for problems bag SA020.			
4	An agent of the SOC, is in front of his computer. He alerts the Baggage Handlers to go to the new destination carousel. When there would be no SATIE alerting and detection tools, any bags could be loaded into the aircraft. This catastrophic event would certainly result in financial casualties. events.	BP-IDS ComSEC Correlation Engine Incident Management Portal	This attack has been launched on the BHS Digital Twin to validate the detection through the Physical Probe ComSEC and virtual probes BP-IDS installed in the digital twin platform, the reception of the logs by Correlation Engine and the alert display in SOC Interface.	The physical probes ComSEC have been inserted in the network of the real BHS. The CyberRange stored the virtual probes BP-IDS. Implemented at airport site, raised alerts passed to CyberRange and displayed to SOC operators at airport site. The same expected behaviour occurred as with the digital twin.

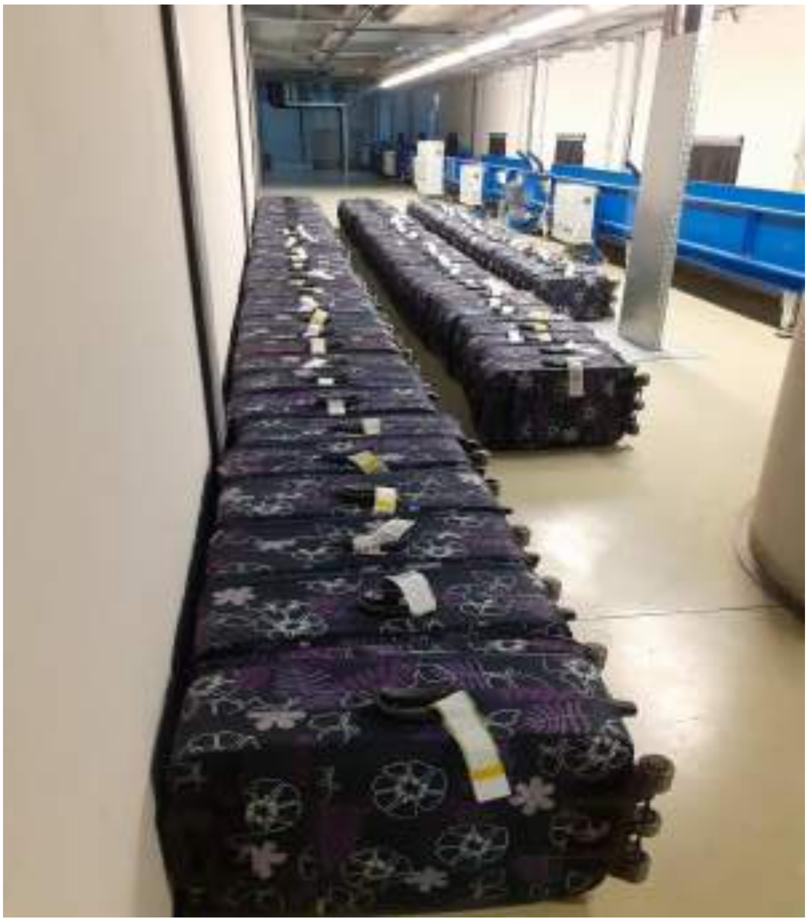


Figure 2.8: Purchased bags behind check-in counters ready for the demonstration

Figure 2.9: Filming of the baggage handling operator during the demonstration for the live stream

2.2.4 Sub-scenario #4 “The Lost Baggage”

The following Table 2.4, Figure 2.10 and Figure 2.11 show details of “The Lost Baggage” sub-scenario.

Table 2.4: Sub-scenario #4 “The Lost Baggage”

Scenario Step	Description	Involved Tools	Simulation Set-Up	Demonstration Set-Up
1	Corrupted BHS operator enters the secured airside using his valid ID card, and goes in the BHS area. He carries a Raspberry Pi and connects it to a			

	port on a BHS switch.			
2	Raspberry Pi floods the BHS network and network loop is created. A Distributed Denial-Of-Service (DDoS) attack is performed on the BHS.			
3	The BHS system is disorganized - the SAC temporarily cannot send order to PLCs and thus sort the bags.			
4	An agent of the SOC, is in front of his computer. He alerts the Maintenance operator to use the degraded maintenance procedures, which leads to make operator to force all bags being rejected to security chute.	BP-IDS ComSEC Correlation Engine Incident Management Portal	The DDOs attack was launched on the digital twin platform. The sorter was full of baggage because it couldn't sort any ones, due to the fact that the network was so busy that the softwares couldn't communicate together. After a long time, the baggage pieces were automatically throwed in a special chute. Thanks to the SATIE Solution, the operators realized that the time was too long and that they had to put a procedure to shorten this time before the system	We didn't realize this test for the demonstration on 27th July 2021 but we did it during our preparation period in the weeks before. The behaviour was the same as with the digital twin

			to send to the special chute.	
5	Undoubtedly a certain amount of baggage would remain unloaded into the aircraft before scheduled departure times. That way some bags will be lost and will have to be processed through the lost & found office - that is why this storyline is called "The Lost Baggage".			

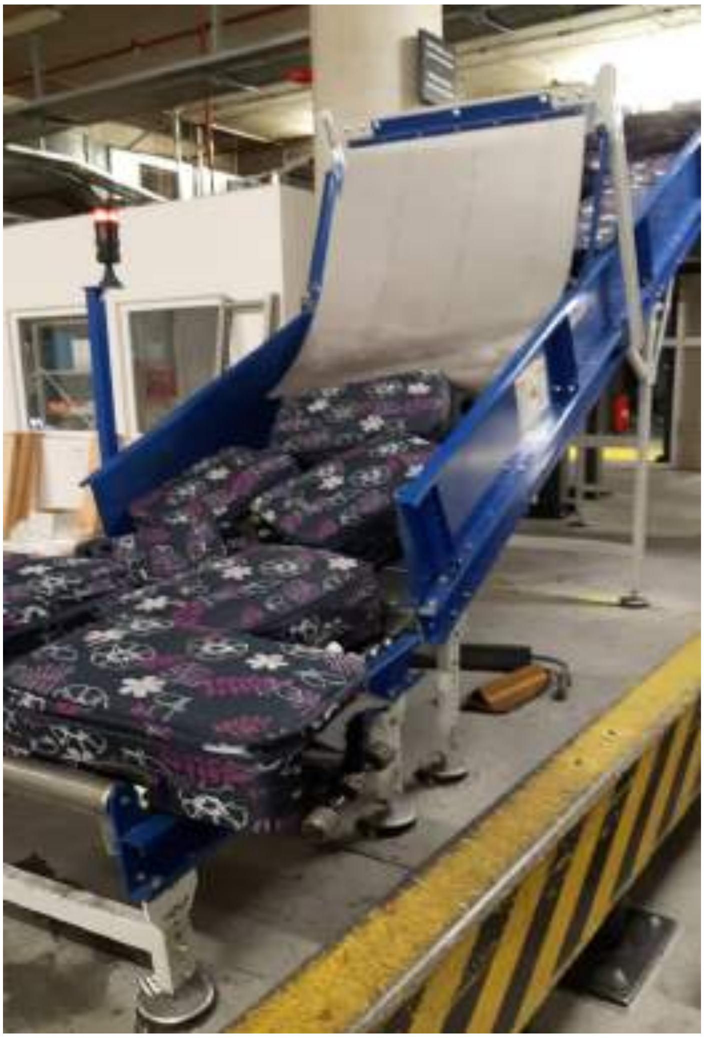


Figure 2.10: Bags finishing at the wrong BHS carousel and not loaded into the aircraft

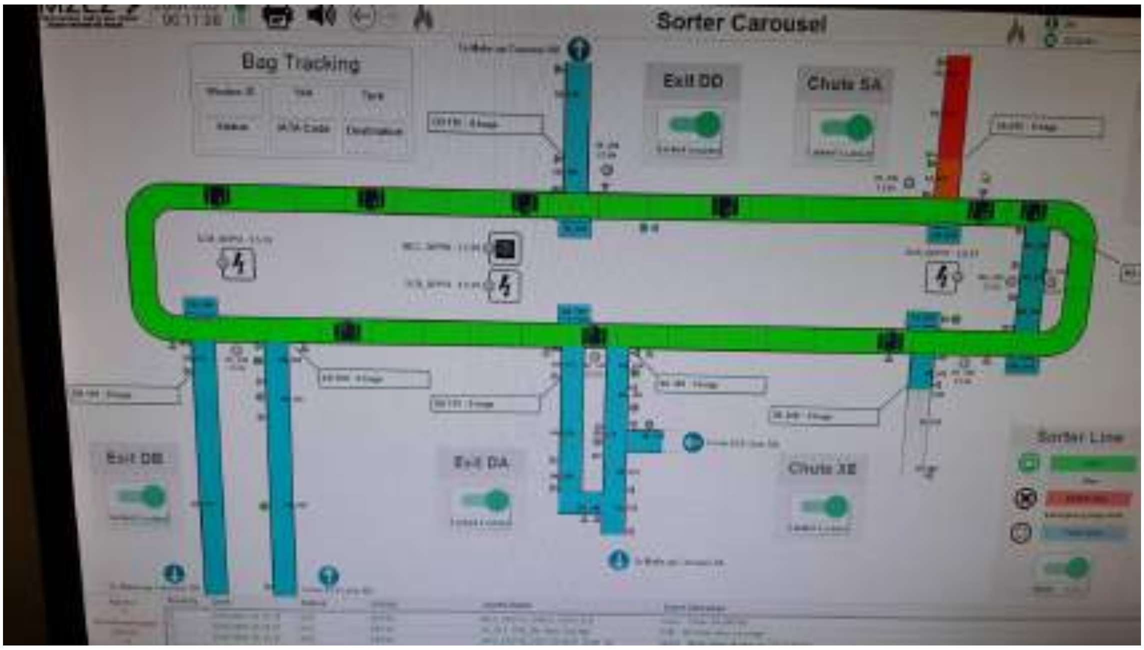


Figure 2.11: Problematic carousel loaded with bags and marked red on the SCADA workstation

3 SATIE response

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

3.1 Correlation Engine

The Correlation Engine was used in three of the four sub-scenarios; it received events from the physical and cyber SATIE threat detection systems. The main detection system are Malware Analyser, ComSEC and BP-IDS. Figure 3.1 shows an example of events displayed in the Correlation Engine.

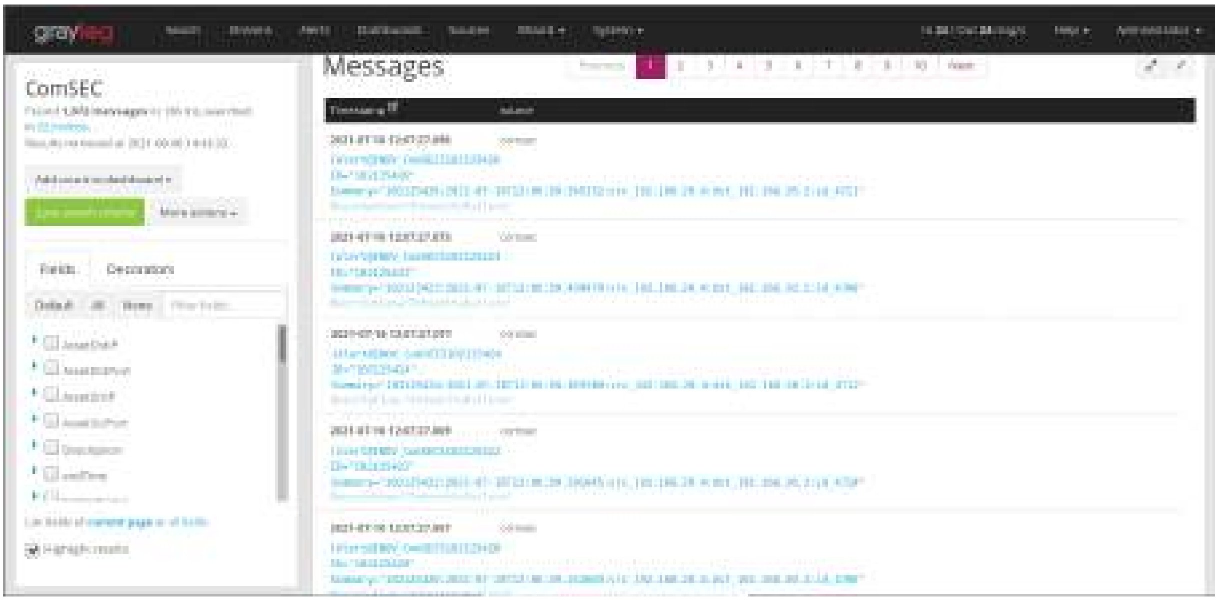
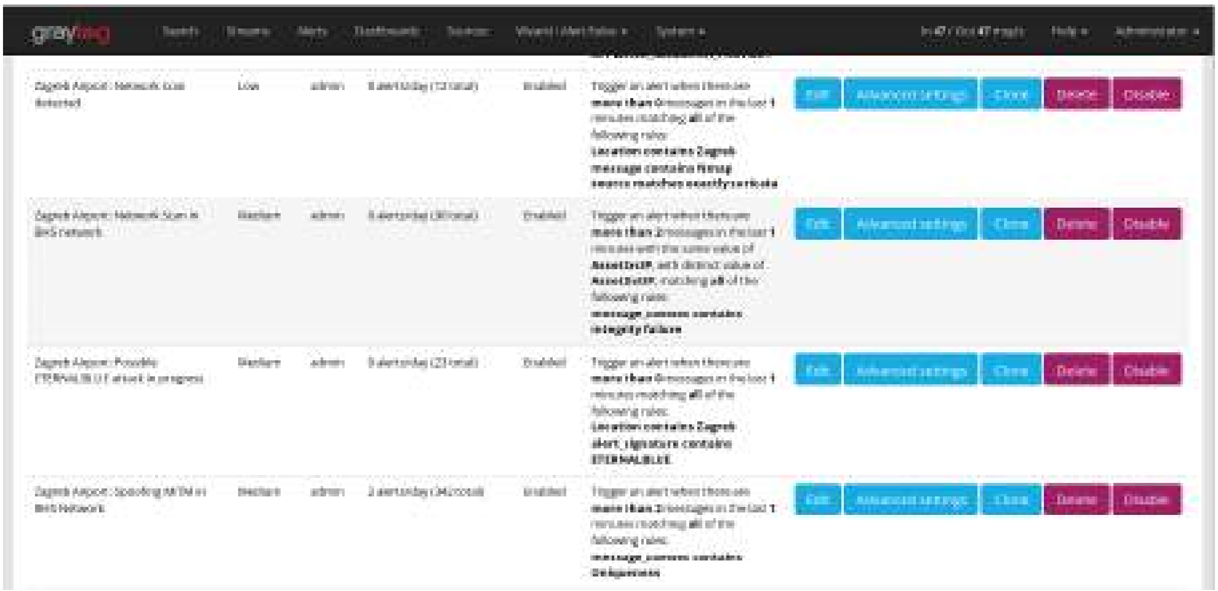


Figure 3.1: Correlation Engine events

With different rules defined, an alert was raised to the Incident Management Portal. Figure 3.2 below shows examples of rules.



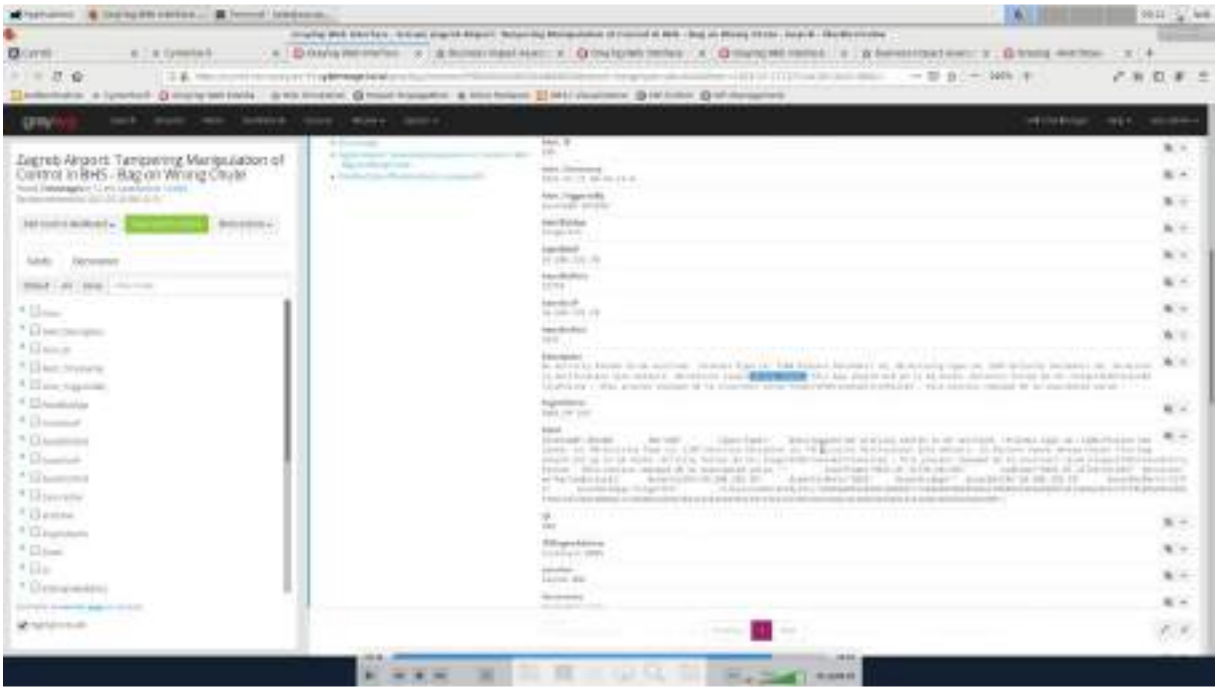
Zagreb Airport : Network Scan detected	Low	admin	0 alert today (12 total)	Enabled	Trigger an alert when there are **more than** 0 messages in the last **1** minutes matching **all** of the following rules: **location contains Zagreb** **message contains Nmap** **source matches exactly suricata**
Zagreb Airport: Network Scan in BHS network	Medium	admin	0 alerts today (30 total)	Enabled	Trigger an alert when there are **more than** 2 messages in the last **1** minutes with the same value of **AssetDstIP**, with distinct value of **AssetSrcIP**, matching **all** of the following rules: **message_content contains integrity failure**
Zagreb Airport: Possible ETERNALBLUE attack in progress	Medium	admin	0 alerts today (23 total)	Enabled	Trigger an alert when there are **more than** 0 messages in the last **1** minutes matching **all** of the following rules: **location contains Zagreb** **alert_signature contains ETERNALBLUE**
Zagreb Airport: Spoofing MiTM in BHS Network	Medium	admin	2 alerts today (342 total)	Enabled	Trigger an alert when there are **more than** 2 messages in the last **1** minutes matching **all** of the following rules: **message_content contains [illegible]**

Figure 3.2: Correlation Engine rules

The first sub-scenario is “The Wrong Hold”. Table 3.1 shows the alert raised with events from ComSEC and BP-IDS and Figure 3.3 shows the BP-IDS event received in the Correlation Engine

Table 3.1: Raised alerts form sub scenario “The Wrong Hold”

Time	Title	Detection systems	Affected assets
00:01	Network Scan in BHS network	ComSEC	BHS Network
00:03	Spoofing MiTM in BHS Network	ComSEC	PLC
00:04	Tampering Parameter modify in BHS network packet	ComSEC	PLC
00:05	Tampering Manipulation of control in BHS– Bag on Wrong Chute	BP-IDS	PLC



Zagreb Airport: Tampering Manipulation of Control in BHS - Bag on Wrong Chute

Figure 3.3: BP-IDS event

The second sub-scenario is “The Ransom”. The Table 3.2 shows the alerts raised from events from Suricata, which is an intrusion detection system, and ComSEC.

Table 3.2: Alerts raised in the sub-scenario “The Ransom”

Time	Title	Detection systems	Affected assets
00:01	Network scan detected	Suricata	BHS Network
00:03	Tampering Parameter modify in BHS network packet	ComSEC	SCADA
00:04	Possible ETERNALBLUE attack in progress	Suricata	SCADA

The third sub-scenario, the Correlation Engine was involved, is “The Lost Baggage”, Table 3.3 shows the alerts raised with events from ComSEC and Figure 3.4 shows the events received by the Correlation Engine.

Table 3.3: Alerts raised in sub scenario “The Lost Baggage”

Time	Title	Detection systems	Affected Assets
00:02	Tampering Parameter modify in BHS network packet	ComSEC	PLC
00:02	DDoS attack in progress on BHS	ComSEC	PLC

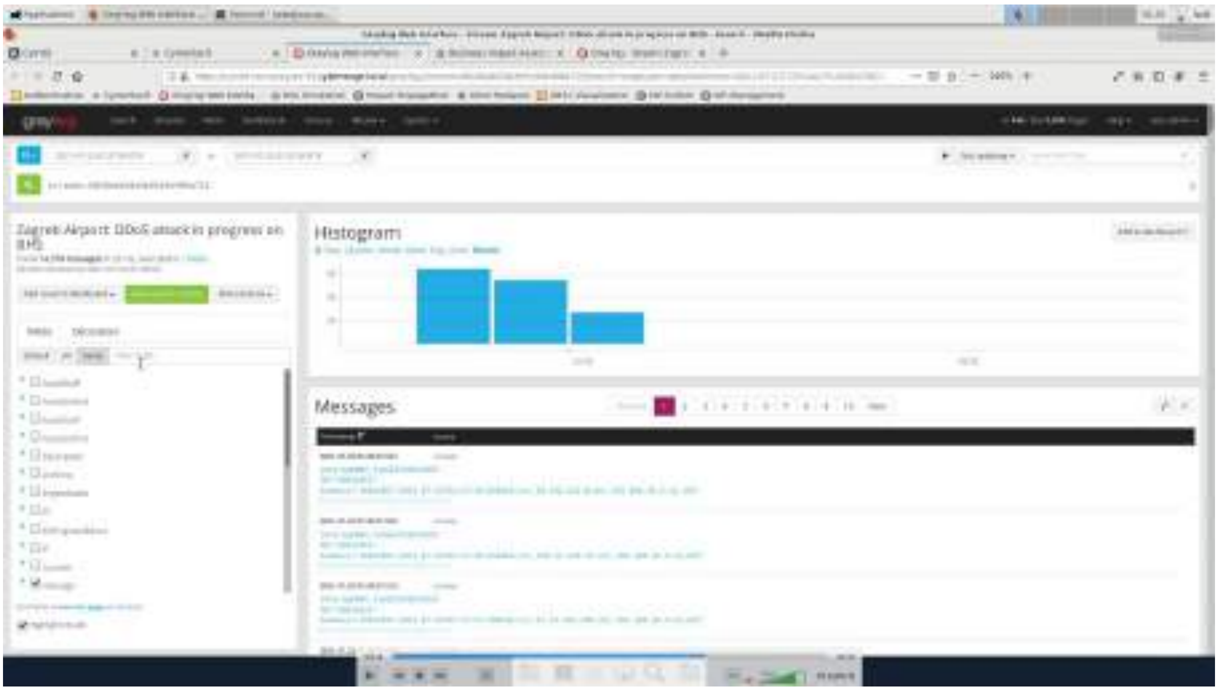


Figure 3.4: ComSEC events

3.2 Incident Management Portal

The Incident Management Portal received alerts from the Correlation Engine. An operator checks each alert, and assigns it to another operator that will be in charge of the investigation. The operator can classify the alert as an incident or close it. From the Incident Management Portal, the operator can access the Business Impact Assessment, and the Correlation Engine to go further in the investigation.

The Table 3.4 shows the list of alerts received in the Incident Management Portal for the sub-scenario "The Wrong Hold".

Table 3.4: Alerts and incident raised in the sub-scenario "The Wrong Hold"

Time	Title	Severity	Affected assets	Operator actions
00:01	Network Scan in BHS network	Medium	BHS Network	Convert to incident
00:03	Spoofing MiTM in BHS Network	Medium	PLC	Convert to incident
00:04	Tampering Parameter modify in BHS network packet	Medium	PLC	Convert to incident
00:05	Tampering Manipulation of control in BHS– Bag on Wrong Chute	High	PLC	Call the BHS operator to confirm, and convert to incident

Figure 3.5 shows the view of the Incident Management Portal by an operator with the alert received for the sub scenario “The Wrong Hold”.

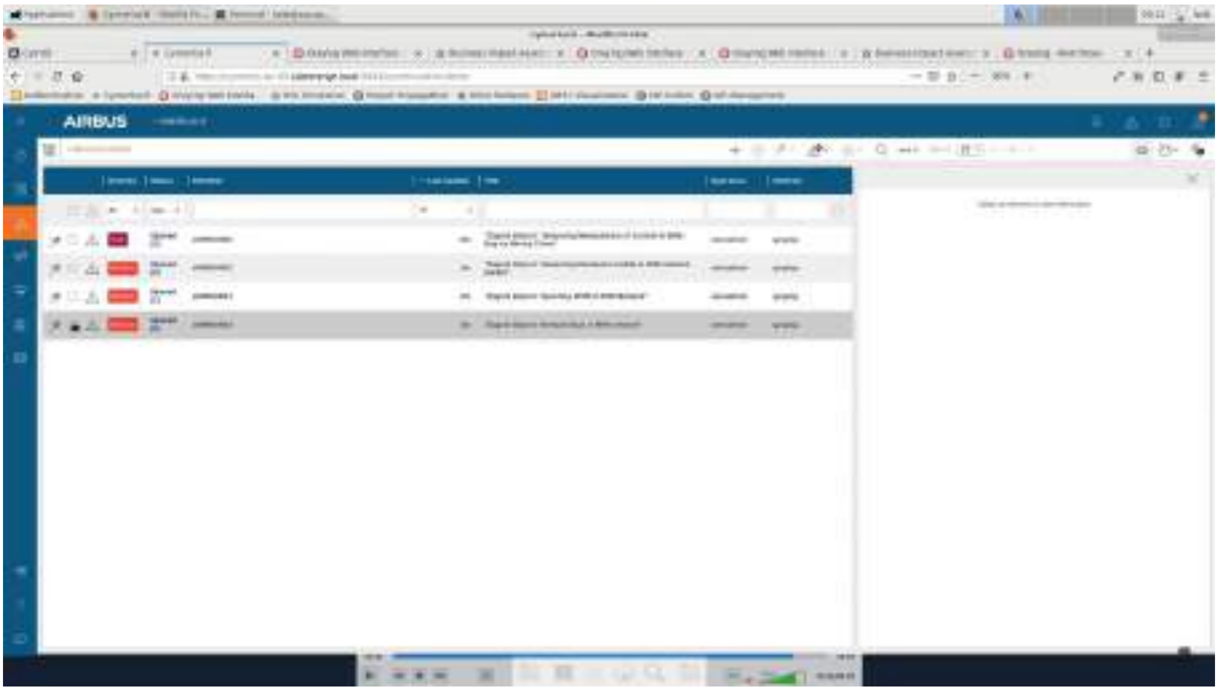


Figure 3.5: Alerts in the sub-scenario “The Wrong Hold”

Table 3.5 shows the list of alerts received in the Incident Management Portal for the sub scenario “The Ransom”.

Table 3.5: Alerts and incidents raised in the sub scenario “The Ransom”

Time	Title	Severity	Affected assets	Operator actions
00:01	Network scan detected	Low	BHS Network	Nothing
00:03	Tampering Parameter modify in BHS network packet	Medium	SCADA	Convert to incident
00:04	Possible ETERNALBLUE attack in progress	Medium	SCADA	Call the SCADA operator, who confirm that an attack is in progress. Change the severity to high and convert to incident.

Figure 3.6 shows the view of the Incident Management Portal by an operator with the alert received for the sub scenario “The Ransom”.

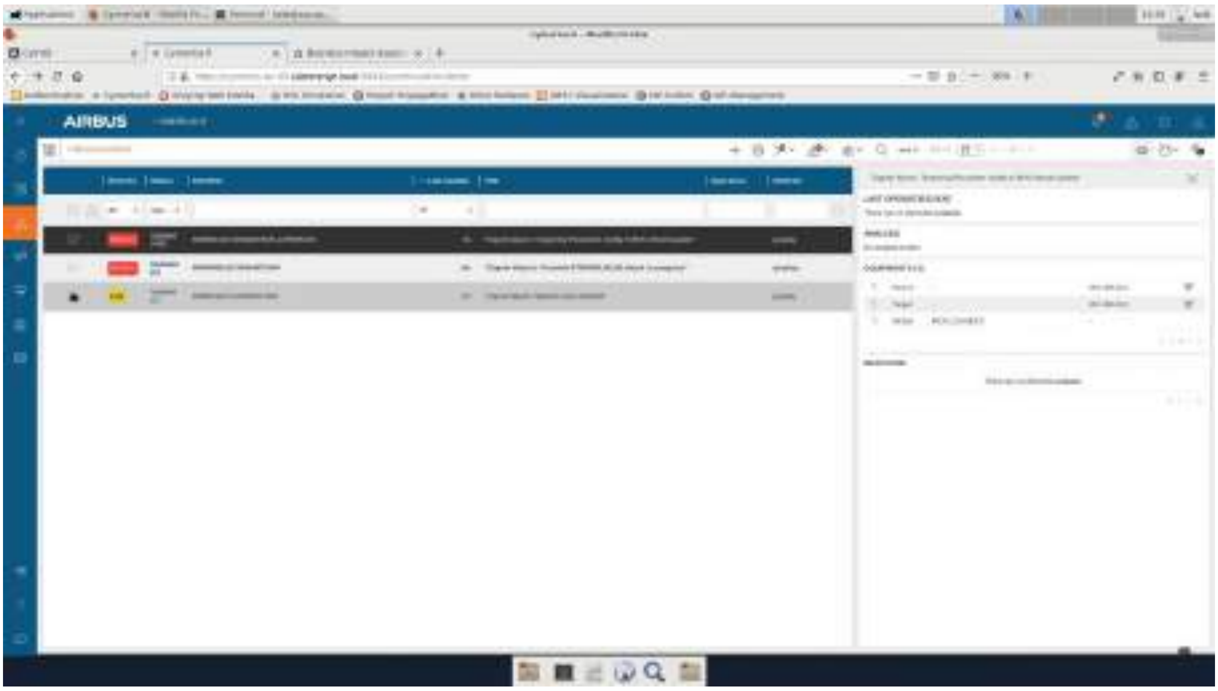


Figure 3.6: Alerts in sub-scenario "The Ransom"

Table 3.6 shows the list of alerts received in the Incident Management Portal and Figure 3.7 the view of the operator for the sub-scenario "The Lost Baggage".

Table 3.6: Alerts and incidents raised in the sub-scenario "The Lost Baggage"

Time	Title	Severity	Affected assets	Operator actions
00:02	Tampering Parameter modify in BHS network packet	Medium	PLC	Nothing
00:02	DDoS attack in progress on BHS	High	PLC	Convert to incident

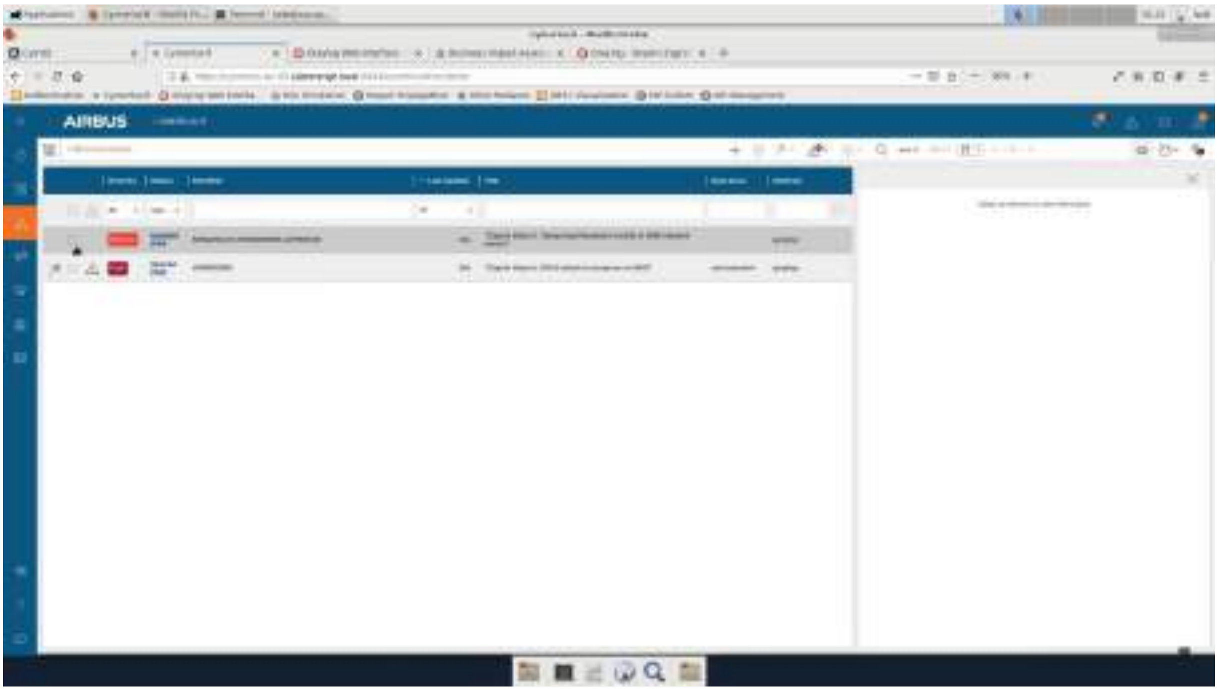


Figure 3.7: Alerts in sub-scenario “The Lost Baggage”

3.3 GLPI / Vulnerability Management System

During the Zagreb Airport demonstration, the Vulnerability Management System (VuMS) and GLPI (Gestion Libre de Parc Informatique) were presented.

The role of the Vulnerability Management System is to prevent cyber-attacks that exploit cyber vulnerabilities. Within the sub-scenario "The Ransom", it triggers an early alert when the vulnerability exploited by the EternalBlue exploit is detected on a managed asset.

Figure 3.8 shows the alert in the Incident Management Portal that results from the detection of the vulnerability on a test machine (which is not integrated into the BHS digital twin). This alert would have been triggered before the execution of the sub-scenario "The Ransom" because it is raised at the time of the *detection* of the vulnerability, not at the time of the *exploitation* of the vulnerability.

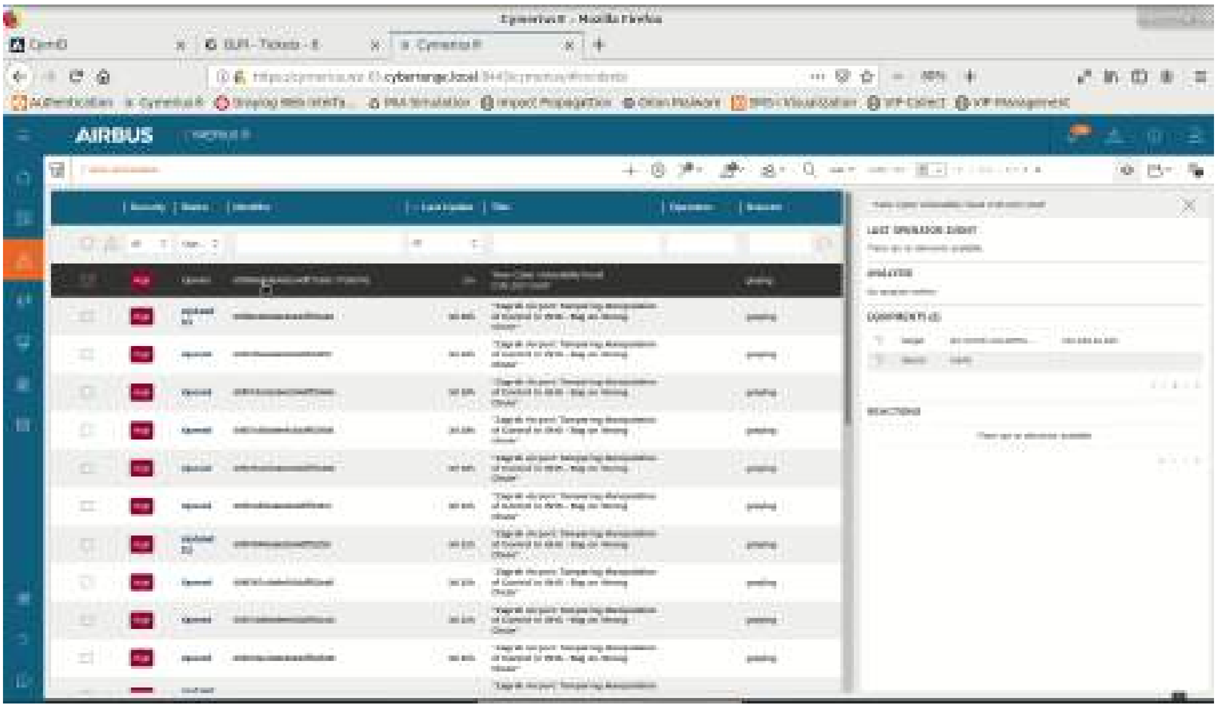


Figure 3.8: An alert in the Incident Management Portal, generated by the Vulnerability Management System

GLPI integrates an efficient inventory solution for both IT assets (computers, displays, peripherals, network equipment...) as well as physical assets. For IT assets, inventories are built automatically using an inventory agent deployed on the assets. GLPI inventories are made available for other SATIE Tools via a REST API.

An inventory contains the complete list of the software installed on the managed assets. Figure 3.9 displays the software inventory of a test asset, showing software and their associated version number.

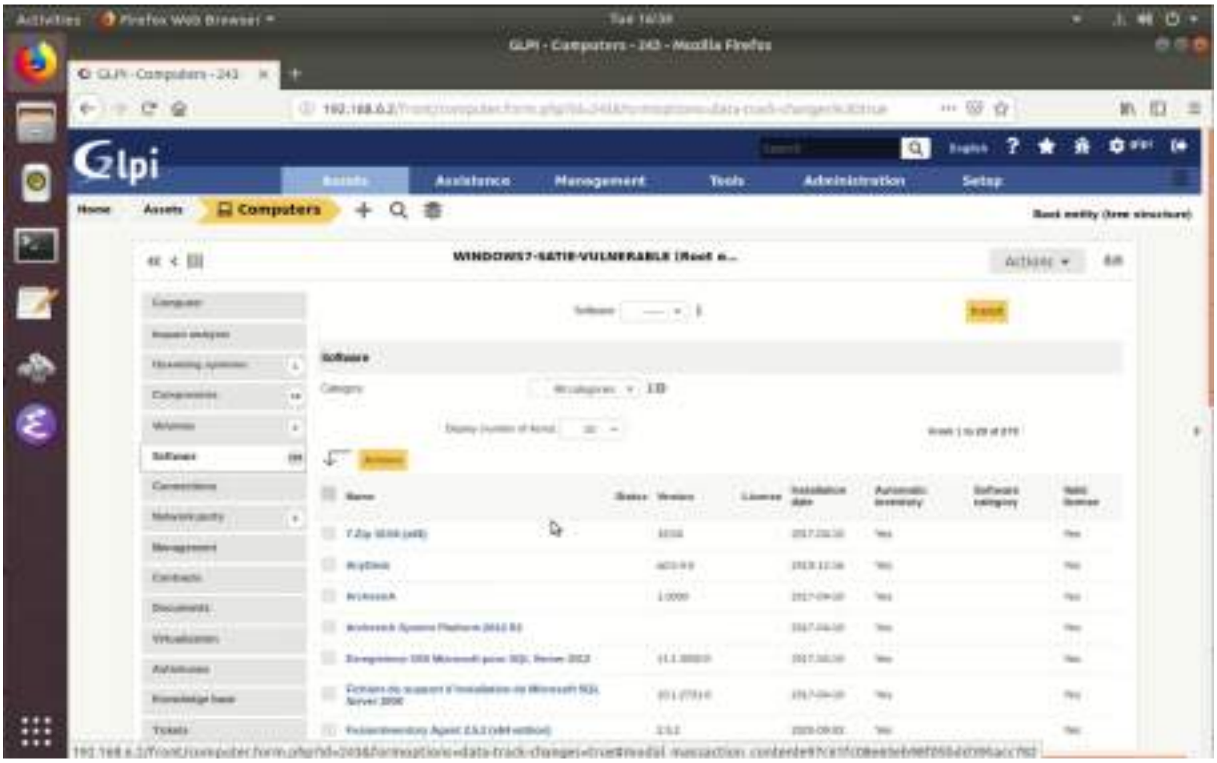
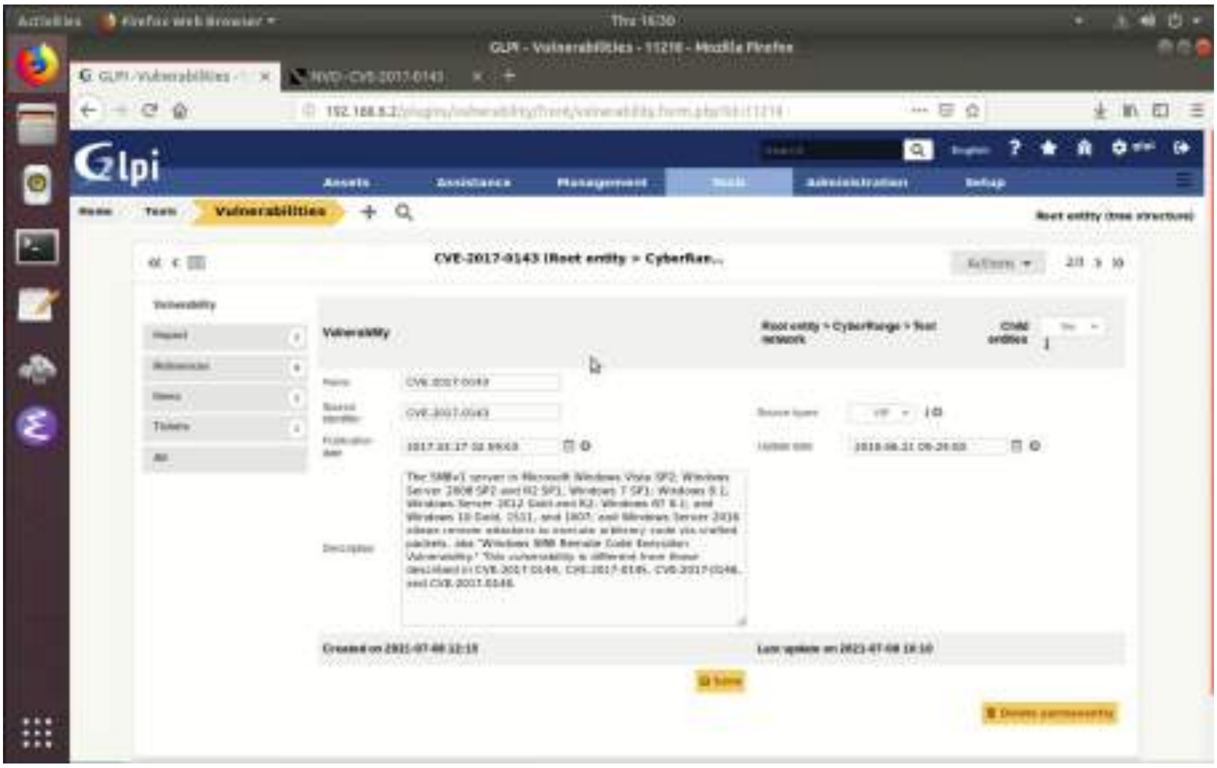


Figure 3.9: Inventory of an asset with installed softwares

Based on the inventory of software, matching software name and version allows to establish whether the installed software is vulnerable to know vulnerabilities. Figure 3.10 presents the details of a CVE (Common Vulnerabilities and Exposures) vulnerability as it is stored in GLPI.



CVE-2017-0143 (Root entity > CyberRan...

Vulnerability — Root entity > CyberRange > Test network

Name: CVE-2017-0143

Source identifier: CVE-2017-0143

Description: The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Figure 3.10: Details of a CVE vulnerability in GLPI

Vulnerability data (description, date, impact...) are obtained by the Vulnerability Intelligence Platform, or VIP. Figure 3.11 shows the same vulnerability stored in VIP. VIP, apart from being the main data source for VuMS, is also used to perform matching between software/version and known vulnerabilities.

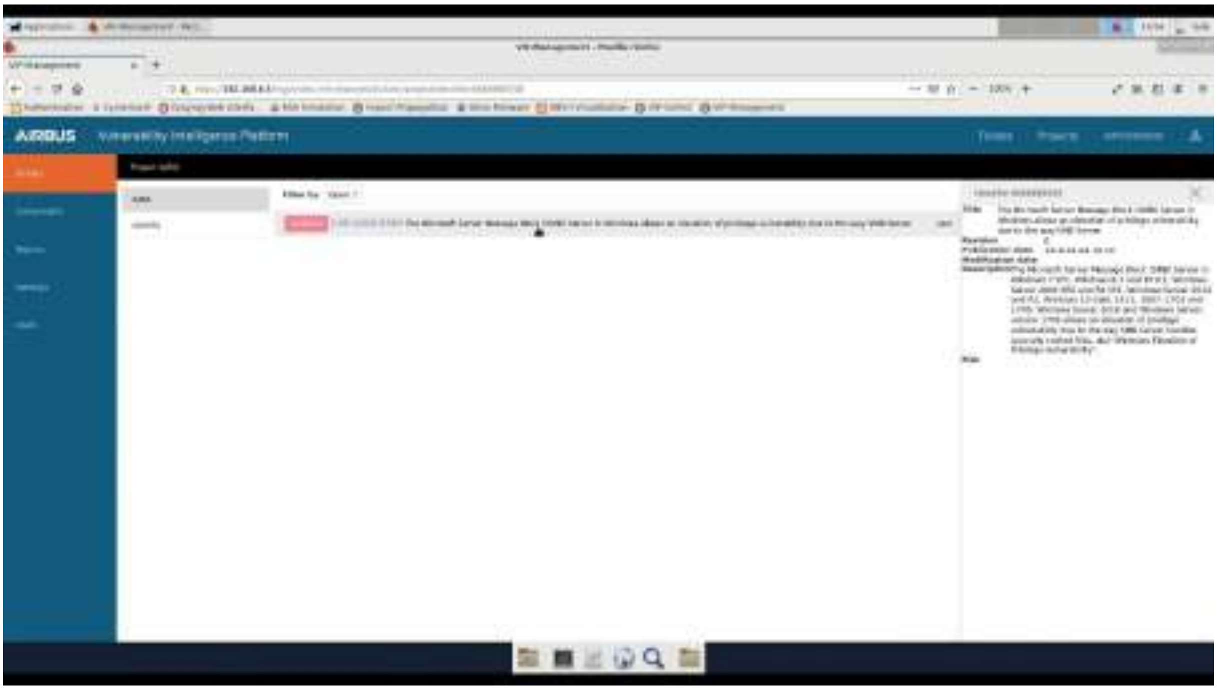
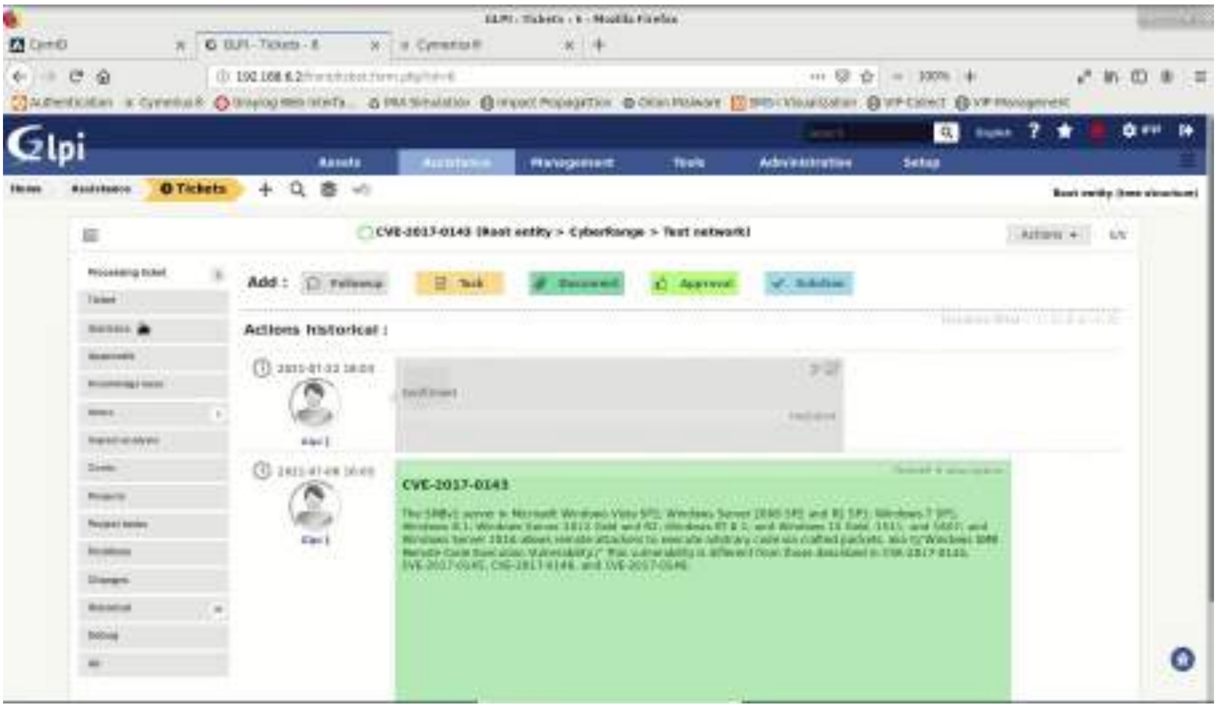

VIP Management - Mozilla Firefox
AIRBUS
Vulnerability Intelligence Platform

Figure 3.11: A vulnerability in VIP

After scanning assets for vulnerabilities, vulnerable assets are signalled to the SOC operators by generating a GLPI ticket. The confirmation of the vulnerability by a possible manual review will in turn trigger an alert in the Incident Management Portal. Figure 3.12 presents such a ticket, containing all needed information (vulnerable assets, vulnerability, severity).



CVE-2017-0143 (Root entity > CyberRange > Test network)

CVE-2017-0143

The SMBv1 server in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Figure 3.12: GLPI ticket associated with a vulnerability detection

3.4 ComSEC, BP-IDS and BIA

To demonstrate sub-scenarios #2 and #3 (“The Ransom” and “The Wrong Hold”) of the Zagreb demonstration ComSEC and BP-IDS inspected the BHS network traffic, while BIA served as an IMP supporting tool for the investigation conducted by the operator. To that end, the Zagreb demonstration encompassed two stages: the installation and public demonstration.

3.4.1 Installation stage

The three tools followed a different schedule for the installation stage. The first tool deployed was ComSEC, on 28 June 2021. Two physical hardware ComSECs were connected on the BHS, one for each PLC. ComSEC was placed with one network interface connected to one PLC, and another network interface connected to the BHS switch, and one network interface connected to the simulation platform. During the period the ComSECs were deployed, they served as a bump-in-the-wire for all traffic that reached the PLCs. With this ComSEC inspected the network traffic and forwarded any detected integrity failures to the SOC. Throughout June, 28th (installation day) until July, 28th (end of demonstration), ComSEC operated continuously including during the normal airport operation period. Throughout the time ComSEC was active, there were no downtime nor there were any necessity to intervene for troubleshooting. Thus, showing ComSEC is compatible with the BHS infrastructure and capable of withstanding the airport normal operation conditions. Pictures of the deployment can be seen in Figure 3.13. The pictures show ComSEC installed on the airport switches where the PLCs are located. In the deployment ComSEC was strategically placed in the switch cabinet since the switch is protected by lock, showing that in an airport installation it would be very difficult to have physical access ComSEC, since it would be as difficult as accessing a network switch (which only a limited number of authorized personnel have access to).

The other two tools, BP-IDS and BIA, were deployed inside the simulation platform, which was installed on the Zagreb site at July 12th. Since both tools function using specification, the migration from the BHS installation in Elancourt (reported on deliverable D6.3 (2)) to the installation on BHS of Zagreb required changing the specification. This was due to mainly two points:

1) Change on the network topology – There were differences between the Elancourt BHS digital twin and the Zagreb real BHS system. Mainly the changes made for adapting to Zagreb involved change the IP addresses of the assets and the network map specified on both BIA and BP-IDS;
2) Changes in BHS business process procedures – BP-IDS and BIA model the behaviour of the BHS as business processes. These processes serve as specification of the BHS procedures the accuracy is imperative to have good results. Although the digital twin provided in Elancourt was a very accurate replica of the Zagreb Airport, both systems still had some differences. Particularly in the communication sent from the PLCs to the decision server (BAGWARE) during baggage screening. Some of the messages that were sent by the digital twin PLCs were omitted on the real system, these differences between real system and the digital twins were particularly hazardous for BP-IDS detection and caused false alarms in all bags inspections performed by the detection tool, before the necessary changes in the specification were performed.

Three days were necessary to make all the necessary changes required for BP-IDS and BIA to be compatible with the BHS. Throughout July 15th (new specification day) until July 28th (demonstration day), BP-IDS and BIA were continuously operating on the simulation platform. During that period, experiments were conducted throughout seven days (six days of rehearsal, and the one day for demonstration). The experiments had the objective to show that BP-IDS could detect bags that were routed by the BHS to wrong locations. To make these experiments, a man-in-the-middle attack was performed between the PLCs to BAGWARE. The man-in-the-middle intercepted all the sortation orders sent from BAGWARE to the PLCs and replaced it with wrong sortation orders. These experiments were able to sort bags expected to go to flight chutes (where the bags are loaded to the plane) to the problem chute (where the bags need to be sorted manually by the operator). Both chutes used in the experiments are presented in the pictures of Figure 3.14.

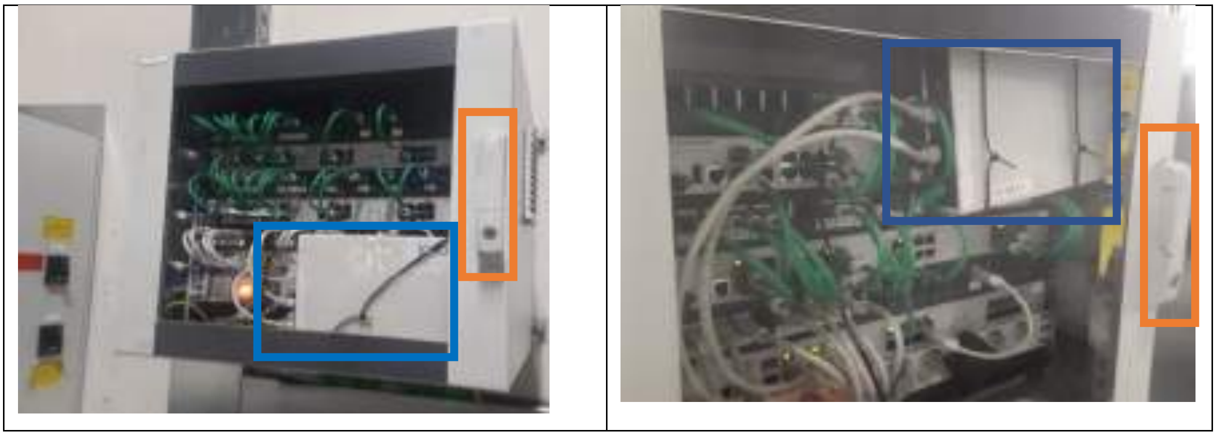


Figure 3.13: ComSEC (in blue) installed on the lock (orange) protected airport switch cabinets

Figure 3.14: Chutes problem and flight used in the demonstration (left and right respectively)

Throughout the experiments a quantitative evaluation was made to the BP-IDS system. Two metrics were used for this measurement. The first metric was the time that BP-IDS required for raising an alert. While the second metric was the number of alerts BP-IDS raised during the experiments.

Regarding the first metric, for each alarm raised by BP-IDS the detection time was measured. To do so, it was measured the timestamp of all messages captured by the BP-IDS sensor (TSc), measured all the timestamps of the corresponding alarms (TSa), and calculated the detection time (TSa – TSc). The detection times are shown in Figure 3.16. The time varied between 1 second to 11 seconds, taking on average 5 seconds to raise the alarm. This shows the BP-IDS detection was in real-time with little delays that allow operators to make a timely decision before bags accumulate in the problem bags chute.

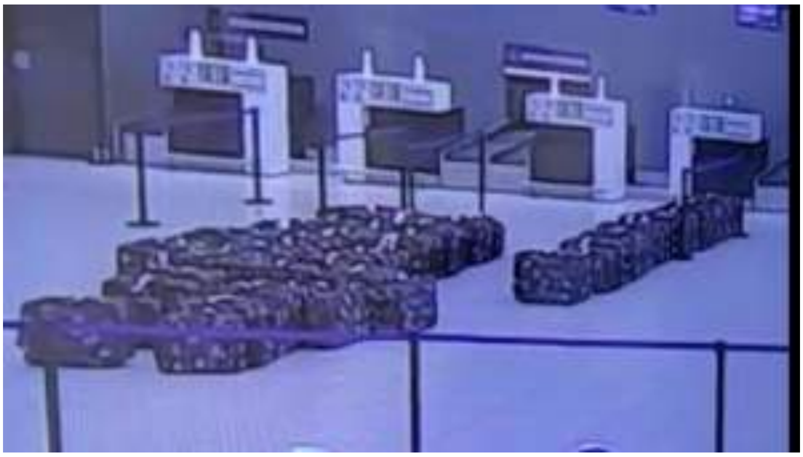


Figure 3.15: CCTV image showing the check-in counters with 30 bags used for demonstration

Regarding the second metric, for each experiment day the number of alarms raised by BP-IDS was registered. As can be seen in Figure 3.17, the number of alarms per day varies between 1 to 80. On the first four days, only four bags were used for the experiment since the aim was to ensure that all components were ready for the demonstration, the number of alarms vary according to the amount of times the experiment was conducted. On the last three days thirty bags were used for the experiment this allowed to have a visual impact on the live audience and to test the systems with high quantity of bags circulating at the same time. As can be seen, on the 5th day BP-IDS raised 80 alarms since the experiment ran several times in order to adjust the lights and camera for the live show, while the 6th and 7th day have more a less the same number of alerts since the 6th day rehearsal attempted to be a full-dress copy of the live show. On all cases BP-IDS was able to detect the bags without false alarms.

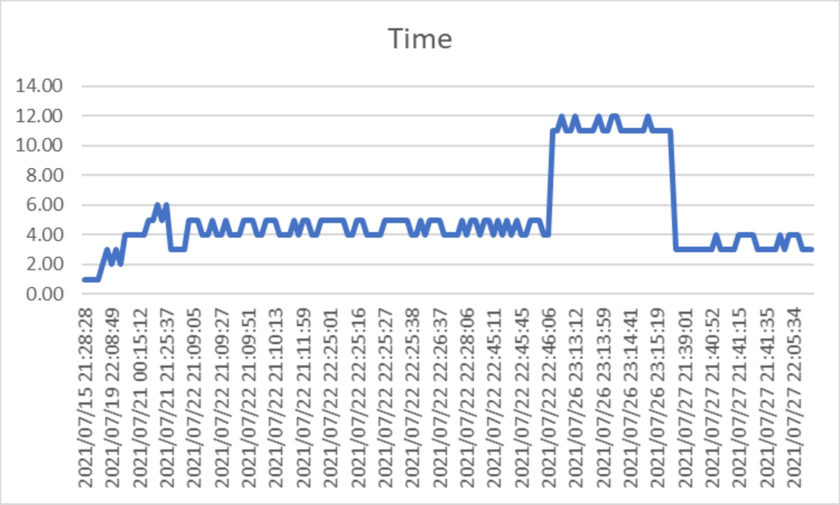


Figure 3.16: Time taken for BP-IDS to raise alerts for bag deviation

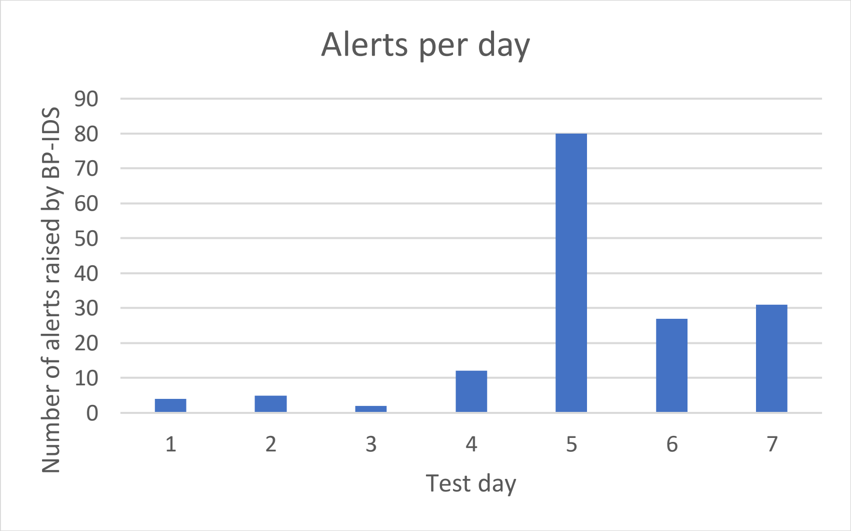


Figure 3.17: Number of alerts raised by BP-IDS per day

3.4.2 Public demonstration stage

During the Zagreb Airport demonstration, the three tools ComSEC, BP-IDS and BIA were presented in two scenarios: sub-scenario #2 “The Ransom” and sub-scenario 3 “The Wrong Hold”.

Regarding the sub-scenario #2 the demonstration was composed of several steps where ComSEC and BIA were involved, which can be summarized as detection and analysis.

In the first step, detection, a ransomware is placed in one the machines of the simulation platform (representing the airport check-in counters computers) and which then automatically propagates to the SCADA system. As can be seen in Figure 3.18, this step is detected by ComSEC system which raises an alert of anomalous communication targeting the SCADA system. The alert is raised since the machine where the ransomware was placed sent a network packet to the SCADA which ComSEC does not allow.

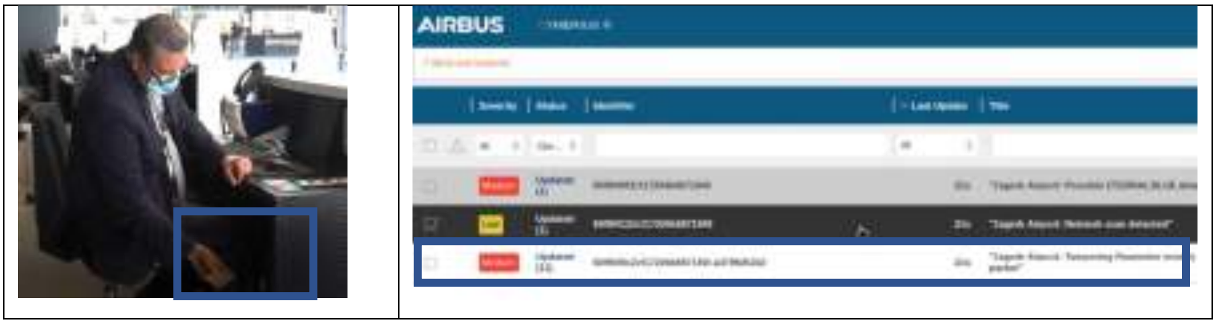


Figure 3.18: Ransomware on the computer (left square), with ComSEC detection (right square)

In the second step the operator analyses the impact of the ransomware in BIA based on the ComSEC alert (Figure 3.19) where the attacker is able to compromise the communications between the BAGWARE and PLCs.

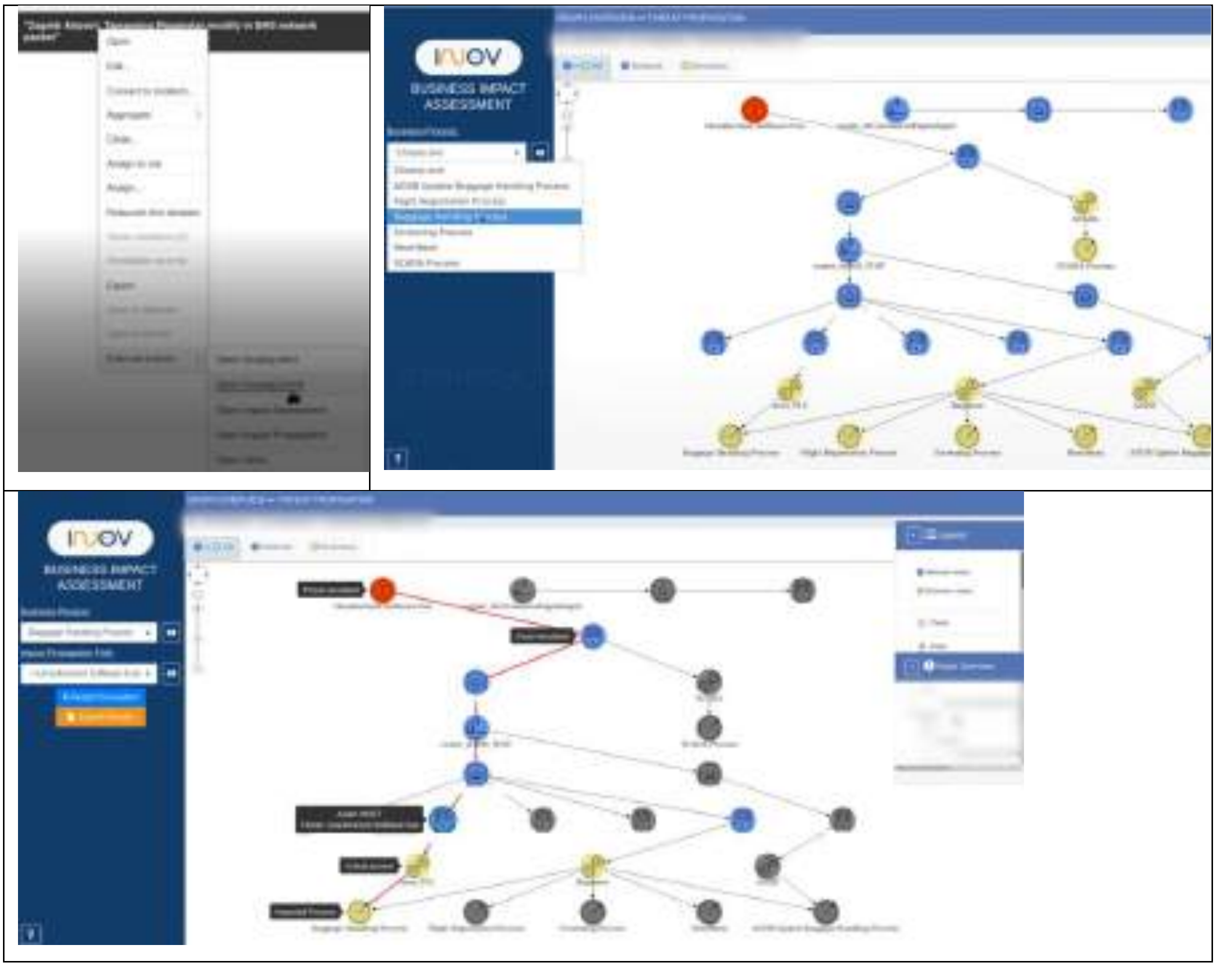


Figure 3.19: Impact assessment conducted by the operator

Regarding the sub-scenario 3, demonstration can be summarized in two steps where ComSEC and BP-IDS were involved: establishing a man-in-the-middle between BAGWARE and PLCs; performing the change of sortation orders.

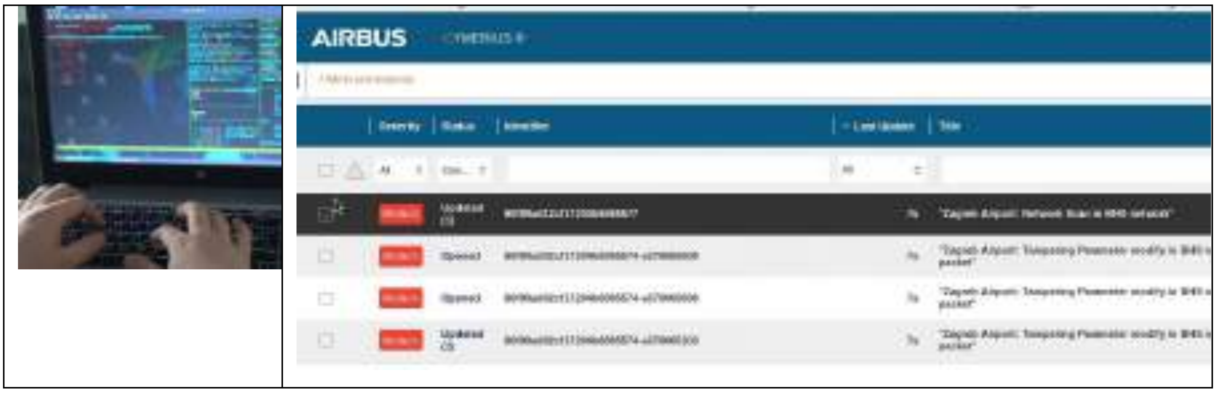


Figure 3.20: Attacker performing the man-in-the-middle and ComSEC alarms

In the first step (depicted in Figure 3.20), an attacker obtains access to the BHS network by cracking the wi-fi credentials of an airport operator employee and launches a man-in-the-middle attack (left picture of Figure 3.20). At this point ComSEC detects the man-in-the-middle attack, since ComSEC has a packet replay protection (right picture of Figure 3.20). This means that due to the man-in-the-middle the PLC's ComSEC will receive two network packets, the original one (sent from the PLC) and one sent by the attacker machine with the same signature, and will thus raise an alert[1].

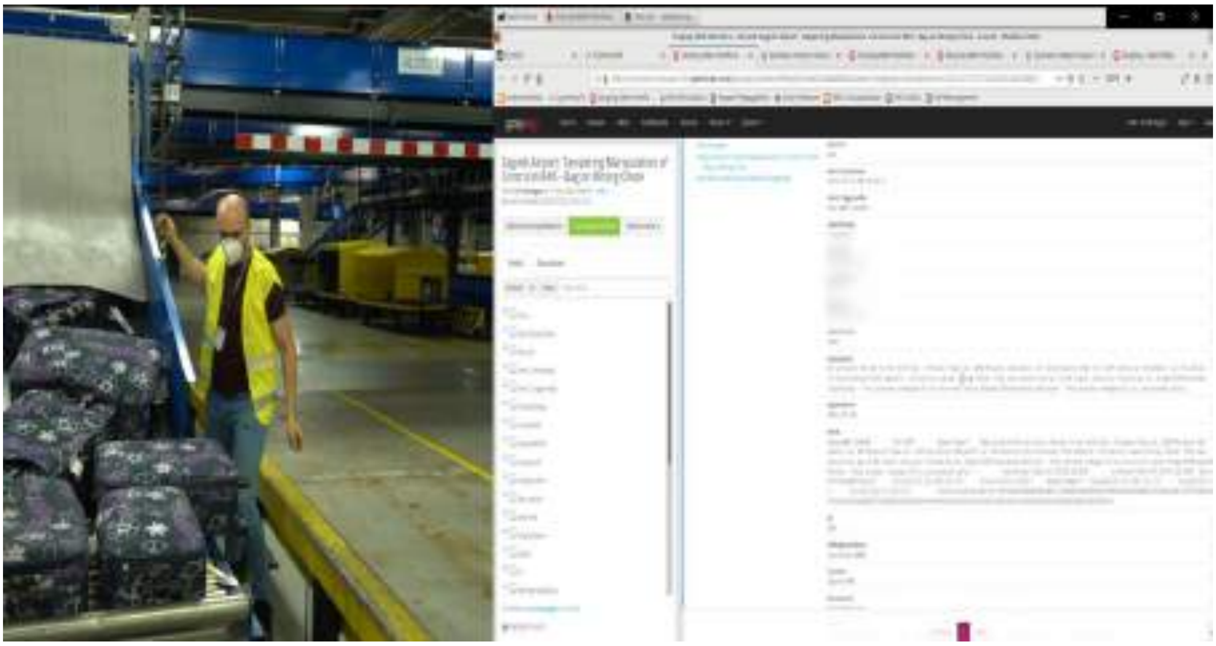


Figure 3.21: Bags wrongly routed to problems chute (left) and BP-IDS real-time detection alarm (right)

In the second step, the attacker makes use of the man-in-the-middle to change the sortation order sent from BAGWARE to the PLC, from flight chute to the problems chute (Figure 3.21 left-side). This is detected by BP-IDS because of its specification[2]. The detection is due to BP-IDS having knowledge of the conditions to which a bag should go to each chute and can validate BAGWARE decisions. Particularly, BP-IDS could inspect the clearance of the bag when the it was screened by the explosive

[1] The packet replay protection mechanism is detailed in the SATIE D3.2 deliverable (5).

[2] The detection technique employed by BP-IDS and how it was applied for BHS incident detection is detailed in the SATIE D4.4 deliverable (6).

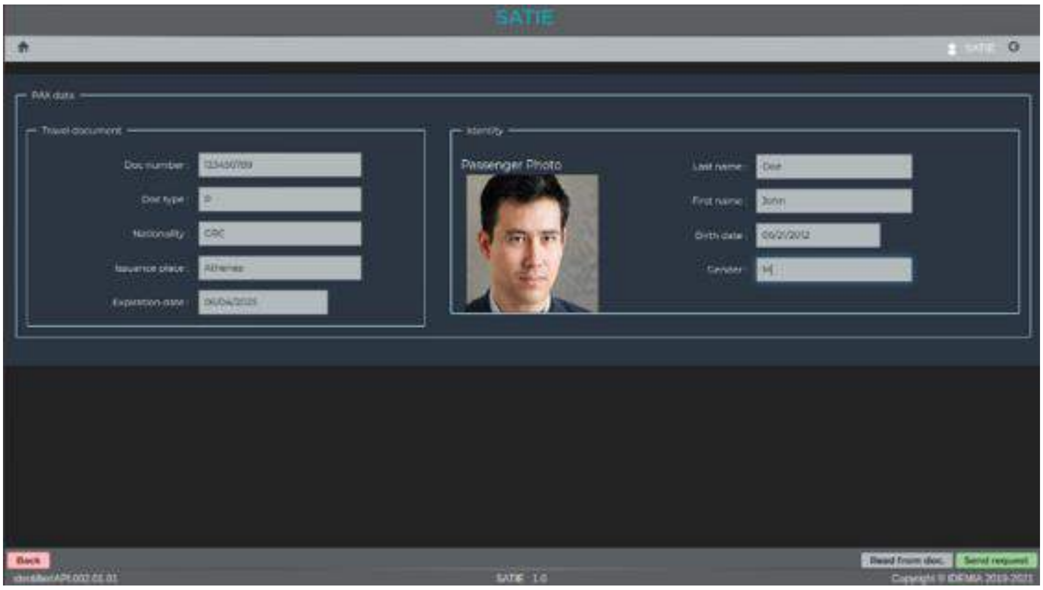
detection machine, and was also able to identify tag based on the automatic tag reader recognition. This gave all the elements for BP-IDS to infer the chute that should be assigned by BAGWARE. This inference allowed in real-time to validate BAGWARE decisions, detect anomalies and raise alerts to the IMP in real-time (Figure 3.21 right-side).

3.5 Anomaly Detection On Passenger Records

During the Zagreb Airport demonstration, the Extended Passenger Concept was presented by combining the Passenger Anomaly Detection (PAD) and Luggage Anomaly Detection (LAD) tools together as Anomaly Detection On Passenger Records (ADPR) tool.

The Extended Passenger Concept relies on that anyone who enters in a restricted area with its items (baggage for example) should have/carry them with him and leave the area with them.

To do so, the Passenger Anomaly Detection tool was introduced at the check-in desk to enhance the current passenger check-in process to control the passenger ID and its travel document before issuing the boarding document, as shown in Figure 3.22.



PAX data

Travel document

Doc number : 123456789

Doc type : P

Nationality : GRC

Issuance place : Athenes

Expiration date : 06/04/2025

Identity

Passenger Photo

Last name : Doe

First name : John

Birth date : 09/21/2012

Gender : M

Figure 3.22: PAD graphical interface

The check is done against a database of known threats and the decision of the risk assessment is displayed to the agent as “OK to Board” or “Further Control Needed”. According to the risk assessment, the agent processes or refuses the check-in of the passenger, as shown in Figure 3.22.

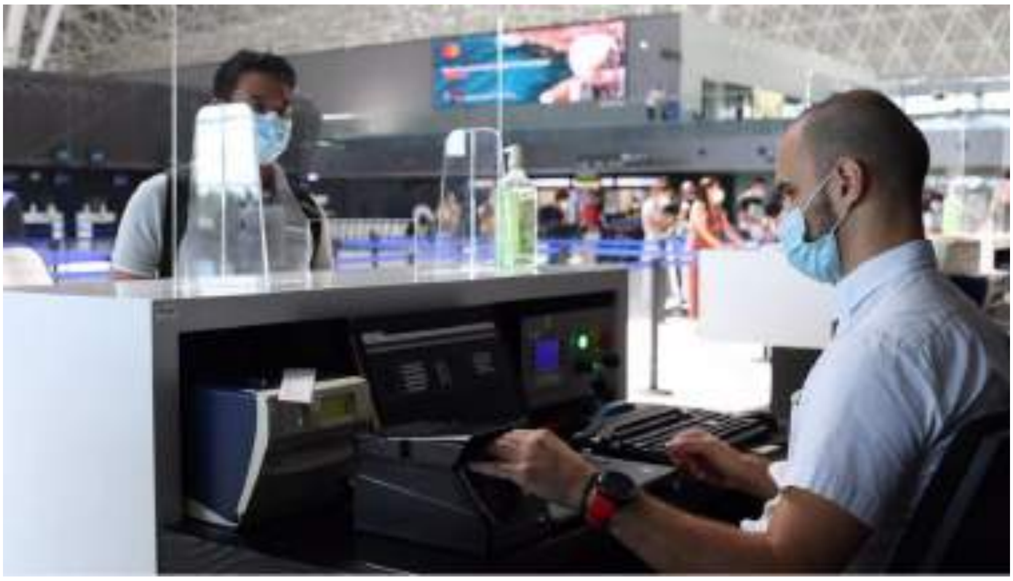


Figure 3.23: PAD usage at the check-in desk

The Luggage Anomaly Detection Tool (LAD) was introduced at the check-in desk to illustrate the luggage enrolment process as shown in Figure 3.22 and create the extended passenger record (Figure 3.24).

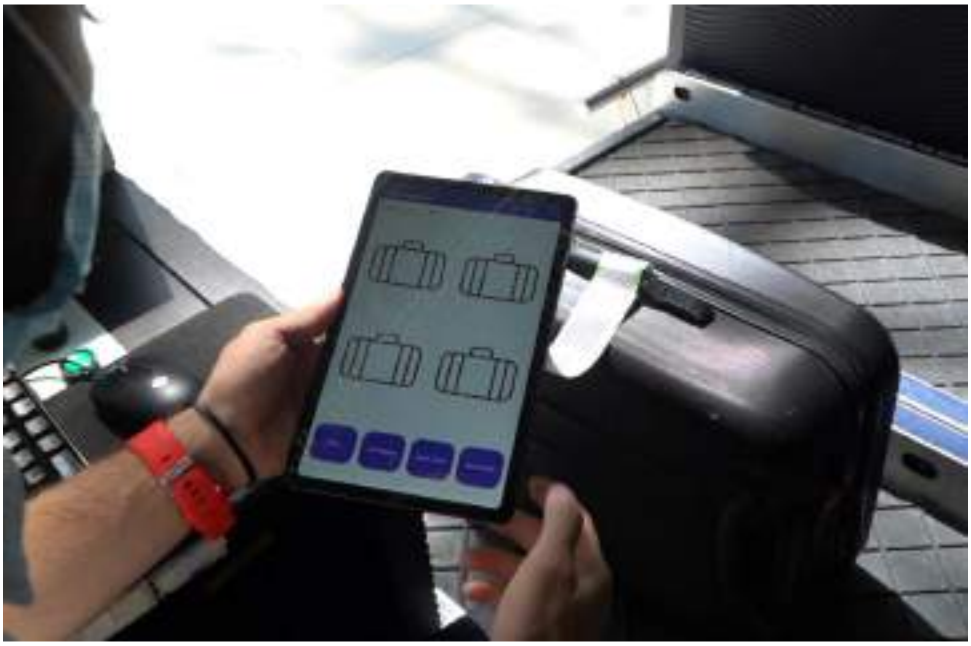


Figure 3.24: Luggage enrolment using the LAD tablet

The LAD was then used at different strategic/critical areas of the airport to illustrate the security enhancement on existing processes:

1) At the boarding gate to perform a luggage authentication check before allowing the passenger to enter into the plane, as shown in Figure 3.25.

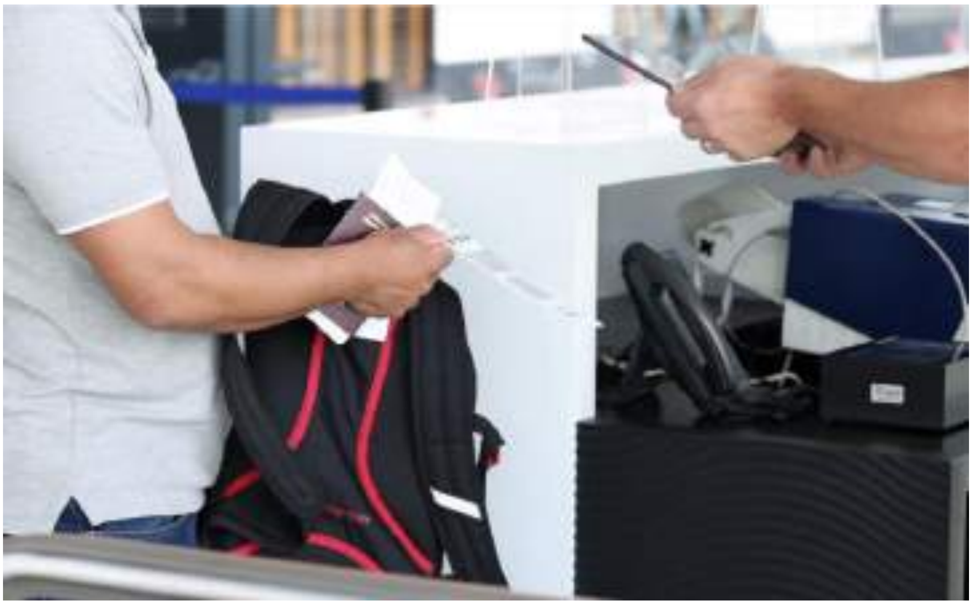


Figure 3.25: Hand Luggage check at the boarding gate using the LAD tablet

2) In the BHS, at the manual coding station, to perform a luggage authentication check, when the BHS rejects a luggage because it cannot process it due to a creased tag, as shown in Figure 3.26.

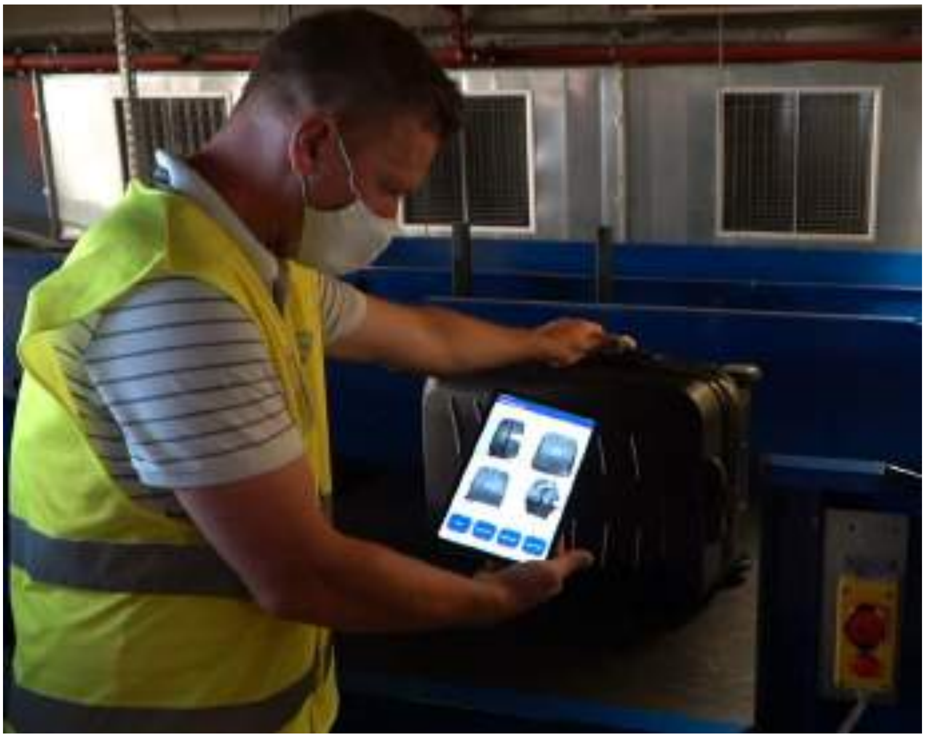


Figure 3.26: Authentication check with a creased luggage tag at manual coding station

3) In the BHS, at the manual coding station, to perform a luggage identification check, when the BHS rejects a luggage because it cannot process it due to no tag, as shown in Figure 3.27.

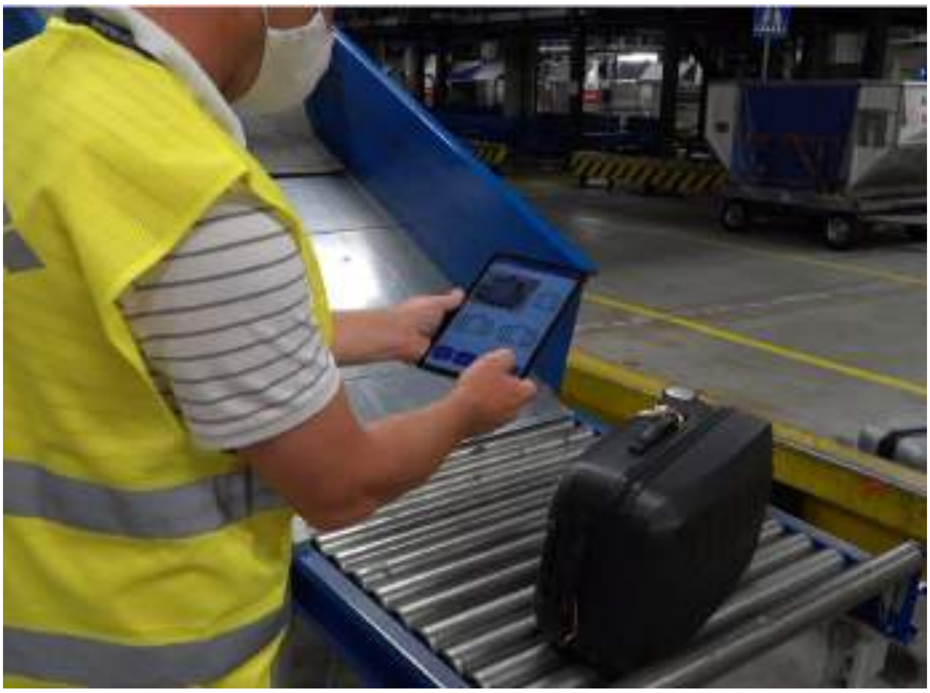


Figure 3.27: Identification check on a luggage without tag

4) In the BHS, at the carrousel, when the agent collects the luggage for a destination before being loaded into the plane, as shown inFigure 3.28.

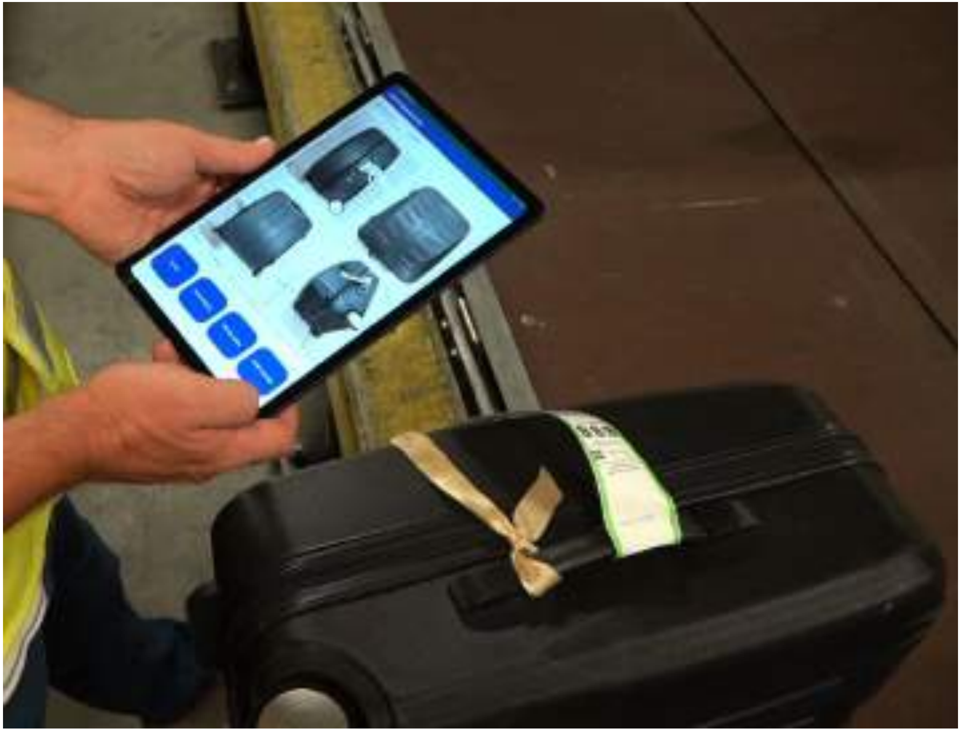


Figure 3.28: Authentication check on a luggage before loading into the plane

5) At the plane station, when the agent has to remove a luggage because the passenger is not in the plane after the boarding is closed, as shown in Figure 3.29.

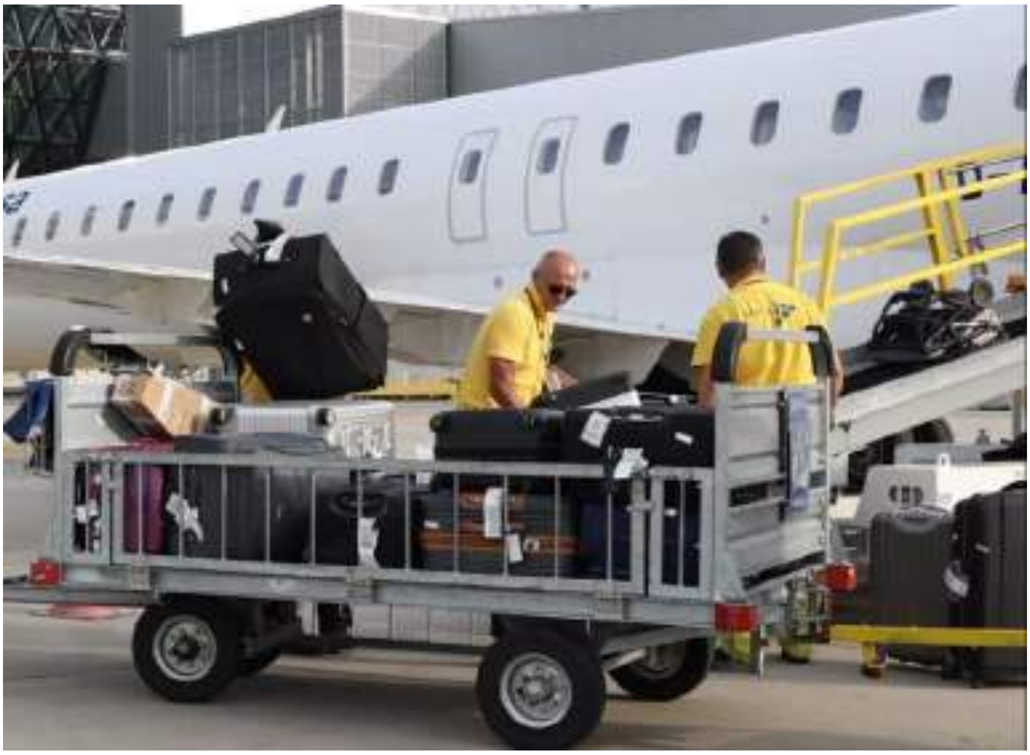
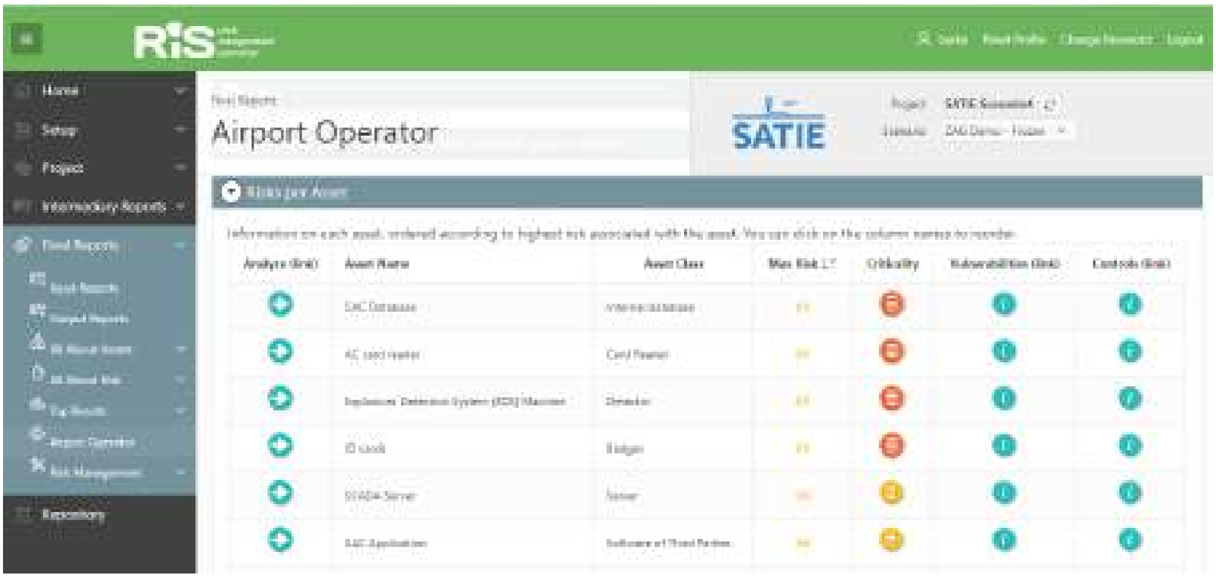


Figure 3.29: Identification check to remove a luggage at the plane station

Each time the Passenger Anomaly Detection (PAD) or the Luggage Anomaly Detection (LAD) tool is used a notification is sent to the Correlation Engine to inform the SOC agents on the activities and allow them to take the appropriates actions if required.

3.6 Risk assessment platform

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.



Final Reports

Airport Operator

Project: SATIE Scenario4
Scenario: ZAG Demo - Ticket

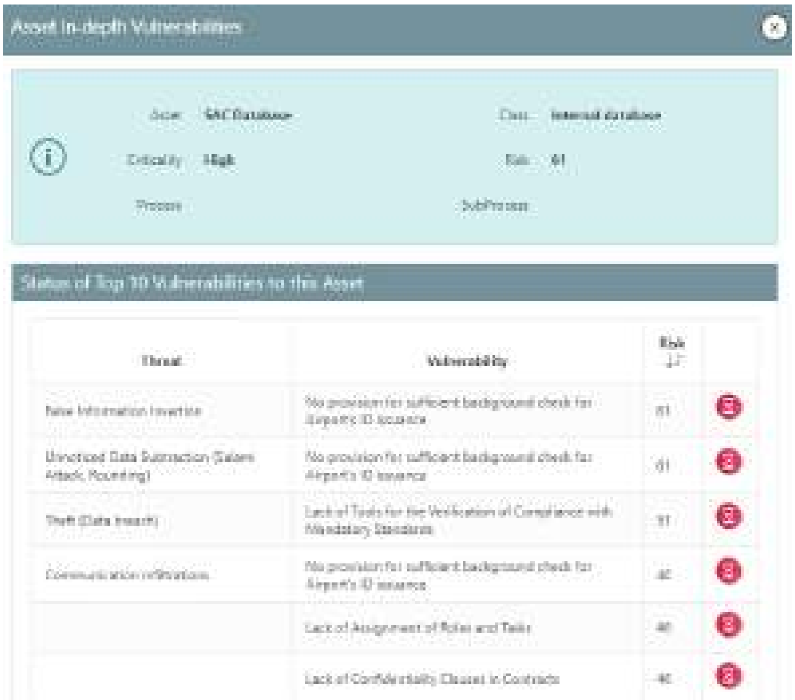
Risks per Asset

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)
●	SAC Database	Internal database	[illegible]	●	●	●
●	AC card reader	Card Reader	[illegible]	●	●	●
●	Explosive Detection System (EDS) Machine	Detector	[illegible]	●	●	●
●	ID cards	Badges	[illegible]	●	●	●
●	SCADA Server	Server	[illegible]	●	●	●
●	SAC Application	Software of Third Parties	[illegible]	●	●	●

Figure 3.30: The Airport Operator page of RIS showing the assets with the highest risks

The scenario at ZAG was broken down into multiple, smaller sub-scenarios all taking place in the BHS, but in order to demonstrate different types of attacks all taking place in the BHS. However, for the risk assessment, all assets, threats and vulnerabilities relevant within the scope of all scenarios were included together to offer a comprehensive assessment on the BHS and other pertinent airport operations. The results demonstrate that the asset with the highest risk is the SAC (Sort Allocation Computer) database (see Figure 3.30), which is the sort allocation controller of the BHS, so this is important for the bags to be sorted properly. The threats contributing to this high risk the most are shown in Figure 3.31 and include false information insertion and communication infiltration, which means attacks such as a man-in-the-middle.


Asset In-depth Vulnerabilities

Asset: SAC Database
Class: Internal database
Criticality: High
Risk: 61
Process:
SubProcess:

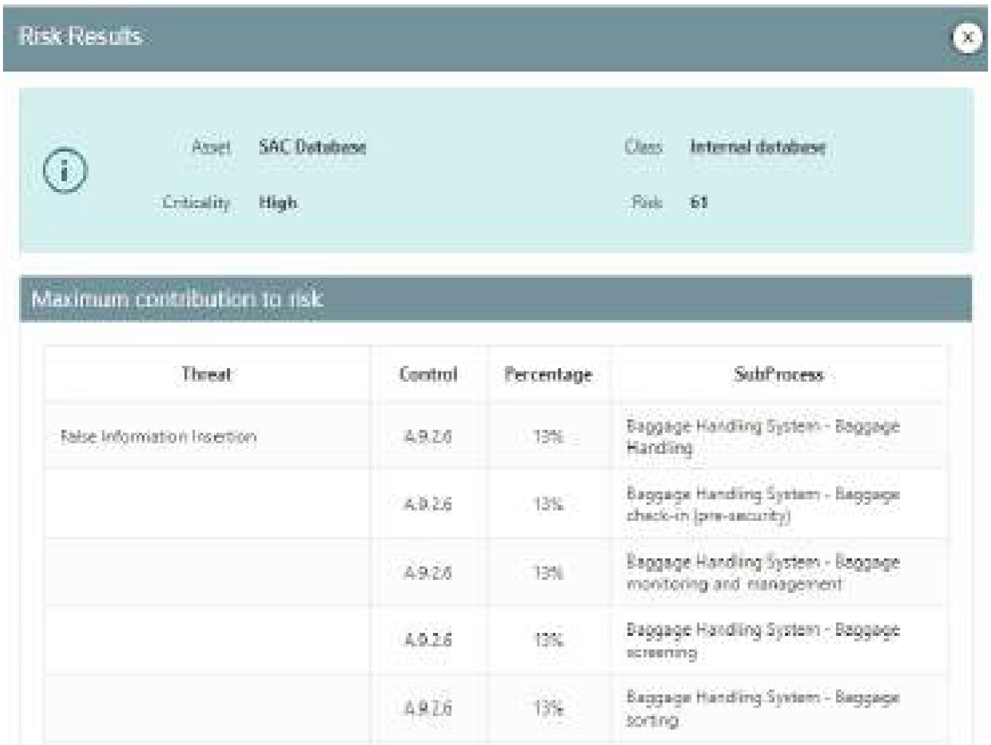
Status of Top 10 Vulnerabilities to this Asset

Threat	Vulnerability	Risk	
False Information Insertion	No provision for sufficient background check for Airport's ID issuance	61	●
Unnoticed Data Subtraction (Salami Attack, Rounding)	No provision for sufficient background check for Airport's ID issuance	61	●
Theft (Data breach)	Lack of Tools for the Verification of Compliance with Mandatory Standards	51	●
Communication infiltrations	No provision for sufficient background check for Airport's ID issuance	40	●
	Lack of Assignment of Roles and Tasks	40	●
	Lack of Confidentiality Clauses in Contracts	40	●

Figure 3.31: The threats and vulnerabilities contributing the most to the high risk of the SAC database

A risk manager seeing these results would understand that there are high risks that someone would infiltrate and feed the sorter incorrect information, which would consequently send bags to incorrect destinations and incorrect aircraft. An attack like this could have repercussions throughout the whole

BHS organization. To understand how to address these vulnerabilities, one should look at which security measures are not in place well. Regarding this same asset, the relevant security controls are shown in Figure 3.32.



Risk Results

Asset SAC Database

Class Internal database

Criticality High

Risk 61

Maximum contribution to risk

Threat	Control	Percentage	SubProcess
False Information Insertion	A.9.2.6	13%	Baggage Handling System - Baggage Handling
	A.9.2.6	13%	Baggage Handling System - Baggage check-in (pre-security)
	A.9.2.6	13%	Baggage Handling System - Baggage monitoring and management
	A.9.2.6	13%	Baggage Handling System - Baggage screening
	A.9.2.6	13%	Baggage Handling System - Baggage sorting

Figure 3.32: The weakest applied security controls that could reduce risks for this asset

Control A.9.2.6 (see Figure 3.32) is related to the ISO27002 standard and is related to access rights to systems being updated with changes of employment or roles. If someone is demoted or quits, their access rights should be adjusted accordingly in a timely manner. Overall, the highest risks of this scenario indicate that an employee – not an external attacker – has a high risk of being able to successfully insert incorrect information to the SAC database which could change bag destinations and cause chaos. This is in fact exactly what happened in one of the scenarios during the ZAG demonstration.

RIS also offers a 'What-if Scenario' to model how the risks would change if various controls were applied better so that a risk manager could see if improving a particular security control would greatly reduce risks in general or to specific, highly-critical assets. It allows the airport to best determine where to apply their time and financial efforts to reduce risks and improve their situation.

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

4 Results and Evaluation

This section presents the evaluation results of the Zagreb 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 Zagreb Airport demonstration event. They participated in the demonstration as observers and provided useful input concerning the SATIE Solution. The evaluation questionnaire form communicated to the audience is presented in the Annex 1 - Evaluation questionnaire, chapter 7.

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

- Calculate the final value for each KPI related to the Zagreb 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 Zagreb 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 Zagreb Airport demonstration and presented in Table 4.1. Moreover, the table displays the KPIs which are relevant to the Zagreb 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 Zagreb 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 four demonstration sub-scenarios of Zagreb Airport are considered.

Regarding the demonstration Scenario #4, seven cyber-attacks were committed:

- USB device with malware is connected to a workstation on check-in counter ("The Ransom")
- Malware spreads through the BHS network using the EternalBlue exploit ("The Ransom")
- Malware reaches SCADA and ransomware infected BHS is forced to shut down in order to prevent the infection ("The Ransom")
- Wi-Fi network intrusion over the bruteforce password crack ("The Wrong Hold")
- Man-In-The-Middle attack between the SAC and the PLC ("The Wrong Hold")
- Raspberry Pi is connected to a BHS network switch ("The Lost Baggage")
- BHS network is flooded and network loop is created causing a distributed denial of service of the BHS ("The Lost Baggage")

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

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

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

IE2: Vulnerability management system for ICS and OT systems (GLPI).

IE3: Encryption framework for secured IoT communications.

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.

IE14: Emulation platform for improved cyber defence strategies.

As a result, ten capabilities were demonstrated in the Zagreb Airport event, and the target was to perform nine of them.

SATIE KPI #Number of participants trained.

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

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

This KPI value was calculated according to the evaluation questionnaire responders, defined in section. Five participants from security industry were answering the questionnaires, which reached targeted three.

SATIE KPI #Number of project external demo visitors (Demo ZAG) 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, only one invitee was able to join the event physically. In addition to that, external demo visitors were 28 people who attended online.

Table 4.1: Current values of KPIs with respect to the Zagreb Demonstration event

KPI	Objective	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
Number of different attacks implemented in the	O8	N/A	7	N/A	This calculation includes only the subset of cyber and physical attacks	All attacks of the four sub-scenarios carried out

KPI	Objective	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
demonstration of the final scenarios.					demonstrated in Zagreb. The target (23) is not applicable, as it is counting all 4 scenarios demonstrated in the 3 locations (Zagreb Airport, Milan Airport, Athens Airport).	within the Zagreb Airport demonstration are counted.
Number of capabilities demonstrated (Demo ZAG)	O8	9	10	Yes	The Zagreb Demonstration event overpassed successfully the targeted value of the specific KPI with the demonstration of 10 Innovation Elements (IEs).	Counting how many SATIE Innovation Elements (IEs) were demonstrated during the Zagreb Airport event.
Number of participants trained (Demo ZAG)	O8	3	5	Yes	2 SOC operators, 2 AOC operators and 1 observer were trained for the Zagreb Airport demonstration. During the demonstration, there was no need to include AOC operators since CAS was not used in the sub-scenarios.	3 roles were trained: AOC, SOC and Observer.
Number of security practitioners/participants answering a questionnaire (Demo ZAG)	O8	3	5	Yes	The Zagreb 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	Objective	Target	Current	Fulfilled?	Comment/ Justification	Formula Calculation
Number of project external demo visitors (Demo ZAG) online/physical	O8	20 when online 15 when physical	29	Yes	Due to COVID-19 security and safety protocols and to the respective travel restrictions and limitations, there was only one physical external visitor in the Zagreb Airport demonstration event, and 28 online present externals.	Project external demo visitors were counted as individuals and not per organisation.

4.2 Evaluation questionnaire results

In this section, the participants subjective assessment of the SATIE Solution as shown during the Zagreb demonstration is presented. A subset of the questions already asked during the simulation validations (described in D6.2 (1) and D6.3 (2) was used and – if needed - adapted to the demonstration (questions addressing parts of the SATIE solution not shown during the demonstration have been omitted from the questionnaires compared to the simulation validation questionnaires). The questionnaire was the same as the one used in the Athens demonstration and described in the respective report D6.5 (4). During the event, only participants external to the project were asked to answer the questionnaires. Hence, the results presented here are only from these "independent external" participants. 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. The affiliation of participants can be seen in Table 4.6. The total number of considered questionnaire responses was N=12, which is considered as a very good value regarding the time the questionnaire was administered (around midnight). The evaluation of operators was already performed during the simulation validations and is described in D6.3 (2) and not included in this report.

Table 4.2: Results of evaluation questionnaire responders

Statement	Average	Minimum	Maximum	Standard deviation	No. of participants
The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	6.08	5	7	0.67	12
The SATIE Solution is an excellent way to monitor and raise security alerts.	6.33	5	7	0.78	12
The SATIE Solution provides all relevant information.	6.25	4	7	0.97	12

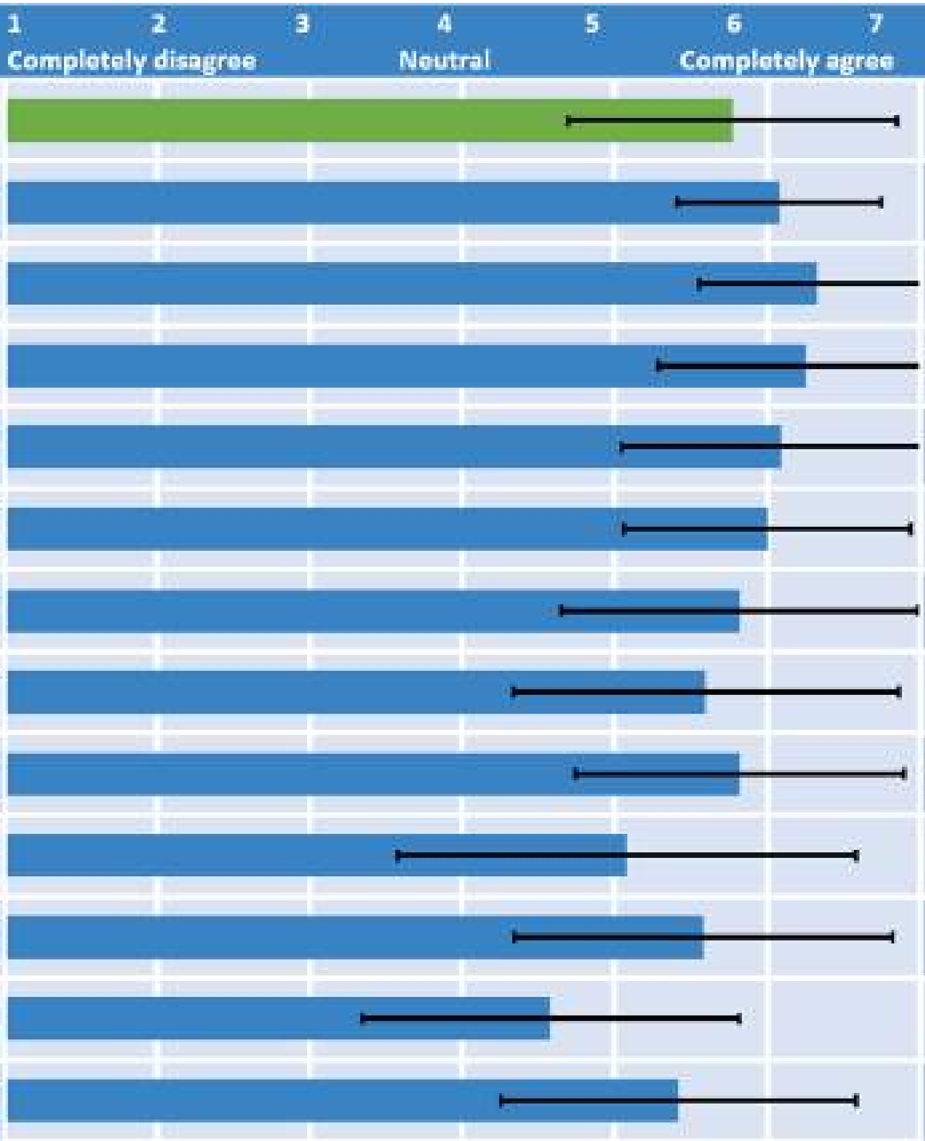
The SATIE Solution enables a faster detection of cyber threats compared to current systems.	6.09	4	7	1.04	11
The SATIE Solution enables a faster detection of physical threats compared to current systems.	6.00	4	7	0.94	10
The SATIE Solution enables a faster response to cyber threats compared to current systems.	5.82	4	7	1.17	11
The SATIE Solution enables a faster response to physical threats compared to current systems.	5.60	3	7	1.27	10
The use of the SATIE Solution increases the efficiency compared to current systems.	5.82	4	7	1.08	11
I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	5.08	2	7	1.51	12
The SATIE Solution is innovative compared to others on the market.	5.58	3	7	1.24	12
I think the SATIE Solution will boost airports' revenues.	4.58	2	6	1.24	12
I think airports will like to secure their systems with the SATIE Solution.	5.42	4	7	1.17	12
I think that the shown scenario(s) were suitable to illustrate the SATIE Solution's capabilities.	6.25	5	7	0.97	12
The SATIE Solution has good usability.	5.92	4	7	1.08	12
Summary	5.77	4	7	1.08	

As can be seen 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 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. 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 and that the SATIE Solution is innovative compared to others on the market. Slightly lower, but still agreement, could be observed for the statement regarding the ease of integrating the SATIE Solution with necessary airport systems and the statement that the SATIE solution will boost revenues for airports. The shown scenarios at Zagreb demonstration were rated as suitable to illustrate SATIE Solution´s capabilities. Concluding, the participants agreed that airports will like to secure their systems with the SATIE Solution.

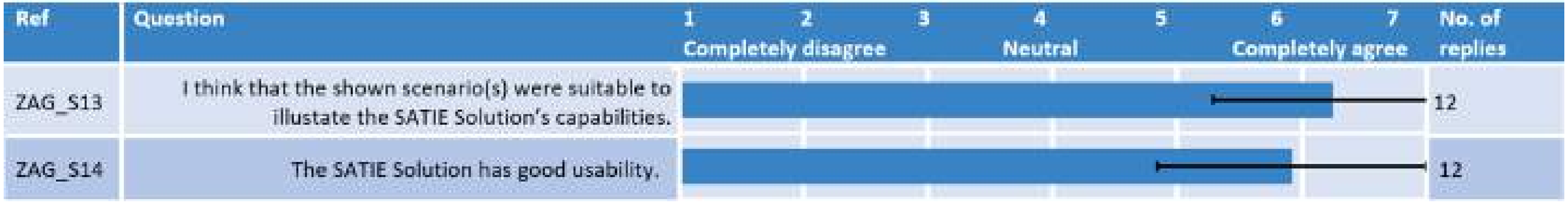
The participants had the opportunity to choose Innovation Elements which stood out for them and were offered a free text field to explain their choice (see Table 4.4). The correlation of security events from disparate systems was seen as key to understand attacks, because this greatly simplifies incident management. The ability to see the impact of an asset on the other and the graphic representation was evaluated as useful and innovative for end users, because it makes identifying services impacted by an attack very easy. Furthermore, the baggage registration service was seen as an elegant way to keep track of luggage on the BHS. The Secured Communication on the BHS (ComSEC) was rated as having a very good cost-benefit-ratio due to the plug-and-play approach. It was seen as easy to install and therefore attractive for airports. The digital twin of the baggage handling system was stated to be very impressive and the Vulnerability Intelligence Platform (VIP) was seen as very complete. Even though many SATIE Tools received promising feedback, some SATIE Tools involved in the demonstration were not so visible to the participants, and therefore they did not stand out to them and appear in Table 4.4. This is the case of the GLPI and BP-IDS, two back-end systems with their novelty not so easily noticeable to the end-users who just saw their produced alerts in the IMP. Despite of that, as could be observed in Sections 3.3 and 3.4, GLPI and BP-IDS were crucial to the demonstration. In an additional question, all participants had the opportunity to add further remarks and general feedback (see Table 4.5). Unifying the communication and the HMIs of all tools was mentioned as a suggestion for future work and it was raised the concern that the baggage identification could be a possible problem because of slowing down the baggage handling process. Besides that, the overwhelming amount of feedback was very positive. According to the participants the demonstration at Zagreb airport provided a very good vision of the SATIE Solution and its benefits for the safety and the security, the SATIE Solution was rated as a really good solution that allows detection and comprehension of new types of attacks. Furthermore, participants wrote that SATIE is going in the right direction and provides good solutions to many critical infrastructures. SATIE was seen as an impressive accomplishment in developing a practically useful, complex system under the very difficult circumstances of a pandemic and the team was thanked for the demo, which was carried out in live with a good mix of simulations and physical systems.

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

Table 4.3: Statistical results concerning the evaluation questionnaire answers



Ref	Question	No. of replies
Statements	Overall	
ZAG_S01	The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	12
ZAG_S02	The SATIE Solution is an excellent way to monitor and raise security alerts.	12
ZAG_S03	The SATIE Solution provides all relevant information.	12
ZAG_S04	The SATIE Solution enables a faster detection of cyber threats compared to current systems.	11
ZAG_S05	The SATIE Solution enables a faster detection of physical threats compared to current systems.	10
ZAG_S06	The SATIE Solution enables a faster response to cyber threats compared to current systems.	11
ZAG_S07	The SATIE Solution enables a faster response to physical threats compared to current systems.	10
ZAG_S08	The use of the SATIE Solution increases the efficiency compared to current systems.	11
ZAG_S09	I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	12
ZAG_S10	The SATIE Solution is innovative compared to others on the market.	12
ZAG_S11	I think the SATIE Solution will boost airports' revenues.	12
ZAG_S12	I think airports will like to secure their systems with the SATIE Solution.	12



Ref	Question	1	2	3	4	5	6	7	No. of replies
		Completely disagree			Neutral		Completely agree		
ZAG_S13	I think that the shown scenario(s) were suitable to illustate the SATIE Solution's capabilities.								12
ZAG_S14	The SATIE Solution has good usability.								12

Table 4.4: Innovation Elements Feedback

Question	"Which of the Innovation Elements stood out for you and why?"	
Innovation Element	**Frequency**	**Reasons**
Correlation Engine	5	Correlation of security events from disparate systems greatly simplifies incident management. Key to understand attacks
Risk Integrated Service (RIS)	4	
Vulnerability Intelligence Platform (VIP)	4	Very complete
Business Impact Assessment (BIA)	4	Very convenient to see the impact of an asset on the other. The graphic interface makes it very easy to identify services impacted by an attack. Useful and innovative for end user.
Anomaly Detection On Passenger Records (PAD)	3	Even though it sometimes seems cumbersome to use, the baggage registration service seems like an elegant way to keep track of luggage on the BHS.
CyberRange	3	Make simulations for all different type of possible attacks.
Secured Communication on the BHS (ComSEC)	2	Very good cost-benefit-ratio due to the plug-and-play approach, easy to install and therefore attractive for airports (even without rest of SATIE Solution).
Incident Management Portal (IMP)	2	
Digital Twin of the Baggage Handling System (BHS)	2	The digital twin is very impressive.

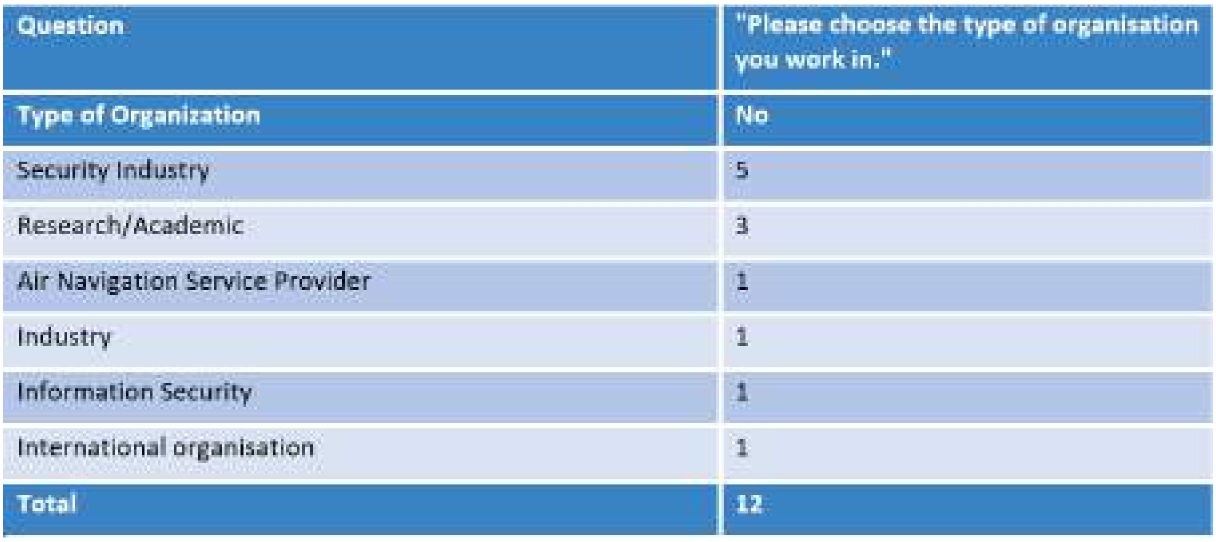
Question	**"Which of the Innovation Elements stood out for you and why?"**	
Innovation Element	**Frequency**	**Reasons**
Application Layer Cyber Attack Detection (ALCAD)	1	
Investigation Tool (SMS-I)	1	
Crisis Alerting System (CAS)	1	

Table 4.5: General feedback and suggestions

Question	**"Is there anything else you would like to mention about the SATIE Solution?"**
Type of feedback	**Feedback answers**
Positive reinforcement	No, just continue to improve system cyber security.
Positive reinforcement	Combining physical and digital attacks informations.
Positive reinforcement	The demonstration at Zagreb airport provide us a very good vision of the SATIE solution and its benefits for the safety and the security.
Improvement proposal	Needed integration with other cyber systems.
Positive reinforcement	SATIE is an impressive accomplishment in developing a practically useful, complex system under the very difficult circumstances of a pandemic.
Positive reinforcement	Thanks to all the teams for the demo, carried out in live with a good mix of simulations and physical systems.
Improvement proposal	Baggage identification could be a possible problem because of slow process.
Positive reinforcement	Very good work, congratulations for the good demos!

Question	"Is there anything else you would like to mention about the SATIE Solution?"
Type of feedback	**Feedback answers**
Positive reinforcement	SATIE solution is a really good solution that allows detection and comprehension of new types of attacks.
Improvement proposal	The GUIs used by the operators have a very non-uniform appearance. I think that a next step, after unifying the communication between different systems, could be to unify the interfaces as well. This could greatly benefit the work of the operators and the time needed to grow accustomed to the solution.
Positive reinforcement	It seems to me that SATIE is in the right direction and should provide good solutions to many critical infrastructures.

Table 4.6: Affiliation of participants



Question	"Please choose the type of organisation you work in."
Type of Organization	**No**
Security Industry	5
Research/Academic	3
Air Navigation Service Provider	1
Industry	1
Information Security	1
International organisation	1
Total	**12**

5 Conclusion

The current deliverable is the result of Task 6.3 which was aimed at successful demonstration in operational conditions of the BHS at Zagreb Airport. The purpose of the demo was to show that the SATIE Solution is capable of recognizing the threats and detecting the problems, as well as enabling subsequent forensics, range of impact and risk analysis of incidents that have occurred.

The SATIE Toolkit was created as a result of close collaboration of all partners involved in the project, for which the demonstration confirmed that it meets cyber and physical security requirements and needs. SATIE is directed at both existing gaps reduction and specific airport service improvement. Airports have developed a need to protect people and business processes against cyber threats that can easily turn into physical ones. In order for such request to be accomplished, regular monitoring of developed interaction systems and usage of belonging supporting systems proved sufficient during the demo.

This report presents the main objective of the demonstration at Zagreb Airport with physical and cyber infrastructure deployed, a detailed description of all four demonstration sub-scenarios, response of the SATIE Tools and evaluation results analysis. All sub-scenarios, whether shown live or over video, had a similarity in that they were oriented towards baggage handling. Since this process is very sensitive and of great importance to the airport, it was decided that the demonstration would take place at night not to disrupt the normal traffic flow. Another reason for such a late event is of technical nature because it was not possible to have PLCs connected on both BAGWARE servers at the same time. Therefore, although it may not be customary to show it in the concluding chapter, below on the Figure 5.1 is Zagreb Airport passenger terminal building at night when the demo took place.

Figure 5.1: Passenger terminal building at night after the demonstration

In short, several possibilities of the SATIE Toolkit were presented through four described sub-scenarios. "The Extended Passenger Concept" served to recognize unauthorized baggage manipulation by taking photos of the bag and its pairing with unique baggage tag number. It has also proven useful when looking for a particular bag among bunch of others according to the look of the bag and known baggage tag number. "The Ransom" represented an attack on the BAGWARE Sort Allocation Computer which was hacked and put out of service. At first glance it may seem that SATIE has not found its use since the attack was carried out to the end, but in reality, the attack would not take place in those few minutes as shown during the demo. It was important to show that SATIE's threat prevention and detection systems immediately recognized the threat leaving enough time for the SOC operator to take further steps. Last two sub-scenarios ("The Wrong Hold" and "The Lost Baggage") showed two attacks triggered through the Raspberry Pi connected to the BHS switch and through the denial of WiFi service, which resulted with bags finishing on the wrong place in the BHS area. Those bags would not be loaded on the plane and would be reported as lost by the passengers, which was the reason why the last sub-scenario was called so.

Already after midnight, participants were kindly asked for their assessment of the SATIE Solution shown at the demonstration. The questionnaires resulted in very useful, mainly similar feedback, including positive reinforcement and encouragement. SATIE was rated as an excellent way to monitor and raise security alerts with a good usability while enabling faster threat detection. The sub-scenarios demonstrated at Zagreb Airport were evaluated as suitable to show possibilities of the SATIE Solution, where its ease of integration with the existing airport systems may present difficulties.

Successful demonstration would not have been achieved without the engagement of all SATIE partners and respectable guests, for which sincere gratitude was expressed. Some of them can be found on the Figure 5.2, at least those who could visit Zagreb while the others gave their great share remotely due to the COVID-19 measures and travel restrictions. Ultimately, this demonstration reaffirmed our hope for creating successful solution that could find its purpose and wide usage in the future.

Figure 5.2: SATIE project partners' representatives in BHS area at Zagreb Airport

6 References

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

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

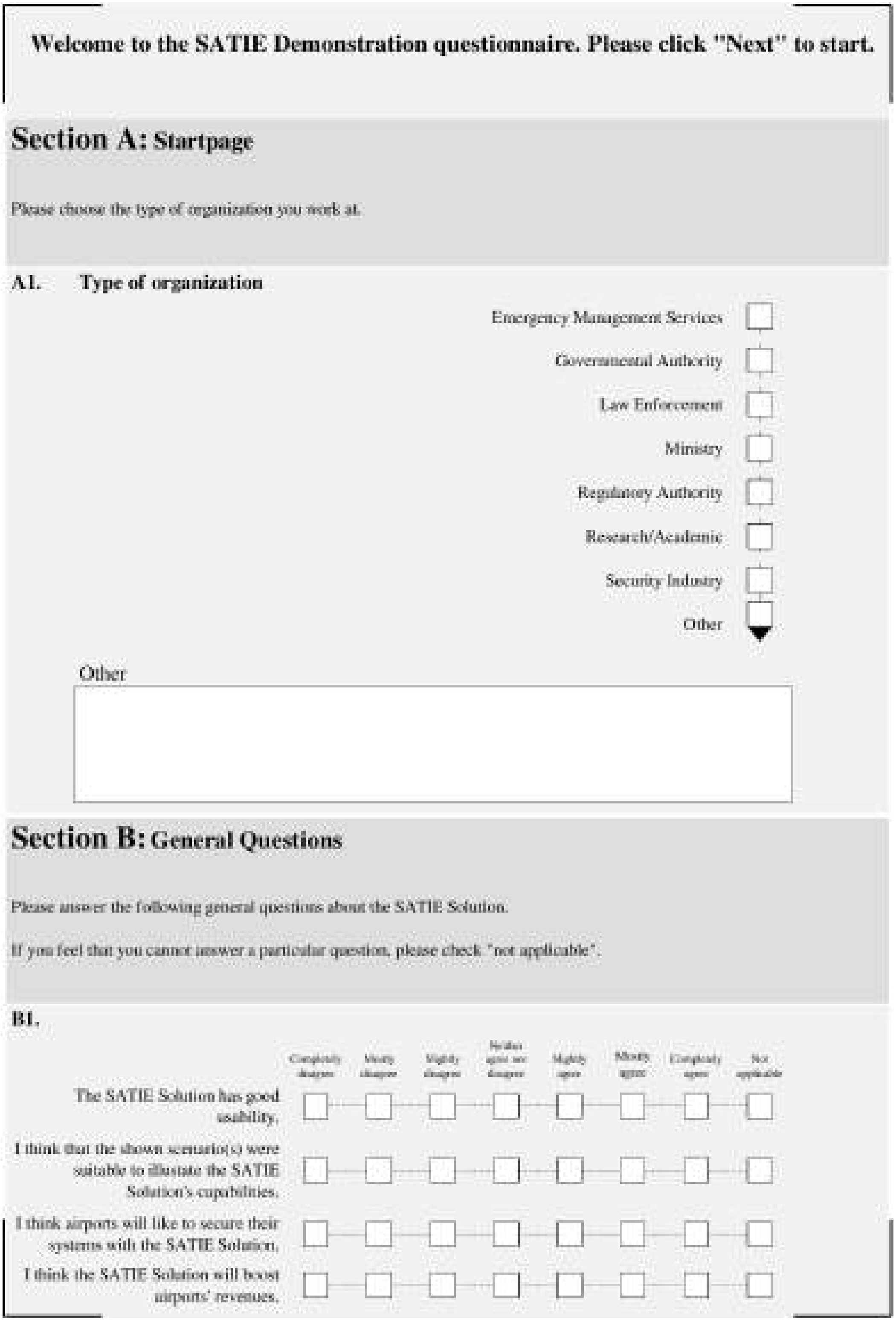
3. —. *D2.3 - Cyber-physical risk analysis.* 2020.

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

5. —. *D3.2 - Secured IoT communications on the baggage handling system.* 2020.

6. —. *D4.4 - Intrusion Detection System on Business Processes.* 2020.

7 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

□

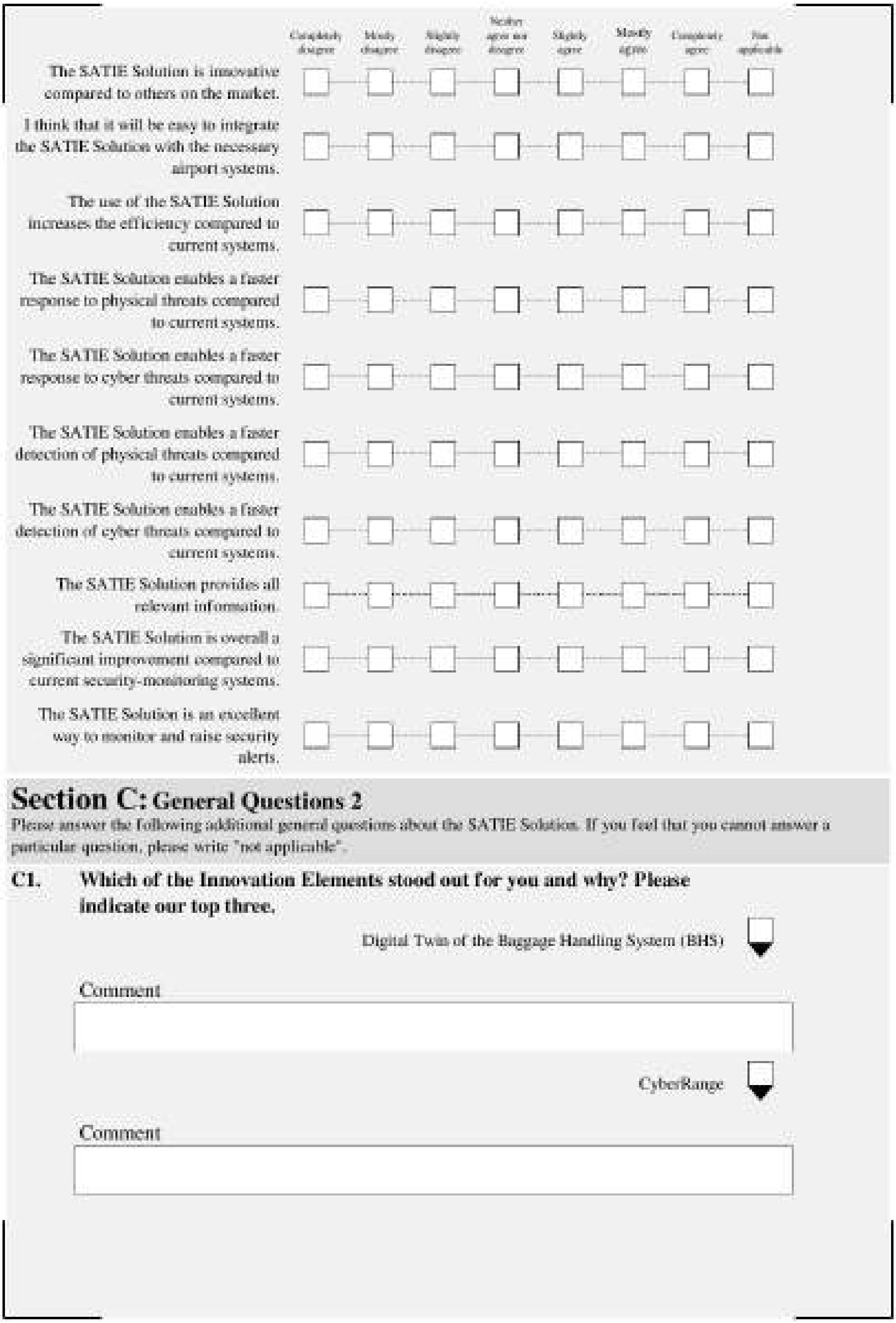
Section B: General Questions

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 illustate 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".

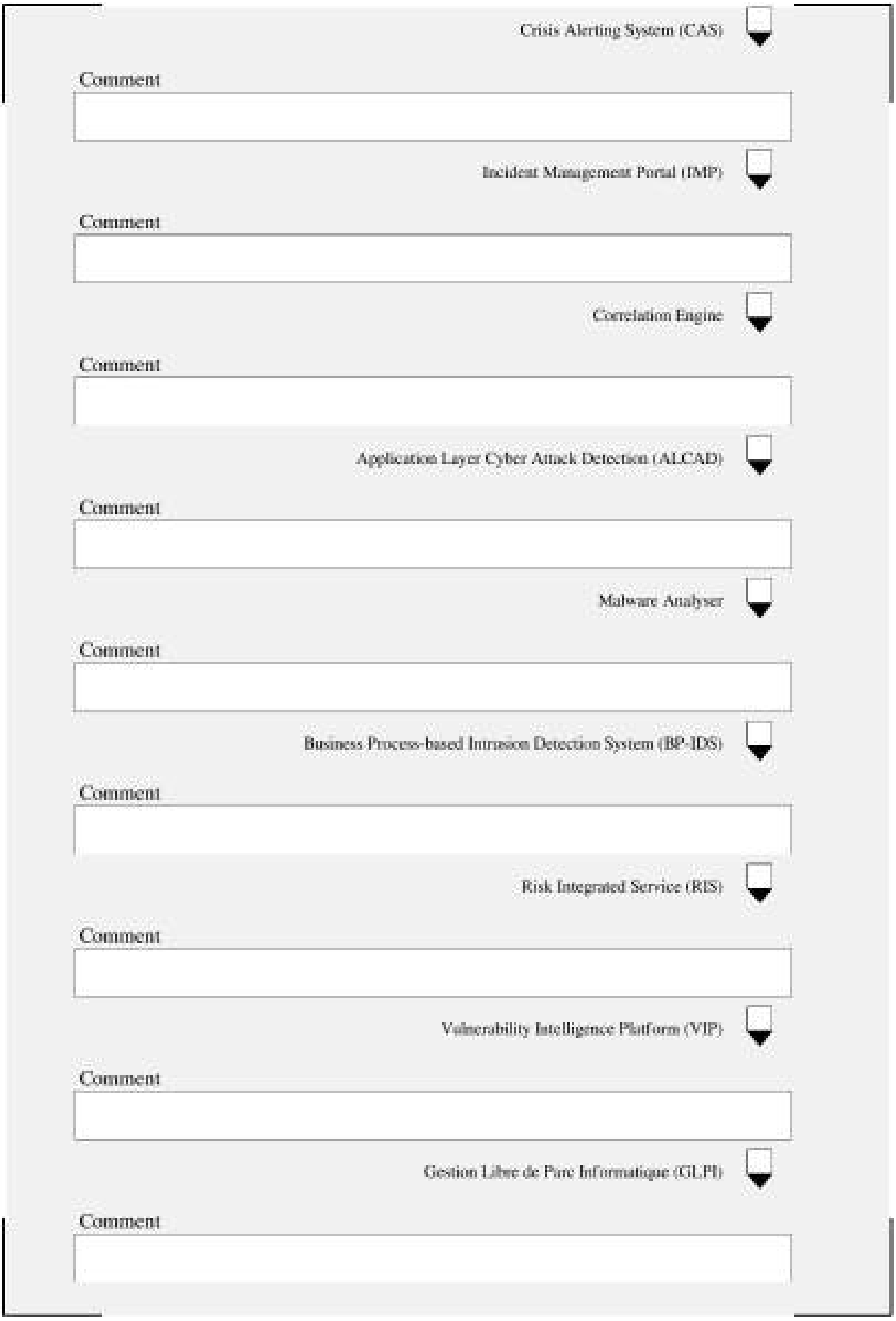
C1. Which of the Innovation Elements stood out for you and why? Please indicate our top three.

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) ▼

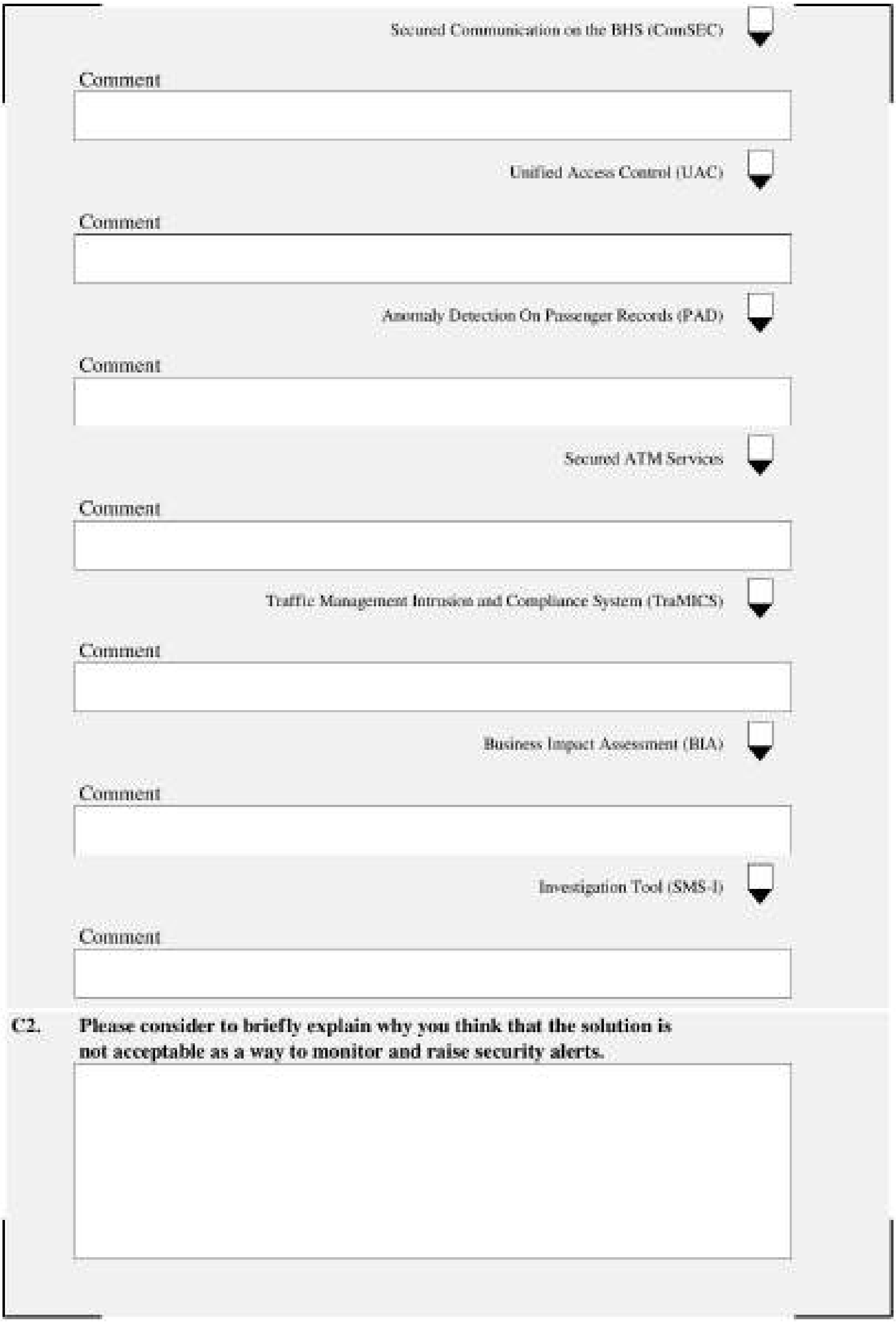
Comment

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

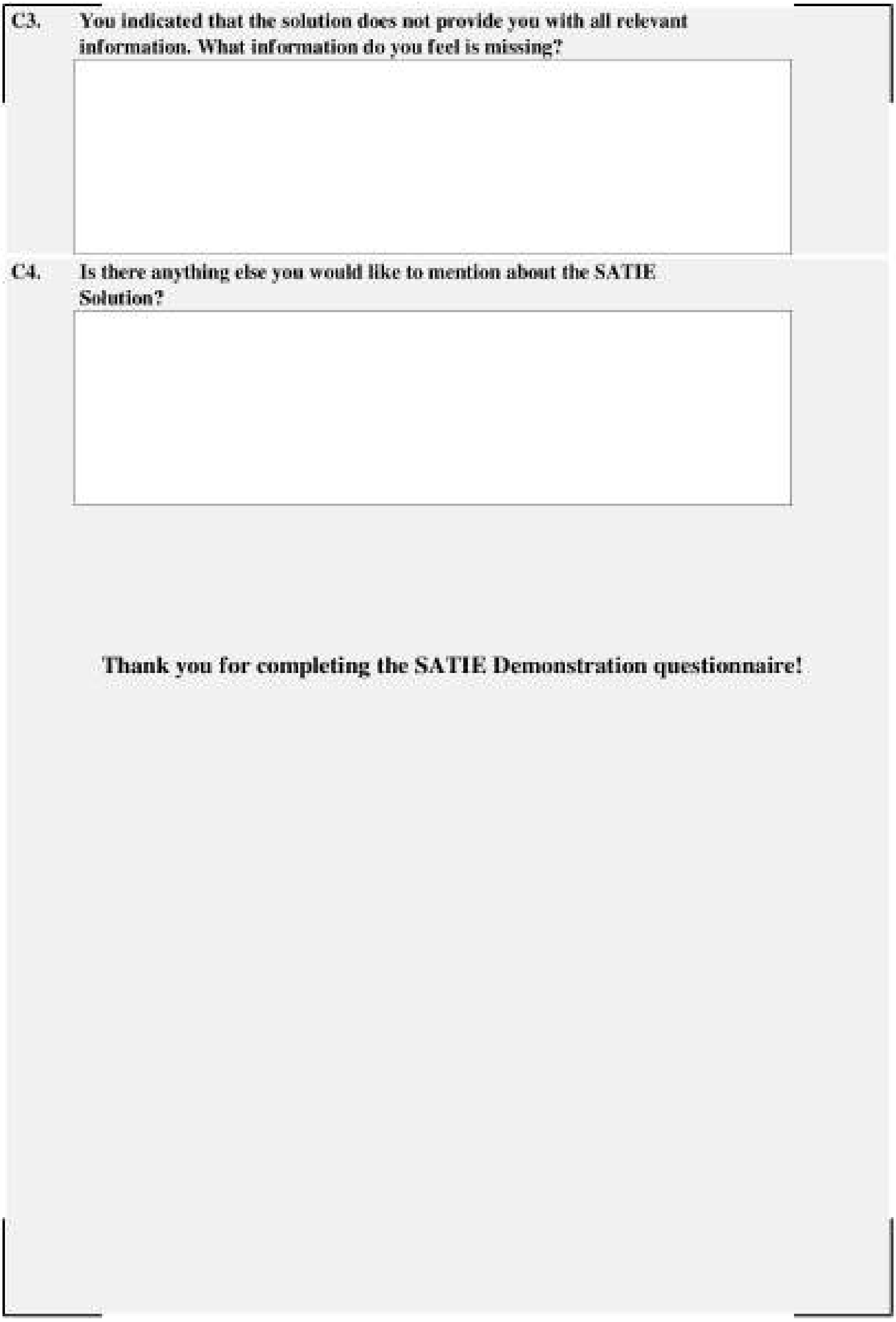
Business Impact Assessment (BIA) ▼

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!