SATIE

Security of Air Transport Infrastructures of Europe

D6.3 – Test and validation results on the simulation platform

Deliverable Number	D6.3
Author(s)	All Partners
Due/delivered Date	M26/2021-07-09
Reviewed by	ACS, DLR, KEMEA
Dissemination Level	PU
Version of template	1.08

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	Matteo Mangini (NIS)	Content Contributor
2	Kelly Burke (NIS)	Content Contributor
3	Gabriele Guasco (NIS)	Content Contributor
4	Nikos Papagiannopoulos (AIA)	Content Contributor
5	Vasilis Kontothanasis (AIA)	Content Contributor
6	Eric Hervé (ALS)	Content Contributor
7	Paul Ingrandt (ALS)	Content Contributor
8	David Lancelin (ACS)	Reviewer
9	Thomas Oudin (ACS)	Content Contributor
10	Tim Stelkens-Kobsch (DLR)	Content Contributor
11	Meilin Schaper (DLR)	Content Contributor, Reviewer
12	Nils Carstengerdes (DLR)	Content Contributor
13	Lisa Oehmigen (DLR)	Content Contributor
14	Fabian Reuschling (DLR)	Content Contributor
15	Johanna Maria Löhr (DLR)	Content Contributor
16	Nour Salih (ERI)	Content Contributor
17	Mirjam Fehling-Kaschek (FHG)	Content Contributor
18	Corinna Köpke (FHG)	Content Contributor
19	Georg Trausmuth (FQS)	Content Contributor
20	Hubert Künig (FQS)	Content Contributor
21	Luc Sonke (IDE)	Content Contributor

No.	Name	Role (content contributor / reviewer / other)
22	Sebastien Clavert (IDE)	Content Contributor
23	Thomas Mauger (IDE)	Content Contributor
24	Nelson Escravana (INOV)	Content Contributor
25	Filipe Apolinário (INOV)	Content Contributor
26	João Guiomar (INOV)	Content Contributor
27	Isabel Praça (ISEP)	Content Contributor
28	Eva Maia (ISEP)	Content Contributor
29	Alda Canito (ISEP)	Content Contributor
30	Iñes Castro de Macedo (ISEP)	Content Contributor
31	Marcin Przybyszewski (ITTI)	Content Contributor
32	Ioannis Chasiotis (KEM)	Content Contributor
33	Eftichia Georgiou (KEM)	Content Contributor
34	Antonis Kostardis (SAT)	Content Contributor
35	Leonidas Perlepes (SAT)	Content Contributor
36	Aggelos Aggelis (SAT)	Content Contributor
37	Robert Sabo (SAV)	Content Contributor
38	Milan Rusko (SAV)	Content Contributor
39	Marian Trnka (SAV)	Content Contributor
40	Elena Branchini (SEA)	Content Contributor
41	Massimo Corradi (SEA)	Content Contributor
42	Francois Déchelle (TLB)	Content Contributor
43	Maja Despot (ZAG)	Content Contributor
44	Marin Tica (ZAG)	Content Contributor
45	Marko Licina (ZAG)	Content Contributor
46	Sven Hrastnik (ZAG)	Content Contributor
47	Thibault Maurel (ACS)	Content Contributor
48	Francois Lainet (ACS)	Content Contributor
49	Vasileios Kazoukas (KEM)	Security Review
50	Nuno Oliveira (ISEP)	Content Contributor
51	Faustin Courant (ALS)	Content Contributor

Document revisions

Revision	Date	Comment	Author
V0.1	2020-04-08	Initial draft	Lisa Oehmigen
V0.1b	2020-10-26	Alternative ToC	Fabian Reuschling
V0.2	2020-11-18	Tables for test results added	Kelly Burke
V0.3	2020-12-14	Scenario descriptions updated	Fabian Reuschling
V0.4	2020-12-23	ALCAD test results added	Marcin Przybyszewski
V0.5	2021-01-11	BP-IDS, ComSEC, and BIA test results added	Filipe Apolinário
V0.6	2021-01-12	BHS results added	Faustin Courant
V0.7	2021-02-09	KPI section reworked	Johanna Maria Löhr
V0.9	2021-02-29	BP-IDS, ComSEC, and BIA quantitative evaluation	Filipe Apolinário, João Guiomar
V0.9	2021-05-07	Results of validation questionnaire added CyberRange, Malware Analyser, IMP and SSO test results added	Fabian Reuschling Thomas Oudin
V0.10	2021-05-08 2021-06-30	Partner contributions added	Fabian Reuschling, all partners
V0.11	2021-06-29	Review and comments	Meilin Schaper
V0.12	2021-07-02	Review comments addressed	Nils Carstengerdes
V0.12	2021-07-08	Final technical check and approval for submission	David Lancelin, Technical Manager
V0.12	2021-07-09	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V1.0	2021-07-09	Final quality check and approval for submission	Meilin Schaper, Quality Manager

Executive summary

Following up on the test and verification plan and the validation plan described in deliverable D6.2 (1), this deliverable reports on the results of the individual SATIE Tools' tests and those gathered during the simulations, the first step of the validation of the SATIE Solution. The results are then discussed with regards to how well the SATIE Objectives are fulfilled, the assessment of the individual tools, and possible implications for the second step of the validation, the demonstrations at the Athens, Milan, and Zagreb airports.

Firstly, in this deliverable, the deviations from the planning laid out in deliverable D6.2 (1) are reported in chapter 2. These modifications became necessary due to slight changes in how the SATIE Tools handle and interact with the overall toolkit. Furthermore, the detailed planning of the simulation validations required the adaption of the validation plan to a fully virtual event.

In chapter 3, an overview of the five threat scenarios used for the simulation validations is presented. The summary presented herein is a shortened version of the detailed scenario steps included in D6.2 (1). For confidentiality reasons, the complete steps and any modifications that were made to the scenarios after the delivery of D6.2 are not be included in this deliverable.

The results of the technical test performed before the simulation validations as well as any deviations from the test cases defined in D6.2 (1) are reported in chapter 4. For space reasons, the detailed results of the test were moved to chapter 11 (Annex 2).

During the simulation validation, the participants subjective evaluation of the SATIE Solution as well as objective data on the performance of the solution were collected and are reported in chapter 5. The subjective evaluation was recorded through a three-level questionnaire consisting of three standard questionnaires, tailor-made general questions on the entire SATIE Solution, and tailor-made bespoke questions on the individual SATIE Tools. The objective data is presented in the form of Key Performance Indicators (KPIs) that were calculated based on logs recorded during the simulation validation and in post-validation experiments. The approaches taken for each tool is described in detail.

In chapter 6, the collected results are discussed with respect to how well SATIE's objectives are fulfilled and the quality of the individual SATIE Tools. The aim of this chapter is to determine whether the SATIE Solution is fit for purpose and to identify potential areas for improvements.

Based on this discussion, implications for the demonstrations are then deduced in chapter 7. As the second step of the SATIE Solution's validation, the demonstrations provide the opportunity to directly address issues identified during the simulation validations (the first step of the validation). During the demonstrations, external stakeholders will then evaluate the (improved) SATIE Solution. The respective results will be reported in deliverables D6.4 (Zagreb demonstration), D6.5 (Athens demonstration), and D6.6 (Milan demonstration).

Table of Content

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
ABC	Automated Border Control
ABM	Agent-based Model
ABPC	Automated Boarding Pass Control
AC	Access Control
ADPR	Anomaly Detection on Passenger Records
AIM-l	long version of the SHAPE Questionnaire for Assessing Mental Workload in Automation
ALCAD	Application Layer Cyber Attack Detection
AOC	Airport Operation Centre
AOCC	Airport Operation Control Centre
AODB	Airport Operation Database
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATR	Automatic Tag Reader
BHS	Baggage Handling System
BIA	Business Impact Assessment
BP-IDS	Business Process-based Intrusion Detection System
BSM	Baggage Source Message
CAS	Crisis Alerting System
CCTV	Closed-Circuit Television
CI	Critical Infrastructure
ComSEC	Secured Communication on the BHS
DoA	Description of Action
DPO	Data Protection Officer
EDS	Explosives Detection System
FAR	False Acceptance Rate
FIDS	Flight Information Display System
FIMS	Flight Information Management System

Acronym	Definition
FNIR	False Negative Identification Rate
FPIR	False Positive Identification Rate
FPR	False Positive Rate
GDPR	General Data Protection Regulation
GLPI	Gestion Libre de Parc Informatique
GUI	Graphical User Interface
HMI	Human Machine Interface
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICS	Inductrial Control System
IMP	Incident Management Portal
IoT	Internet of Things
IPS	Impact Propagation Simulation
IT	Information Technology
M-AIS	Milan Airports Information Systems
ML	Machine Learning
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NOTAM	Notice To Airmen
OT	Operational Technology
PA	Public Announcement
PLC	Programmable Logic Controller
Q	Queues
REST API	REpresentational State Transfer Application Programming Interface
RIS	Risk Integrated Service
RMS	Resource Management System
SAC	Sort Allocation Computer System
SATI	SHAPE Automation Trust Index
SCADA	Supervisory Control And Data Acquisition
SD	standard deviation
SHAPE	Solutions for Human Automation Partnerships in European ATM

Acronym	Definition
SLTD	Stolen and Lost Travel Documents
SMS-I	Investigation Tool
SOC	Security Operation Centre
SR	Spawn Rates
SSO	Single Sign-On
SUS	System Usability Scale
TDAWN	Travel Documents Associated with Notices
TraMICS	Traffic Management Intrusion and Compliance System
UAC	Unified Access Control
UDP	User Datagram Protocol
VIP	Vulnerability Intelligence Platform
VM	Virtual Machine

1 Introduction

The general aim of the SATIE project is to develop a holistic toolkit to improve the detection and mitigation of physical threats and cyber threats as well as to combat combined cyber-physical threats through correlation of the alerts raised. The structure of the SATIE Toolkit is presented in Figure 1.1. It consists of two central interaction systems, the Incident Management Portal (IMP) designed for the Security Operation Centre (SOC) operators and the Crisis Alerting System (CAS) used by the Airport Operation Centre (AOC) operators. The work of the operators is aided by nine supporting systems. These are the Investigation Tool (SMS-I) that supports in the decision making, the Impact Propagation Simulation (IPS) and Business Impact Assessment (BIA) as Impact Propagation Tools, the Risk Integrated Service (RIS) used for a a-priori risk assessment, the Correlation Engine as central tool for the correlation of cyber threats and physical threats, and the Vulnerability Management System (VuMS), consisting of the Vulnerability Intelligence Platform (VIP) and the Gestion Libre de Parc Informatique (GLPI), that keeps an inventory of all connected assets and associated know vulnerabilities.

The Correlation Engine is fed by the Unified Access Control (UAC), the Anomaly Detection on Passenger Records (ADPR), and the Traffic Management Intrusion and Compliance System (TraMICS) as physical threat prevention and detection systems and the Malware Analyser, the Application Layer Cyber Attack Detection (ALCAD), the Secured Communication on the BHS (ComSEC), the Business Process-based Intrusion Detection System (BP-IDS), and the Secured ATM Services (ATM = Air Traffic Management) as cyber threat prevention and detection systems. The threat prevention and detection systems secure and pull data from several airport and ATC (Air Traffic Control) systems. These are: The Closed-Circuit Television (CCTV) system, the Access Control system, the Automated Boarding Pass Control (ABPC) system, the Automated Border Control (ABC) system, the baggage registration, the Baggage Handling System (BHS) (or the Digital Twin for the simulation validation), the Public Announcement system, the Airport Operation Database (AODB) and Flight Information Display System (FIDS), the Resource Management System (RMS), the flight plan communication and the controller working position.

This entire SATIE Solution is embedded into the validation environments. For the first validation step, the simulation validations, the solution and the airport and ATC systems are fully virtualized on the CyberRange. For the second validation step, the demonstrations at the airport sites, the SATIE Solution implemented on the CyberRange is connected with the actual airport systems (as far as that is possible).

Throughout this document, the following terms are used to refer to the different systems relevant to the SATIE project:

SATIE Tool: The singular parts that comprise an Innovation Element (IE). As an example, the IE #11 “Impact Propagation Tools” is comprised of the SATIE Tools “Business Impact Assessment” and “Impact Propagation Simulation”.

SATIE Airport Environment: The airport and ATC systems SATIE’s threat prevention and detection systems receive information from.

SATIE Solution: All IEs developed in SATIE, except the CyberRange.

SATIE Concept: The combination of the SATIE Airport Environment and the SATIE Solution.

SATIE Toolkit: All IEs developed in SATIE, including the CyberRange.

SATIE Environment: The combination of the SATIE Airport Environment and the SATIE Toolkit.

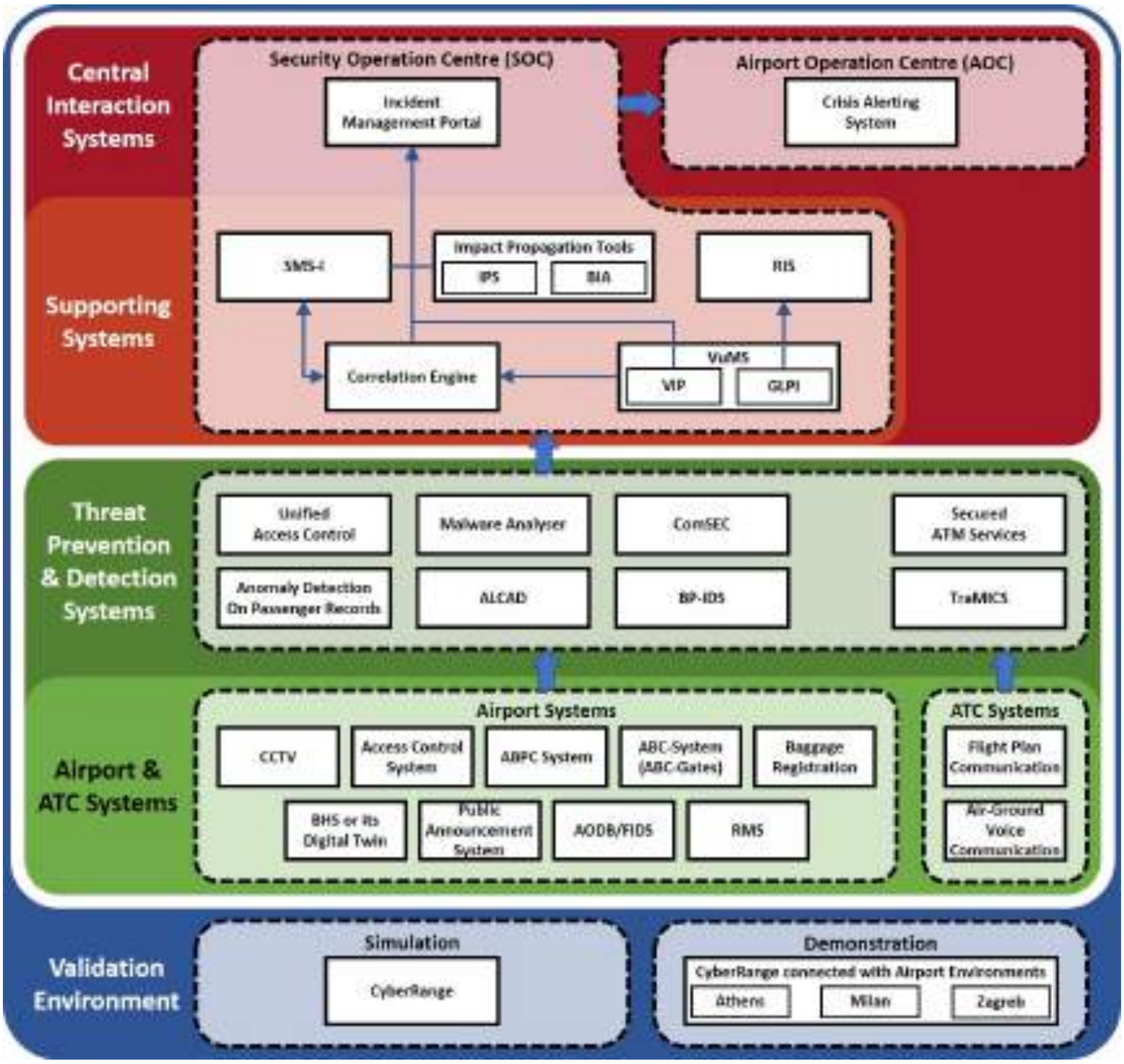


Figure 1.1: Overview of the SATIE Environment

2 Deviations

During the continuous preparation of the validation activities, the test and verification plan and the validation plan originally described in deliverable D6.2 (1) had to be slightly altered to account for changes in the details of the SATIE Toolkit and the validation scenarios. The specific changes required are described in the following.

2.1 Deviations from test and verification plan

The test and verification plan was generally carried out as described in D6.2 (1). However, the test cases of some SATIE Tools had to be aligned with the tools' development up until the simulation validations. The affected tools are the Anomaly Detection on Passenger Records, the Gestion Libre de Parc Informatique, the Risk Integrated Service, the Impact Propagation Simulation, and the Crisis Alerting System. The specific deviations are described in the respective sections of chapter 4.

2.2 Deviations from validation plan

Compared to D6.2 (1), the validation plan had to be adapted in multiple areas. The first deviation is that, due to updates to Scenario #2, an Automated Border Control (ABC) officer working position and a manual creation of alerts is no longer necessary. Hence, the requirements Sc2_3 (ABC officer working position) and Sc2_4 (Manual input of alerts) presented in Table 4.9 of D6.2 (1) are no longer valid.

The most notable change not reflected in the previous plan, however, is the transfer of the entire validation activities to a fully virtual event given the ongoing travel restrictions and mandatory social distancing measures. The access to the SATIE Tools' Graphical User Interfaces (GUIs) was provided remotely via the web portal of the CyberRange simulation environment identically to how the participants' training was conducted (see deliverable D7.2 (2)). During the validation activities themselves, the SOC operators and AOC operators were placed in two separate video conferencing rooms analogous to a typical set-up at an airport site. In each room, the screen of the currently interacting operator was shared enabling the observers to have a complete overview of the actions in the SOC and the AOC. The move to a fully virtual event also made it possible to have all scenarios performed by all airport teams and by both SOC operators and AOC operators, in contrast to the AOC operators being only involved in Scenario #1 and Scenario #2 as originally planned in D6.2 (1). Consequently, Table 4.7 of D6.2 was updated as shown in Table 2.1 below.

Table 2.1: Updated table of validations performed by each airport's participants; changes compared to the validation plan are marked in bold

	Scenario #1 (Athens)	Scenario #2 (Athens)	Scenario #3 (Milan)	Scenario #4 (Zagreb)	Scenario #5 (-)
Athens' participants	Base	Base	**Additional**	Additional	Additional
Milan's participants	Additional	Additional	Base	Additional	Additional
Zagreb's participants	Additional	Additional	**Additional**	Base	Additional

The simulation validations for the Zagreb and Athens airport teams were carried out within one workday. For better availability of the validation participants, the validations for the Milan airport team were distributed over two days. The respective schedules can be found in Annex 1 (chapter 10). Furthermore, the consent form and Non-Disclosure Agreement (NDA) signed by the participants in advance of the simulation validations is also included in Annex 1.

The simulation validation questionnaire remained unaffected by the previously described deviations. The only change to the questionnaire is the removal of one statement on the Traffic Management Intrusion and Compliance System (TraMICS) and the slight alteration of two further statements described in section 5.1.3.8. These were necessary due to changes in the handling of the TraMICS in the SATIE Toolkit.

3 Scenarios

In this chapter, an overview of the five developed validation scenarios is presented. Due to security concerns, only broad summaries of the scenarios are included herein. The detailed descriptions of the scenarios and the individual steps are available in deliverable D6.2 (1).

3.1 Scenario #1

Scenario #1 takes place at the Athens Airport and specifically involves attacking the Flight Information Display System (FIDS), Access Control (AC), and Public Announcement (PA) systems.

Summary: This threat scenario involves two unsuspecting cyber-attacks to gain enough information to be able to stage a sure-fire physical attack and control the movement of people, allowing for even more physical attacks. The mitigation of the two cyber-attacks also occupies the airport's security response teams increasing the probability that the subsequent physical attacks become a devastating success.

Reflection: This scenario comes down to one final catastrophic attack but requires coordinating people's movements and - in order to access the PA system, which is not connected to any outside network - it requires physical access to it. Therefore, the attacker causes both confusion in people's movements through the misinformation of FIDS, and is able to grant himself physical access. Ultimately, it requires coordination of both cyber- and physical attacks but results not only in airport operations coming to a standstill, but also potentially atrocious physical damage to people and to the airport.

3.2 Scenario #2

Scenario #2 also takes place at Athens Airport, but involves the PA system along with the passport and border police control and passenger control operations.

Summary: Malicious airport personnel has become an increasing threat at airports. This threat scenario is performed by a duo of attackers and includes a corrupt employee exploiting their privileges, which allows for a cascade of threats and events, disabling the airport's resources to counteract the threats and eventually potentially resulting in a serious terrorist attack on EU soil by person(s) who should not even be allowed to cross borders.

Reflection: Starting with a simple action from a malicious employee, an attacker who has already made contacts with a terrorist group in the country, is able to perform a terrorist attack in the country, and at the same time creates chaos at the airport making it even more difficult to, retroactively, determine what occurred and how someone, who should not have, managed to cross the border controls. The scope of the attackers is to execute the attacks (physical and cyber) and potentially cause mass casualties of civilians. Additionally, they disrupt the air transportation network, and inflict fear and terror to civilians. The purposes could be either political or religious. To that end, the attackers deploy several cyber- and physical attacks as described in the scenario to provoke congestion and manage to concentrate as many passengers/victims as possible nearby the ABC-gates.

3.3 Scenario #3

Scenario #3 takes place at the Milan Malpensa Airport and involve the AODB (Airport Operation Database), otherwise referred to as Milan Airports Information Systems (M-AIS), the portion of the Resource Management System (RMS) related to the gate assignment and stand assignment, and the Airport Operation Control Centre (AOCC).

Summary: Upon a terrorist's request, an attacker seeks to execute cyber-attacks on the AOCC system so as to manipulate the information displayed in the FIDS, modify gate assignments, resulting in passenger movements which result in an ideal hostage situation and airplane movements on the apron to create a fatal collision.

Reflection: In this attack, the attacker has planned multiple back-up plans which is realistic given the difficulty with which it could be to reach critical airport systems. While this attack starts with cyber-attacks it ultimately results in a huge risk to passenger lives within the airport by creating a panicked crowd in a particular location where an attacker can hurt many people at once, as well as risks to passenger lives in airplanes on the tarmac as two planes change stand assignments at the last minute and potentially crash into each other. Without even stepping foot in the airport, the cyber-attacker can cause enough chaos and damage to bring airport operations to a standstill.

3.4 Scenario #4

This scenario takes place at the Zagreb Airport and is the only one to involve the Baggage Handling System (BHS) and the baggage registration service. It bases on a unique, near-complete Digital Twin of the BHS which is connected directly to the SATIE Toolkit. Therefore, Scenario #4 has been elaborated into three different sub-scenarios to include more threats than originally planned and take advantage of this set-up.

Summary: In order to gain control of the BHS, the attacker proceeds in two ways: By physical intrusion into the BHS room and through social engineering of airport personnel. The first two sub-scenarios result in taking control of the system making it unusable and demanding a ransom payment, while the motive for the last sub-scenario is to drop a bomb on an aircraft.

Reflection: This scenario consists of three different sub-scenarios, among which the most serious is the potential bomb injection into the BHS and consequently into the aircraft. This catastrophic event would certainly result in human casualties and there can be no excuse for it. Consequences of cyber-attacks are a partial or complete lack of usability of the BHS which could lead to flight delays and build-up of crowds where passengers are more vulnerable and easier to attack. Even if this does not happen, reputational and financial losses for the airport would be significant.

3.5 Scenario #5

This scenario is the only one which occurs solely as a simulation. It involves Air Traffic Management (ATM).

Summary: This scenario starts with the bold move of an attacker (e.g. a malicious employee) breaking into the technical room of the airport. He then inserts a USB key with malicious software to one of the servers. Through a chain of cyber-attacks on the computer systems, the attacker is able to stress and distract the Air Traffic Controllers (ATCOs)/Apron Control. A second attacker uses this opportunity to issue some fake clearances and movement advice to aircraft potentially causing collisions of aircraft full of passengers.

Reflection: While physical attacks in the technical room are risky to perform because they require breaking into a series of secure doors, the results are potentially so devastating because of how crucial the data and information is that the ATCOs deal with. Thus, with enough planning of appropriate cyber-attacks and an ounce of confidence, an attacker could be tempted to perform this and bring the airport operations to a screeching halt with potentially hundreds of lives at risk.

4 Results from SATIE Toolkit tests

In the following chapter, the results of the SATIE Toolkit tests and the tool-specific deviations from the test and verification plan laid out in D6.2 (1) are reported. For space reasons, the tables with the detailed results have been moved to Annex 2 (chapter 11).

4.1 CyberRange

4.1.1 Objectives

The CyberRange is used to replicate the Information Technology (IT) infrastructure, Operational Technology (OT) infrastructure, networks, and to simulate cyber-attacks.

4.1.2 Deviations

There were no deviations.

4.1.3 Results of technical tests

All tests were performed successfully. For space reasons, the complete table can be found in section 11.1.

4.2 Emulated Baggage Handling System (BHS)

4.2.1 Objectives

The Digital Twin of the BHS emulates the real behaviour of the Zagreb airport’s BHS and runs the same Sort Allocation Computer System (SAC) software and same Programmable Logic Controller (PLC) code as at the airport site. This allows for the testing of various cyber-attacks in a safe environment and the visualization of the BHS’s behaviour in response to these attacks.

4.2.2 Deviations

There were no deviations.

4.2.3 Results of technical tests

All tests were performed successfully. For space reasons, the complete table can be found in section 11.2.

4.3 Secured ATM Services

4.3.1 Objectives

The Secured ATM Services aggregate information relevant for the provision of Air Traffic Management services, such as flight plans, NOTAMs[1], and weather data, and share them with involved stakeholders. In the SATIE Solution, security aspects of ATM services are integrated into a wider context, including the possibility of correlating cyber-attacks on ATM services with physical attacks. To achieve this goal, the Secured ATM Services provide logging information to the Correlation Engine located in the Security Operation Centre. Automated analysis of log information enables detection of various cyber-threats, for example of malicious access attempts. The Secured ATM Services also accept cybersecurity management commands from the Incident Management Portal to adjust the security configuration (e.g., sensitivity thresholds) to the current threat level. Based on the actual configuration, built-in security mechanisms in Secured ATM Services work more or less stringent, e.g., by allowing or denying individual service access attempts. (Text taken from (3), chapter 11.5.7)

4.3.2 Deviations

There were no deviations with respect to the test plan.

4.3.3 Results of technical tests

All planned tests could be successfully performed. For space reasons, the complete table with the test results can be found in section 11.3.

4.4 Traffic Management Intrusion and Compliance System (TraMICS)

4.4.1 Objectives

TraMICS works at an air traffic controller working position and correlates different indications to a security situation indicator. This indicator expresses how likely it is that the security situation needs attention: “green”, meaning there are no security-related actions needed; “yellow”, meaning something seems strange, be aware; and “red”, meaning that there is most properly a security incident. The security situation indicator is shown to the air traffic controller and additionally send to the Correlation Engine.

4.4.2 Deviations

There were no deviations.

4.4.3 Results of technical tests

All tests were passed. The tests including the results are described in D4.2 (4) and listed in section 11.4.

4.5 Anomaly Detection on Passenger Records (ADPR)

4.5.1 Objectives

The Anomaly Detection on Passenger Records (ADPR system is a sensor of the SATIE Solution. Its goal is to analyse passenger information and match them against a list of persons of interest to raise an alert in case a known threat is detected. The list of persons of interest can either be internal (meaning

[1] NOtice To AirMen. A summary of changes to the published aeronautical information, such as closed runways or temporary obstacles.

hosted on the SATIE Solution) or external (meaning a request for matching is sent to an external system like INTERPOL's Stolen and Lost Travel Documents (SLTD) or Travel Documents Associated with Notices (TDAWN) databases for instance). By default, the SATIE Anomaly Detection on Passenger Records system offers only an internal watch list but support for other watch lists can be added if needs arise.

The Anomaly Detection on Passenger Records system can be connected to different points of the passenger life cycle in the airport, like check-in, boarding pass check, or boarding, to extend the threat analysis of a passenger or it can be used to double check for protection against threat detection system corruption. As a sensor of SATIE Solution, the Anomaly Detection on Passenger Records sends events to the Correlation Engine in the SOC for correlation. Each time passenger data is sent for analysis, the result of this analysis is sent to inform if a threat has been detected and to be correlated with other events to define the proper counter measures. By nature of those threats, alerts generated by the Anomaly Detection on Passenger Records system can be directly processed by airport agents if required.

In addition, the Anomaly Detection on Passenger Records system offers a baggage recognition service. This service allows enrolment, authentication, and identification of baggage through a portable application that can be installed onto a smartphone or tablet. The baggage recognition service is used to ensure the complete traceability of a baggage during its lifecycle in the airport. This second level of verification allows to reinforce the link between a baggage and its tag. Each call to the baggage recognition service is also sent to the Correlation Engine as event to detect a possible large-scale event on the BHS.

4.5.2 Deviations

For the baggage recognition service, the authentication process has been updated. Instead of only displaying "NO HIT" in case an authentication failed, the passenger information and pictures of the bag the scanned tag matches to are displayed. The user then decides whether it is a "HIT" or "NO HIT". This change was implemented to cover also the case where a tag is removed from an enrolled bag and placed on another bag intentionally. Consequently, the expected and obtained results of test cases PAD_BAG_2, PAD_BAG_3, and PAD_BAG_5 are different to those described in the annex of D6.2 (1). An accuracy of authentication can no longer be determined and test case PAD_BAG_6 is no longer applicable. Additionally, test case PAD_ANO_4 is no longer applicable because the data are mainly collected from a passport reader even if the manual insertion is possible.

There were no further deviations from the tests as defined in D6.2 (1).

4.5.3 Results of technical tests

All tests were successfully performed and the results are in line with the expectations. For space reasons, the complete table can be found in section 11.5.

4.6 Unified Access Control (UAC)

4.6.1 Objectives

The Unified Access Control (UAC) solution is part of the physical threat prevention systems within the SATIE Toolkit. The UAC combines fingerprint identification with face recognition over IP camera for airports employees' access control. Adding video analytics allows to detect different threat scenarios that cannot be captured with traditional access control solutions such as a stolen access badge or a tailgating attempt.

4.6.2 Deviations

There were no specific deviations from the tests as defined in D6.2 (1).

4.6.3 Results of technical tests

All tests were successfully performed and the results are in line with the expectations. For space reasons, the complete table can be found in the Annex (section 11.6).

4.7 Business Process-Based Intrusion Detection System (BP-IDS)

4.7.1 Objectives

Business Process Intrusion Detection System (BP-IDS) is part of the cyber threat detection systems BP-IDS is a process monitoring solution that aims at the detection of incidents on technology enabled infrastructures. It operates by collecting traces from sensors scattered on the monitored infrastructure that indicate execution of activities in business processes and in real time matches the activities detected in the executed business process with the specified business process and specified business rules. Whenever those executed process deviate from the specification, the activity is marked as a possible incident and the infrastructure administrator is notified in real-time by BP-IDS with the causes of that anomaly (traces, affected processes, etc.). Thus, offering broad protection against: cybersecurity incidents (such as, intrusions or forgery of equipment behaviour); and operational security incidents (like, equipment and network failure, human error, or natural disasters).

4.7.2 Deviations

There were no specific deviations from the tests as defined in D6.2 (1).

4.7.3 Results of technical tests

The technical tests were performed on the SATIE simulation platform, using the BP-IDS virtual machines deployed on the CyberRange. In all tests, it was possible to verify that BP-IDS was correctly validating BHS network traffic. Also, it was possible to verify that incidents were written on the Kafka communication bus used by the Correlation Engine. For space reasons, the complete table can be found in section 11.7.

4.8 Malware Analyser

4.8.1 Objectives

The Malware Analyser analyses files located on the network it is connected to and provides a detailed security risk analysis report and a risk level.

4.8.2 Deviations

There were no deviations.

4.8.3 Results of technical tests

All tests were performed successfully. For space reasons, the complete table can be found in section 11.8.

4.9 Application Layer Cyber Attack Detection (ALCAD)

4.9.1 Objectives

The Application Layer Cyber Attack Detection (ALCAD) is a Machine Learning (ML)-based anomaly-detection system that uses flow data from the target network to detect suspicious activity in the network. ALCAD is part of the cyber threat detection systems within the SATIE Toolkit. As such, ALCAD delivers additional alerts to the Correlation Engine, thus increasing overall situational awareness. ALCAD's objective is to achieve a high detection performance with preferably low false-positive rate. Thus, an intermediate objective is to teach the ML model using data tailored to Critical Infrastructure (CI) and airport networks not available in openly-available datasets.

4.9.2 Deviations

There were no specific deviations from the tests as defined in D6.2 (1).

4.9.3 Results of technical tests

In this deliverable, only a brief summary for the tests performed for the tool is provided. For a more detailed information on most of these tests, please refer to D4.3 (5) that summarizes work on ALCAD. For space reasons, the complete table can be found in section 11.9.

4.10 Secured Communication on the BHS (ComSEC)

4.10.1 Objectives

Secured Communication on the Baggage Handling System (ComSEC) implements the encryption framework for secured IoT communications on baggage handling systems. ComSEC is network tap system that intercepts network communication packets exchanged between a host and a network switch/router. ComSEC acts as validator component, that intercepts all network traffic and validates the integrity on each network packet. Whenever integrity validation fails to be verified for a given network packet, ComSEC generates integrity alerts.

4.10.2 Deviations

There were no specific deviations from the tests as defined in D6.2 (1).

4.10.3 Results of technical tests

The technical tests were performed on the SATIE simulation platform, using the ComSEC virtual and physical machines deployed on the CyberRange. In all tests, it was possible to verify that ComSEC was correctly validating the network traffic of all BHS machines. Also, it was possible to verify that incidents were written on the Kafka communication bus used by the Correlation Engine. For space reasons, the complete table can be found in section 11.10.

4.11 Business Impact Assessment (BIA)

4.11.1 Objectives

Business Impact Assessment (BIA) is part of the supporting systems located in the SOC. BIA provides threat detection systems capabilities for identifying security incidents in Industrial Control System (ICS) networks and trace the impact of those security events in the business layer of the organization, by clearly stipulating business process and assets compromised. Moreover, the solution combines different techniques for impact assessment, including probabilistic approaches using dependency graphs and probabilistic conditions, for providing a model and a tool for real-time impact assessment that copes with the specific environments found in airport ICS architectures.

Also taking in to account mission-aware impact assessment models, the solution proposed uses knowledge of cyber threats active in the airport infrastructure based on information gathered from intrusion detection systems (e.g. BP-IDS) and inventory systems (e.g. GLPI) and calculate the actual impact on: the assets of the airport; and on the quality of the services offered by the airport (based on business process monitoring offered by BP-IDS).

4.11.2 Deviations

There were no specific deviations from the tests as defined in D6.2 (1).

4.11.3 Results of technical tests

The technical tests were performed on the SATIE simulation platform, using the BIA, IMP and SOC operator virtual machines deployed on the CyberRange. In all tests, it was possible to verify that BIA correctly performed impact assessments. Also, it was possible to verify that BIA was accessible by the SOC operator, through the IMP interface. For space reasons, the complete table can be found in section 11.11.

4.12 Correlation Engine

4.12.1 Objectives

The Correlation Engine is a centralized log management system which receives, analyses, and correlates events. The Correlation Engine triggers alerts with different types of rules to detect cyber and physical threats.

4.12.2 Deviations

There were no deviations.

4.12.3 Results of technical tests

All tests were performed successfully. For space reasons, the complete table can be found in section 11.12.

4.13 Gestion Libre de Parc Informatique (GLPI)

4.13.1 Objectives

GLPI (Gestion Libre de Parc Informatique) is part of the Vulnerability Management System. GLPI is an open source solution for IT service management. Its main functions are: help desk service, assets inventory, and knowledge base management. Its modular architecture allows to extend it using specific plugins. Assets inventories can use a dedicated agent, the FusionInventory agent, deployed on the assets to be inventoried.

In the context of SATIE, GLPI maintains an inventory of the IT assets of an airport. Through its REST API (REpresentational State Transfer Application Programming Interface), GLPI delivers assets information to other SATIE services such as the Risk Integrated Service (RIS), the Correlation Engine, and the Business Impact Assessment. GLPI, with its “Vulnerability” plugin, is able to detect software vulnerabilities in inventoried assets. Using vulnerability data coming from different sources such as the Vulnerability Intelligence Platform (VIP) or the OpenVAS vulnerability scanner, GLPI provides information about vulnerable assets to the other SATIE Tools.

4.13.2 Deviations

There were minor changes from the tests as defined in D6.2 (1), namely anonymizing data such as hostnames, IP address, operating system versions, etc. in order to allow the deliverable to be public without disclosing sensitive information. Apart from these changes, there were no further deviations from the tests as defined in D6.2 (1).

4.13.3 Results of technical tests

The technical tests were performed on the SATIE simulation platform, using GLPI and VIP virtual machines deployed on the CyberRange. In all tests, it was possible to verify that GLPI correctly performed asset management and could access the VIP. For space reasons, the complete table can be found in section 11.13.

4.14 Vulnerability Intelligence Platform (VIP)

4.14.1 Objectives

The Vulnerability Intelligence Platform allows SOC operators to be aware of known vulnerabilities which might be used by hackers.

4.14.2 Deviations

There were no deviations.

4.14.3 Results of technical tests

All tests were performed successfully. For space reasons, the complete table can be found in section 11.14.

4.15 Risk Integrated Service (RIS)

4.15.1 Objectives

The objective of the risk assessment tool as part of SATIE was to offer a clearer and more detailed understanding to airport security staff of where there are vulnerabilities and high risks within the airport environment during the preparatory phase. The risk assessment tool uses compliance to standards and regulations to offer a governance perspective to risks.

4.15.2 Deviations

The only deviations of the tests performed was that originally it was thought that RIS would request vulnerability update information from the VIP tool. However, those vulnerabilities are of a different type: they are very specific, technical, cyber vulnerabilities from a list of known vulnerabilities and not governance-based nor include physical vulnerabilities. Therefore, it would not make sense to overwrite the vulnerabilities in RIS with those. Instead both types of information will be available to the users of SATIE. As a result, integration tests related to getting updated vulnerability data have not been performed.

4.15.3 Results of technical tests

All tests were passed. For space reasons, the complete table can be found in section 11.15.

4.16 Incident Management Portal (IMP)

4.16.1 Objectives

The Incident Management Portal (IMP) receives alerts from the Correlation Engine. It helps the SOC operator to analyse these alerts and understand the severity and consequences of the attack. When a threat is confirmed, the operator classifies the alert as incident. The incidents are sent to the Impact Propagation Simulation (IPS) and to the Crisis Alerting System (CAS).

4.16.2 Deviations

There were no deviations.

4.16.3 Results of technical tests

All tests were performed successfully. For space reasons, the complete table can be found in section 11.16.

4.17 Single Sign-On (SSO) Solution

4.17.1 Objectives

CymID Single Sign-On (SSO) solution provides authentication services implementing a unified log-in experience which makes it possible for a user to authenticate himself only once to access all his applications without having to authenticate himself for each of them separately.

4.17.2 Deviations

There were no deviations.

4.17.3 Results of technical tests

All tests were performed successfully. For space reasons, the complete table can be found in section 11.17.

4.18 Investigation Tool (SMS-I)

4.18.1 Objectives

The SATIE Investigation Tool (SMS-I) is a dedicated web application, that aims to gather information regarding security concerns from the SATIE Toolkit and present them through an Intelligent Dashboard. Using this web app, SOC operators can explore dashboards and information of different levels of detail, including logical information, technical specifications, and a Machine Learning engine used to detect possible incidents and generate association rules which highlight patterns inherent to the alerts' sequential nature.

It communicates with other SATIE Tools, namely the Correlation Engine and the Incident Management Portal, to provide its services. SMS-I periodically fetches data from the Correlation Engine's database and the Incident Management Portal using HTTP/HTTPS (HyperText Transfer Protocol/HyperText Transfer Protocol Secure) requests to obtain new events, alerts, and incidents generated by the SATIE security framework. This data is then used to feed the ML engine and populate the SMS-I's Intelligent Dashboard.

4.18.2 Deviations

There were no deviations.

4.18.3 Results of technical tests

The technical tests were performed on the CyberRange, the SATIE simulation platform. The intended results were achieved. For space reasons, the complete table can be found in section 11.18.

4.19 Impact Propagation Simulation (IPS)

4.19.1 Objectives

The IPS is one of the Impact Propagation Tools which aims to visualize and quantify the impact of certain threats on the airports assets and systems. To this end, IPS receives incidents from the IMP and identifies the affected assets and propagates the impact in a network model. Further, it quantifies the systems' resilience and visualizes the impact of the incident on passenger movement in an Agent-Based Model (ABM).

4.19.2 Deviations

Several changes were needed in the tests to align with some changes in functionality of the IPS that have arisen during the implementation:

- The feature that counters are active or not active has not been implemented in the ABM. The focus had to be moved more to representing the scenarios. Thus, IPS_ABM_1 to _3 have been modified accordingly.
- No mitigation options have been introduced into the ABM. Mitigation options have been implemented in the Network Model instead. As a consequence, IPS_ABM_5 has been removed.
- The mode to trigger the ABM from the Network Model has been implemented slightly differently than originally planned. Thus, IPS_HY_2 is no longer valid and has been removed.

The table in Annex 11.19 has been modified according to the deviations presented in this section. Further, a new test has been introduced to check if not only the ABM but also the Network Model produces the expected output files. Finally, IPS_CON_2 has been rephrased but the content is the same.

4.19.3 Results of technical tests

The tests have been performed on the virtual machine on CyberRange dedicated to IPS. The three simulation engines of IPS have been executed under varying conditions and the expected output files were reviewed. The connection to the Incident Management Portal and the Crisis Alerting System have been tested. All tests – after introducing the deviations mentioned above – could be performed successfully. For space reasons, the complete table can be found in section 11.19.

4.20 Crisis Alerting System (CAS)

4.20.1 Objectives

The CAS is the SATIE component installed in the AOC of an airport, and is used by the AOC operators in order to provide them with common operation picture regarding security incidents. Also, it provides collaboration functionalities, in order to support their communication with the public safety agencies and notification capabilities, for multiple recipient's notification. It receives incidents regrading security issues from the IMP, and presents the IPS results through its GUI.

4.20.2 Deviations

The changes that were made targeted the information visualization and not the core functionality itself. In fact, the naming conventions regarding the incidents sent by the IMP were updated and so the incidents received were called "alarms". This is because for the AOC operators, such an "alarm" could be combined with information from legacy security systems like the Closed-Circuit Television (CCTV) systems and get verified or invalidated. Thus, CAS_INT_1 was modified accordingly.

4.20.3 Results of technical tests

The technical tests were performed through the virtual machines deployed on the CyberRange. Through these tests, the communication channels that were implemented between the CAS and

- the IMP,
- the IPS,
- Public Safety Agencies, and
- Passengers

were tested, and verified. Through this virtual environment, all the functionalities provided by the CAS were also tested. More information regarding these functionalities can be found in D5.4 (6) which is dedicated to the CAS component. For space reasons, the complete table of tests can be found in section 11.20.

5 Results of SATIE Solution validation

Following the presentation of the test results in the previous chapter, the results of the validation performed with SOC operators and AOC operators are described in this chapter. During the validation, subjective data in the form of replies to the simulation validation questionnaire were collected on the level of standard questionnaires – described in section 5.1.1 – general questions – described in section 5.1.2 – and bespoke questions – described in section 5.1.3. Additionally, Key Performance Indicators (KPIs) were determined using objective data recorded during and after the validation exercises and are reported in section 5.2.

5.1 Assessments

In this section, the validation participants subjective assessment of the SATIE Solution is presented. As outlined in the validation plan in deliverable D6.2 (1), it is recorded using a validation questionnaire consisting of three standard questionnaires, tailor-made general validation questions referring to the entire SATIE Toolkit, and tailor-made bespoke validation questions concerning individual SATIE Tools and contributed by the respective tool developer. The results for these are reported in sections 5.1.1, 5.1.2, and 5.1.3, respectively.

In order to limit the number of questions an individual participant had to answer and since not all participants have the background required to answer all questions, the bespoke validation questions on individual tools were only presented to the operators who worked with the tool during the simulation validations. The observers were presented with all bespoke validation questions. The standard questionnaires and the bespoke validation questions were answered by all participants. Additionally, the standard questionnaires, the general validation questions and the bespoke validation questions on the SMS-I, IMP, and CAS were answered by the participants twice: Once after the first exercise and a second time after the last exercise. This allows for a pre-post comparison of how the scores changed over the course of the simulation validation.

A summary of which group of participants (SOC operators, AOC operators, and observers) were presented with which questions and the resulting total number of participants asked per question group is presented in Table 5.1.

Table 5.1: Overview of total number of participants asked per question group

Answered by	Standard Validation Questionnaires	General validation questions	Bespoke validation questions																	
			RIS	VIP	GLPI	ComSEC	UAC	ADPR	Secured ATM Services	TraMICS	BP-IDS	Malware Analyser	Correlation Engine	SMS-I	BIA	IPS	IMP	CAS	CyberRange	Digital Twin of the BHS
SOC operators	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes
AOC operators	Yes	Yes														Yes		Yes		
Observers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Total number of participants asked	**15**	**15**	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**15**	**11**	**8**	**11**	**11**

5.1.1 Standard questionnaires

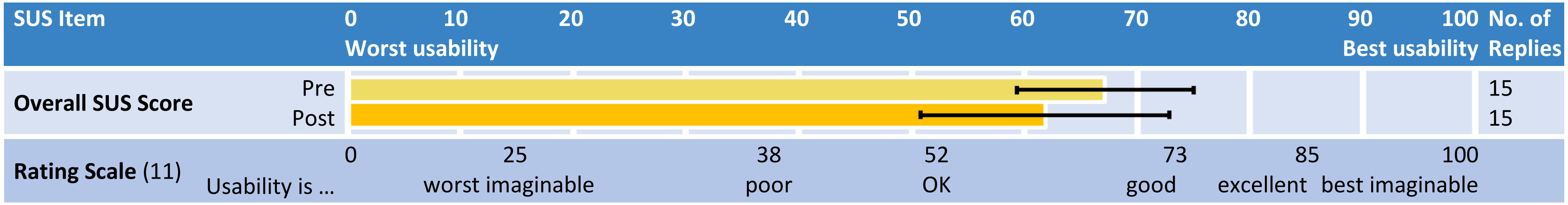
In the SATIE simulation validation questionnaire, three standard questionnaires were used. These are the System Usability Scale (SUS) (7), the SHAPE Automation Trust Index (SATI) (8; 9), and a modified version of the long version of the SHAPE Questionnaire for Assessing Mental Workload in Automation (AIM-l) (9; 10). The results recorded for these questionnaires are reported in the following sections.

5.1.1.1 System Usability Scale

The SUS consists of ten questions rated on a scale from 1 (“strongly disagree”) to 5 (“strongly agree”). The ratings of all questions are aggregated into a single score ranging from 0, equalling the worst possible usability, to 100, equalling the best possible usability. The individual items are not meaningful on their own.

For the SATIE Solution, a SUS score of 67.17 (standard deviation [SD] = 7.84) was recorded directly after the participants completed the first exercise and a slightly lower score of 61.83 (SD = 11.04) after the last exercise, as presented in Table 5.2. According to the rating scale developed by Bangor, Kortum, and Miller (11), these values are in the range of “OK” to “good” usability. The standard deviation is relatively small considering the heterogeneous group of participants coming from three different airports and work environments.

Table 5.2: Results of the System Usability Scale

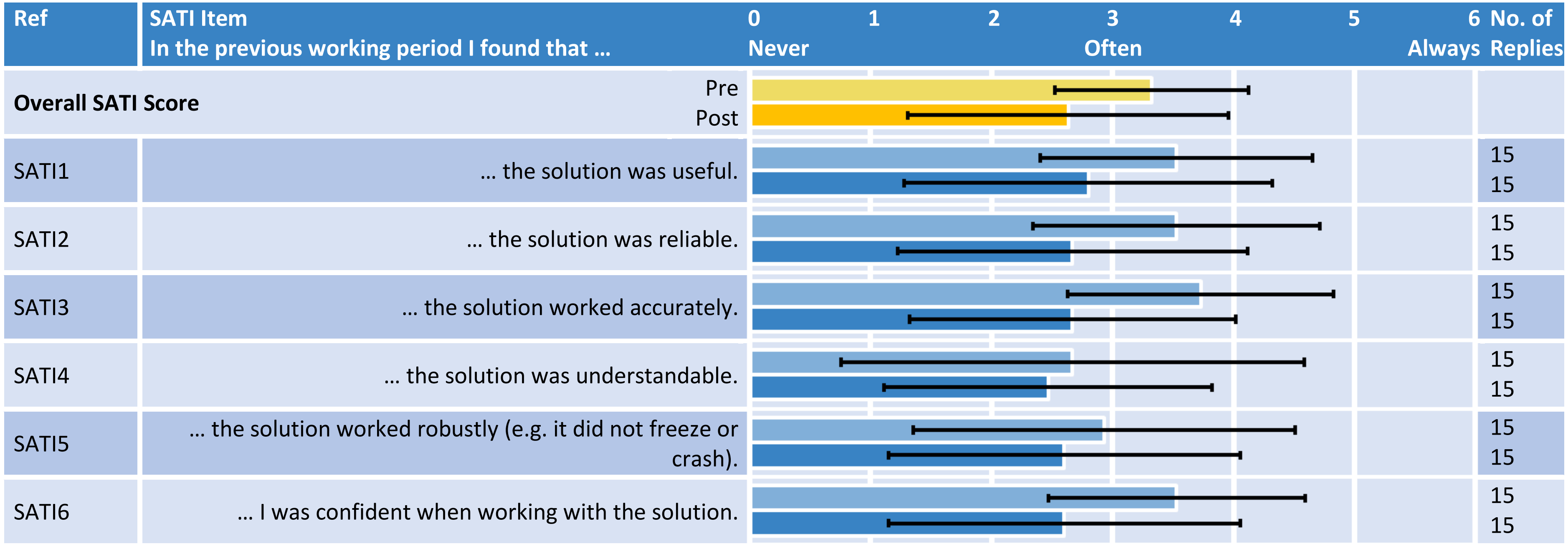


SUS Item		0 Worst usability	10	20	30	40	50	60	70	80	90	100 Best usability	No. of Replies
Overall SUS Score	Pre Post												15 15
Rating Scale (11)	Usability is …	0	25 worst imaginable		38 poor		52 OK		73 good	85 excellent		100 best imaginable	

5.1.1.2 SHAPE Automation Trust Index

For the SATI, the participants rated the six items listed in Table 5.3 (SATI1 through SATI6) on a scale from 0 ("never") to 6 ("always"). In contrast to the SUS, the aggregated SATI score as well as the ratings of the individual items can be interpreted for the SHAPE Automation Trust Index.

Table 5.3: Results of the SHAPE Automation Trust Index



Ref	SATI Item In the previous working period I found that …	0 Never	1	2	3 Often	4	5	6 Always	No. of Replies
Overall SATI Score	Pre Post								
SATI1	… the solution was useful.								15 15
SATI2	… the solution was reliable.								15 15
SATI3	… the solution worked accurately.								15 15
SATI4	… the solution was understandable.								15 15
SATI5	… the solution worked robustly (e.g. it did not freeze or crash).								15 15
SATI6	… I was confident when working with the solution.								15 15

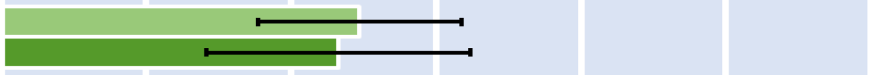
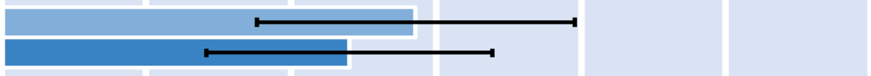
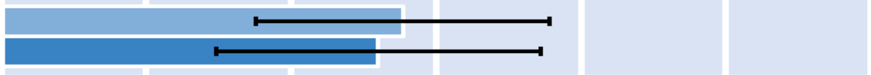
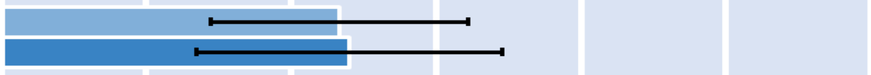
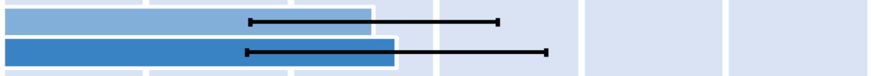
After the first exercise, the participants rated all items except for the understandability (SATI4) and the robustness (SATI5) between a score of three and four. After having completed all validation scenarios, the average rating of all items drops to a similar value between a score of two and three. Throughout all items, a high standard deviation ranging from 0.80 for the overall SATI score after the first exercise to 1.92 for the understandability (SATI4) after the first exercise. Judging by the overall SATI score, the participants placed medium trust in the SATIE Solution.

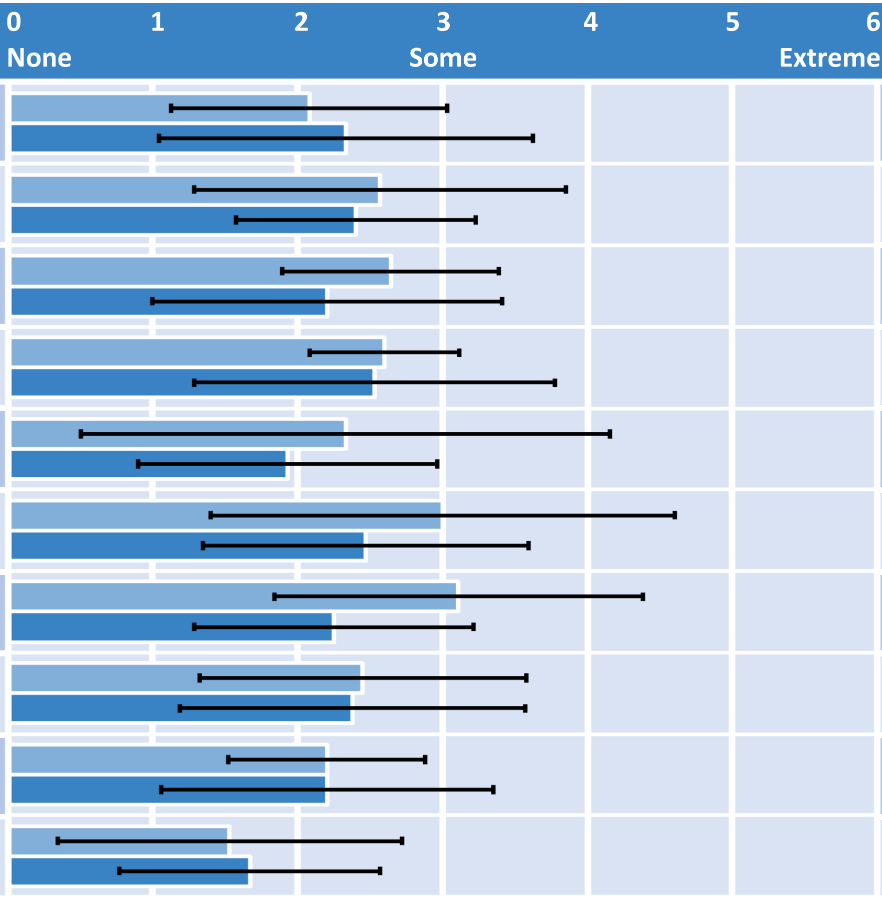
5.1.1.3 SHAPE Assessment of the Impact of Automation on Mental Workload

The assessment of the validation participants' mental workload was performed using a modified long version of the SHAPE Questionnaire for Assessing Mental Workload in Automation (AIM-l). They rated 14 questions about how much effort it took to perform certain actions on a scale from 0 ("none") to 6 ("extreme"). The results are presented in Table 5.4.

In the case of mental workload, a score somewhere in the middle of the rating scale is desirable. A score close to the ends of the rating scale would either indicate a too low workload (lower end of the scale) that could lead to the operator being inattentive and missing important information or a too high workload (upper end of the scale) that could stress and fatigue the operators. The results for the SATIE Solution show a slightly lower than mid-level workload as well for the pre-evaluation as for the post-evaluation. This can also be observed for the individual items that are generally evaluated between a score of 2 and 3. In most cases, the validation participants think that less effort is required for the respective action after handling all threat scenarios compared to the pre-evaluation. The most outstanding items in this regard are "How much effort did it take to understand all information displayed by the system?" (MW10) and "How much effort did it take to evaluate the consequences of a plan (e.g. via IPS and BIA)?" (MW11). The lowest effort was required for sharing information with other parties (MW14) which also was one of SATIE's objectives. As can be expected for a heterogenous group of participants handling the alerts very differently, the standard deviation is overall relatively high, up to a maximum of SD = 1.83 for MW9 pre-evaluation.

Table 5.4: Results of the modified SHAPE AIM-l Mental Workload

Ref	Statement How much effort did it take to …	0 None 1 2 3 Some 4 5 6 Extreme	No. of replies
Overall Score	Pre Post		
MW1	… gather and interpret information?		14 15
MW2	… integrate information from various sources to form a picture?		13 15
MW3	… anticipate the future traffic situation?		12 15
MW4	… verify information sources?		14 15



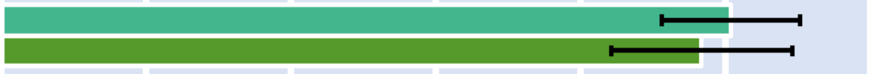
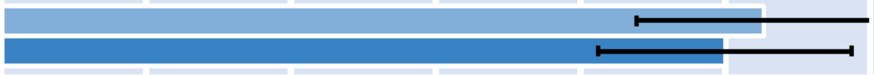
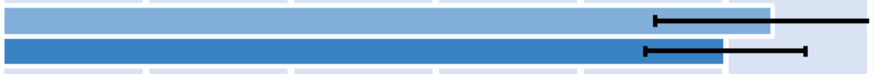
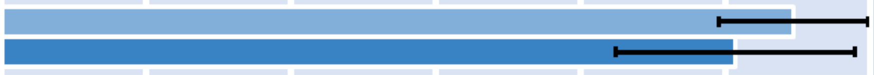
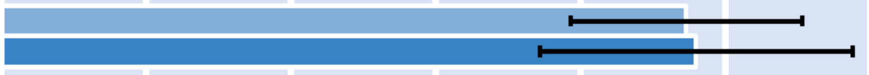
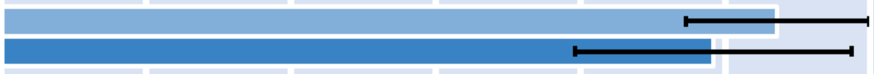
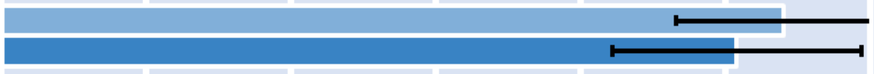
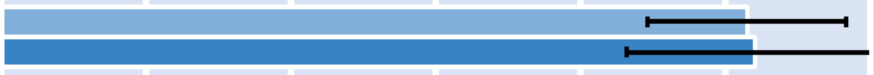
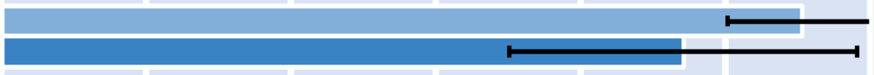
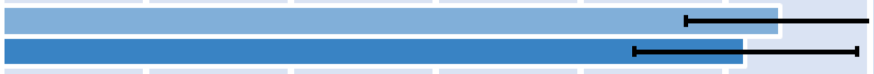
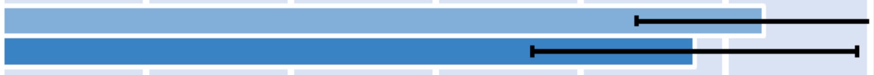
Ref	Statement How much effort did it take to …	No. of replies
MW5	… recall necessary information?	13 15
MW6	… access relevant information?	14 15
MW7	… manage information?	14 15
MW8	… identify potential threats (e.g. via VuMS)?	10 15
MW9	… recognize an attack (e.g. via the alerts)?	12 15
MW10	… understand all information displayed by the system?	15 15
MW11	… evaluate the consequences of a plan (e.g. via IPS and BIA)?	9 12
MW12	… generate mitigation options?	11 13
MW13	… prioritize alerts, security and safety response and recovery actions?	15 15
MW14	… share information with other parties (e.g. SOC, AOC, first responders, general public)?	15 15

5.1.2 General questions

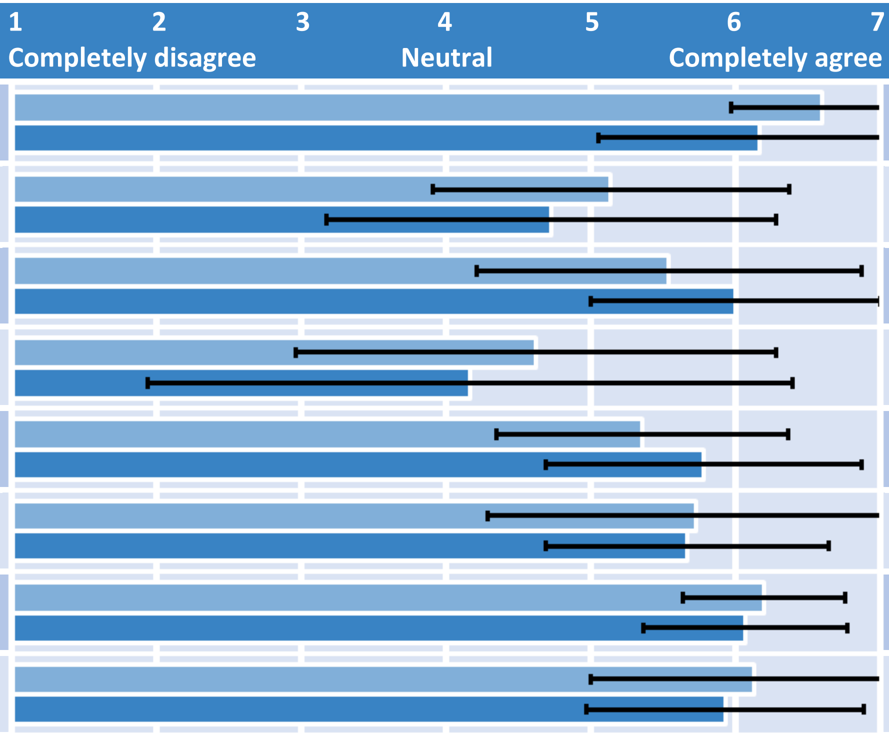
In addition to the standard questionnaires of which the results were reported in the previous sections, tailor-made general questions were answered by the validation participants. The results for these are presented in Table 5.5.

Overall, the participants highly agreed with the statements with only a slight reduction in the agreement from the pre-evaluation to the post-evaluation. This is likely due to a better and more comprehensive understanding of the toolkit after managing all threat scenarios and still a very satisfying result. All individual statements were evaluated on the positive side of the rating scale and most of them around a very good score of 6. The lowest agreement was recorded for the statements “It is easy to integrate the solution with the necessary airport systems.” (GS12) and “The solution boosts revenues.” (GS14). Throughout the individual statements, the standard deviation varies between SD = 0.52 (for GS3 and GS8 pre-evaluation) and SD = 2.23 (for GS14 post-evaluation) which may be attributed to the heterogenous group of participants used to three different airport environments.

Table 5.5: Results of the general questions – Statements (some statements shortened compared to D6.2)

Ref	Statement	1 2 3 4 5 6 7 Completely disagree Neutral Completely agree	No. of replies
Overall	Pre Post		
GS1	The solution is overall a significant improvement compared to my current security-monitoring system.		15 14
GS2	The solution is acceptable as a way to monitor and raise security alerts.		15 14
GS3	The solution provides accurate and up-to-date information.		15 14
GS4	It is intuitive to interact with the solution.		15 15
GS5	The solution provides all relevant information.		14 13
GS6	The solution enables a faster detection of cyber threats compared to my current system.		15 13
GS7	The solution enables a faster detection of physical threats compared to my current system.		13 14
GS8	The solution enables a faster response to cyber threats compared to my current system.		15 14
GS9	The solution enables a faster response to physical threats compared to my current system.		13 14
GS10	The use of the unified SATIE Solution increases the efficiency compared to my current system(s).		15 14

Ref	Statement	No. of replies
GS11	The use of the unified SATIE Solution increases the efficiency compared to using the unconnected IEs and no CE.	15 12
GS12	It is easy to integrate the solution with the necessary airport systems.	14 11
GS13	The solution is innovative compared to others on the market.	13 7
GS14	The solution boosts revenues.	13 6
GS15	I wish to secure my system using the SATIE Solution.	14 9
GS16	I think that the attack could have happened under the presented circumstances.	15 15
GS17	I understood the flow of events in the attack.	15 15
GS18	The simulation on the CyberRange worked flawlessly.	15 15



In addition to the statements, four free text questions were answered by the participants, the results of which can be found in Table 5.6. When asked for the most outstanding Innovation Elements (GT1), the participants replied with a wide variety of SATIE Tools. They named the two central interaction systems, the Incident Management Portal and the Crisis Alerting System, as well as three of the supporting systems (Correlation Engine, RIS, and IPS) and four of the threat prevention and detection systems (Malware Analyser, Unified Access Control, ALCAD, and TraMICS). The reasons stated range from the tools being easy to use or user friendly to them being innovative. Two of the participants replied that all SATIE Tools stood out for them because they all are innovative.
The other three free text questions were designed to be asked in case the participant disagreed with statement GS2 (GT2), GS5 (GT3), or GS11 (GT4). Since none of the participant disagreed with the respective statements, no replies for the questions GT2, GT3, and GT4 were collected.

Table 5.6: Results of the general questions - Free text questions

Ref	Question	Reply
Free text question		
GT1	Which of the Innovation Elements stood out for you and why?	• All of them because they were useful. (2x) • The Correlation Engine. (2x) • The Incident Management Portal, because it is easy to monitor the alerts and perfectly connected with other tools and the CAS because it's so user friendly. • A complete solution built to bring together major aspects of a modern airport in terms of collaborating and managing threats. • RIS, because it's a very innovative tool compared to the tools currently used. • The Malware Analyser and Unified Access Control. • The Incident Management Portal, the CAS, the TraMICS, the ALCAD, the Agent-based Model of the Impact Propagation Simulation. • The TraMICS, because it is really innovative.
GT2	Please consider to briefly explain why you think that the solution is not acceptable as a way to monitor and raise security alerts.	*No participant disagreed with statement GS2.*
GT3	You indicated that the solution does not provide you with all relevant information. What information do you feel is missing?	*No participant disagreed with statement GS5.*
GT4	You indicated that you do not think that the unified SATIE solution is more efficient than the unconnected Innovation Elements. Please explain why.	*No participant disagreed with statement GS11.*

5.1.3 Bespoke validation questions on individual SATIE Tools

In this section, the results of the bespoke validation questions on individual SATIE Tools are presented. The questions were provided by the respective partner developing the tool and are phrased as statement, how-question, free text question, or drop-down question, as outlined in section 4.1.3 of deliverable D6.2.

The statements are evaluated on a scale from 1 “completely disagree” to 7 “completely agree” and the how-questions on a scale with the same number of steps from 1 “very little” to 7 “very much”. The results for both question types are depicted as bar charts representing the average evaluation over all replies with an error bar representing the standard deviation. Additionally, an overall score summarizing all statements or how-questions is presented. For the free text and drop-down questions, the participants’ aggregated replies are reported. More detailed results, including the minimum and maximum values, can be found in Annex 3, section 12.3.

5.1.3.1 Risk Integrated Service

In the following Table 5.7, the results of the statements and how-questions for the Risk Integrated Service are presented. The statements’ overall rating is very positive at a value of 5.91 (SD = 0.63). The statement rated best is “I trust the results to be accurate.” (IE01xNISS01) at a score of 6.27. The worst rated statement is IE01xNISS06 at a score of 5.38 which is still on the positive side of the rating scale. The participants’ average evaluation of the how-question is 5.67 and also a satisfying result. Throughout all statements and how-questions, the standard deviation is relatively small, the maximum is 1.21 for IE01xNISH01, especially since the participants came from three different airports and are used to different work environments.

None of the participants wished for other kinds of results, as indicated by the answers to the free text question (IE01xNIST01) presented in Table 5.8.

Table 5.7: Results for RIS - Statements and how-questions

Ref	Question	No. of replies
Statements	Overall	
IE01xNISS01	I trust the results to be accurate.	11
IE01xNISS02	The interface is user friendly.	10
IE01xNISS03	RIS displays the results in a useful format.	10
IE01xNISS04	I understand how to interpret the risk values of assets.	11
IE01xNISS05	I understand how to interpret the risks associated with threats.	11
IE01xNISS06	The "what-if" scenarios help identify the best countermeasures to take.	8
How-questions	Overall	
IE01xNISH01	How much more useful is this risk assessment approach compared to the one currently in place?	6

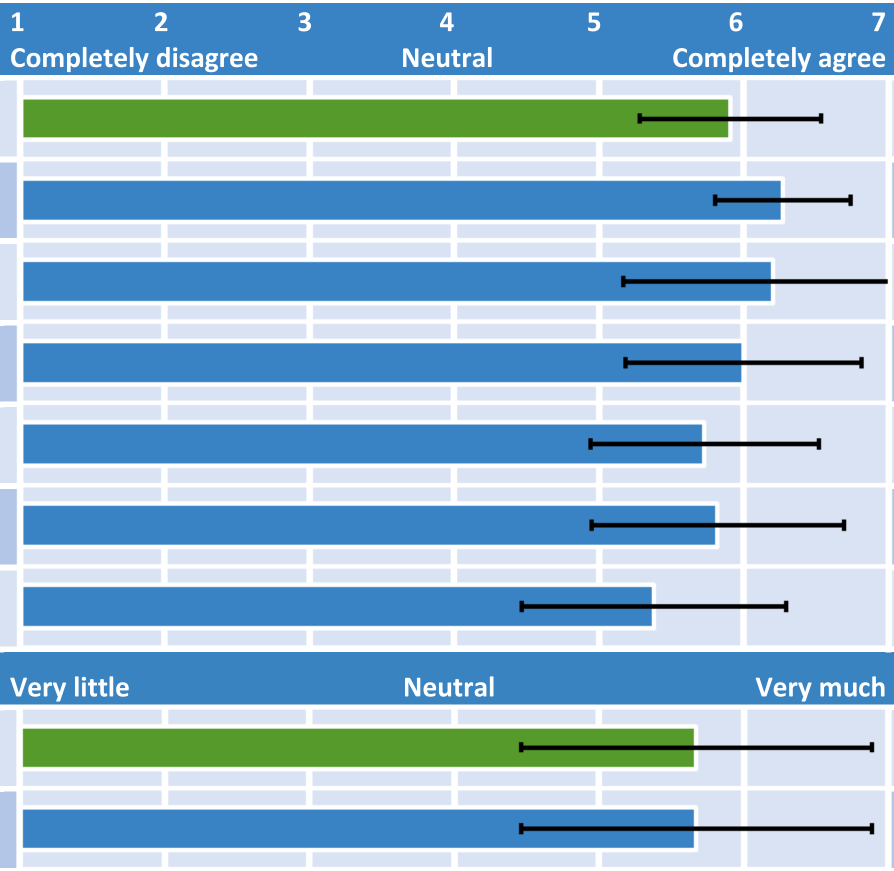


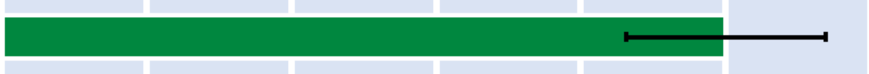
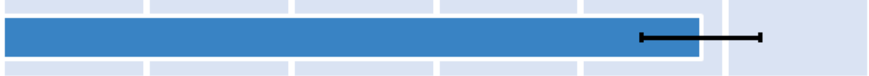
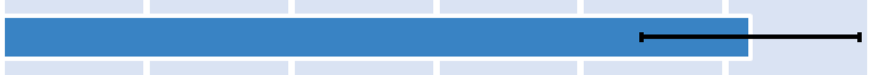
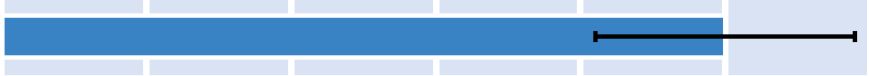
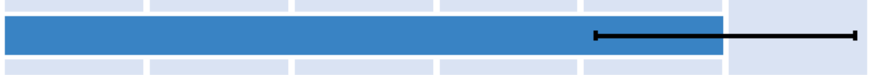
Table 5.8: Results for RIS - Free text question

Ref	Question	Reply
Free text question		
IE01xNIST01	What other kinds of risk results would be useful to have? If none, write 'None'.	• None. (4x)

5.1.3.2 Vulnerability Intelligence Platform

The results for the statements on the Vulnerability Intelligence Platform are summarized in Table 5.9 below. The replies to all statements and the overall score lie in around a score of six indicating a high agreement with the statements. Furthermore, the standard deviation is small at a maximum value of 0.89 which is indicative of a homogenous answering pattern among the validation participants.

Table 5.9: Results for VIP - Statements

Ref	Question	1 2 3 4 5 6 7 Completely disagree Neutral Completely agree	No. of replies
Statements	Overall		
IE02xACSS01	The information about the Common Vulnerabilities and Exposures (CVE) is easily understandable.		11
IE02xACSS02	I trusted the list of vulnerabilities (Common Vulnerabilities and Exposures) to be up to date.		10
IE02xACSS03	The information about possible impacted assets is easily understandable.		10
IE02xACSS04	I trusted the list of vulnerabilities (Common Vulnerabilities and Exposures) to be accurate.		11

5.1.3.3 Gestion Libre de Parc Informatique

In the following Table 5.10, the results for the statements and the how-question on the Gestion Libre de Parc Informatique are summarized. The overall agreement to the statements is 5.67 (SD = 0.90) which is a very good result. Three of the statements received an agreement score above six. These are "I trust the vulnerability information to be accurate." (IE02xTLBS04, 6.50, SD = 0.58), "I can easily find additional information about the asset or vulnerability in the incident." (IE02xTLBS05, 6.25, SD = 0.50), and "I trust the asset information to be up-to-date." (IE02xTLBS02, 6.20, SD = 0.45). The participants agreed the least with statement IE02xTLBS01 ("There is enough information in an alert to identify the particular asset impacted.") at a score of 5.50 (SD = 1.05) that is still a satisfying result. Furthermore, the participants think that it is highly beneficial to access GLPI specifically (IE02xTLBH01) expressed in a score of 6.25 (SD = 0.50). Even though the standard deviation for IE02xTLBS01 and IE02xTLBS03 is above 1.00, it is regarded as generally small considering the diverse group of participants.

Each of the free text questions and the dropdown question (see Table 5.11) were only answered by one participant. The replies indicate that no information needed to identify an impacted asset or to understand a vulnerability is missing and that there was no need to access GLPI because of missing information.

Table 5.10: Results for GLPI - Statements and how-questions

Ref	Question	No. of replies
Statements	Overall	
IE02xTLBS01	There is enough information in an alert to identify the particular asset impacted.	6
IE02xTLBS02	I trust the asset information to be up-to-date.	5
IE02xTLBS03	The asset information in GLPI correctly reflects the information in my airport system.	5
IE02xTLBS04	I trust the vulnerability information to be accurate.	4
IE02xTLBS05	I can easily find additional information about the asset or vulnerability in the incident.	4
IE02xTLBS06	The information about assets and vulnerabilities is easy to understand.	5
How-questions	Overall	
IE02xTLBH01	How beneficial (how much information is gained) is it to access GLPI specifically?	4

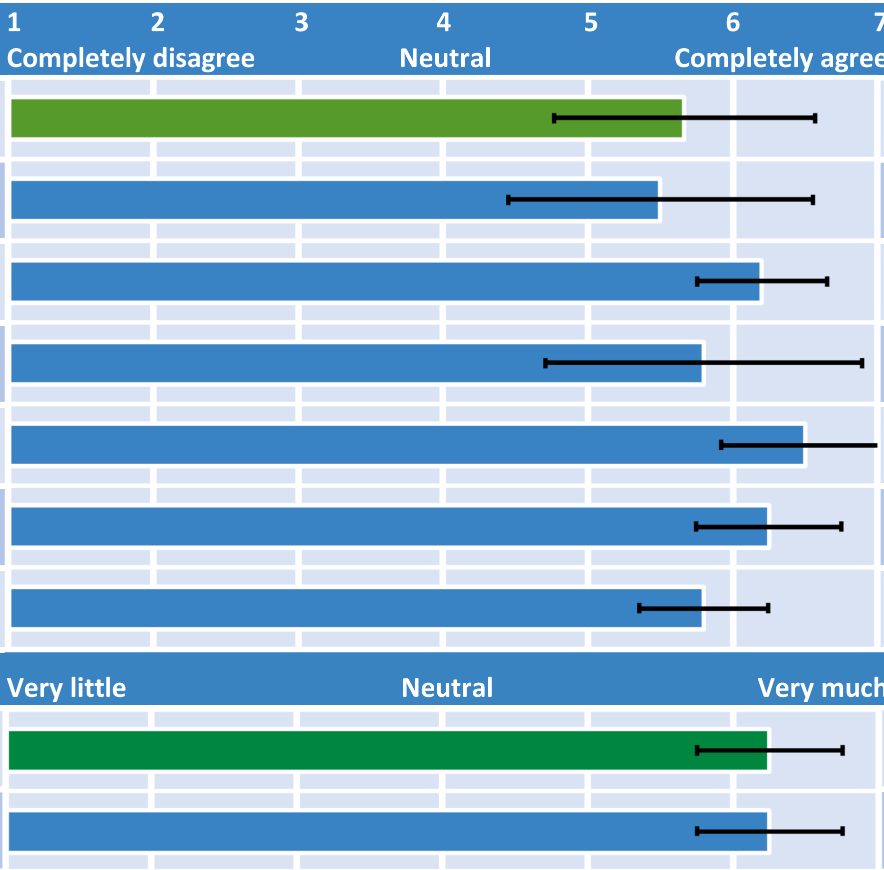


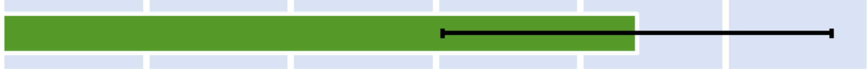
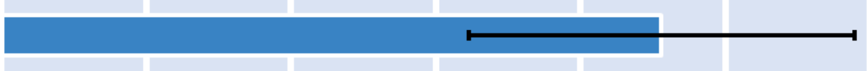
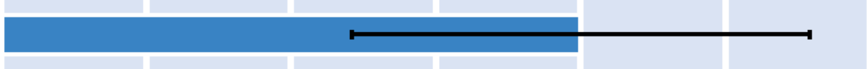
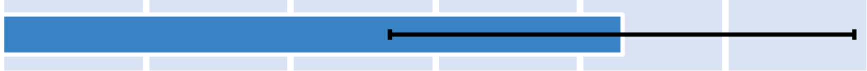
Table 5.11: Results for GLPI - Free text questions and dropdown question

Ref	Question	Reply
Free text questions		
IE02xTLBT01	What information, if any, is missing to identify the particular asset impacted?	• None.
IE02xTLBT02	What additional information should there be to fully understand the vulnerability?	• None.
Dropdown question		
IE02xTLBD01	Did you need to access GLPI during an incident because of missing information?	0x Yes 1x No

5.1.3.4 Secured Communication on the BHS

The questionnaire results for the ComSEC are presented in Table 5.12 (statements) and Table 5.13 (free text and dropdown questions). The overall evaluation of the statements is on the positive side of the rating scale at a score of 5.39 (SD = 1.34). While the participants mostly agree that the ComSEC raises the airport's infrastructure security compared to the current situation (IE03INOVS01), the compatibility of the alert reception with the current SOC (IE03INOVS02) received the lowest agreement (5.00, SD = 1.58), that, however, still is above a neutral score. Throughout all statements, the standard deviation is relatively high, indicating a heterogenous answering pattern as can be expected for a diverse group of participants currently working with different airport systems.

Table 5.12: Results for ComSEC - Statements (some statements shortened compared to D6.2)

Ref	Question	1 2 3 4 5 6 7 Completely disagree Neutral Completely agree	No. of replies
Statements	Overall		
IE03INOVS01	I think that deploying ComSEC would raise the airport infrastructure security compared to the current situation.		9
IE03INOVS02	The possibility to receive ComSEC alerts via Kafka, syslog, or email is compatible with the current SOC.		5
IE03INOVS03	The ComSEC alerts are informative enough to pinpoint cyber-attacks.		7

When asked for the information that are missing in the current alerts (IE03INOVT01), the participants responded that they wish for more alert types, better access to information, and indication of the origin of the alert, and the specific analysis of the network package's content. The preferred way to receive alerts is through Syslog (IE03INOVD01).

Table 5.13: Results for ComSEC - Free text question and dropdown question

Ref	Question	Reply
Free text question		
IE03INOVT01	What information is missing from the ComSEC alert to identify the cyber-attack?	• More security threat types. • Improve access to information. • Origin of alert important to isolate attacker, but not clear. • Analysis of network package content.
Dropdown question		
IE03INOVD01	Which ComSEC alert format is preferred?	1x Kafka 5x Syslog 1x E-mail

5.1.3.5 Unified Access Control

In the following Table 5.14, the results for the statements and how-questions on the UAC are presented. All of the statements were rated at or above a score of six indicating a very high agreement. The lowest agreement and also the highest standard deviation were recorded for the statement "The contactless aspects of this solution are essential for end-users." (IE04xIDES04) at a score of 6.00 (SD = 1.00). Similarly, the statement that received the highest agreement ("The tailgating detection is useful.", IE04xIDES02) at a score of 6.67 is the one with the smallest standard deviation (SD = 0.50). The participants' ratings of the how-questions are both on the positive side of the rating scale, but quite different. The score for the ease of integration with existing systems (IE04xIDEH01) is the comparatively low at 5.00 (SD = 1.41) and the score for the importance of differentiating group access rights between different groups of employees (IE04xIDEH02) is much higher at 6.50 (SD = 0.71).

The validation participants' replies to the free text questions and the dropdown question are listed in Table 5.15. There were no suggestions for additional detections that should be performed by the UAC, but multiple ideas for areas where the face recognition capabilities may also be employed, like all places that only authorized personnel should be able access and specifically the gates, passport controls and the AOC access. Finally, most participants prefer to receive the alerts in the SOC (e.g. displayed in the Incident Management Portal).

Table 5.14: Results for UAC - Statements and how-questions (some statements shortened compared to D6.2)

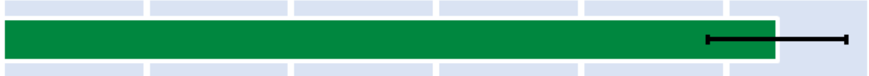
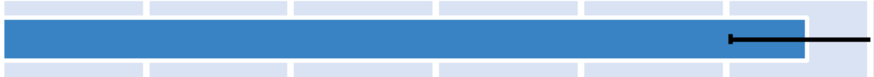
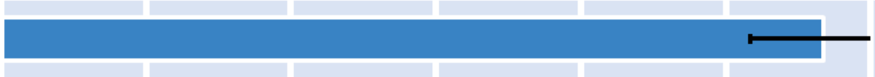
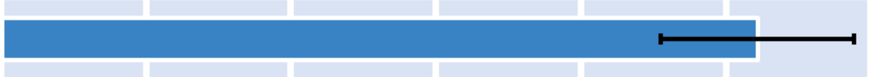
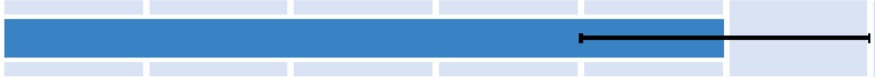
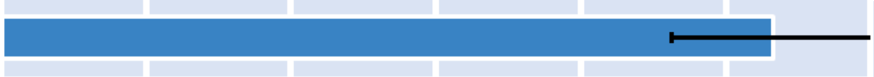
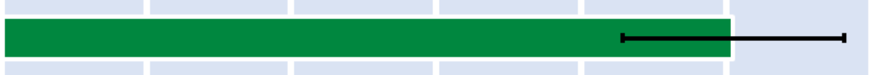
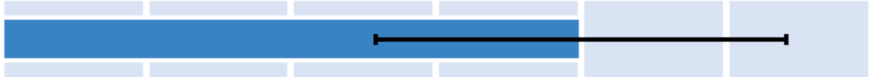
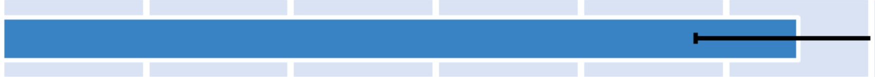
Ref	Question	1 2 3 4 5 6 7 Completely disagree Neutral Completely agree	No. of replies
Statements	Overall		
IE04xIDES01	The dual authentication (face + finger or card) is useful against fraud.		9
IE04xIDES02	The tailgating detection is useful.		9
IE04xIDES03	The detection of threats that are unrelated to the access workflow is useful.		9
IE04xIDES04	The contactless aspects of this solution are essential for end-users.		9
IE04xIDES05	I think that the end-users will like to use this solution.		9
		Very little Neutral Very much	
How-questions	Overall		
IE04xIDEH01	How easy is it to integrate the Unified Access Control solutions in your eco-system?		6
IE04xIDEH02	How important it is to differentiate "group access rights" between different type of employees?		10

Table 5.15: Results for UAC - Free text questions and dropdown question

Ref	Question	Reply
Free text questions		
IE04xIDET01	Do you miss a detection that you find necessary for the access control purpose? If yes, which?	• No detections missed.
IE04xIDET02	Do you think that the face recognition capabilities are useful elsewhere? If yes, where?	• In the IT infrastructure to enhance on the field jobs (e.g. perform tasks inside a DatCenter). • All places/assets that only specific personnel should access. • Gates, passport controls, AOC access.
Dropdown question		
IE04xIDED01	In which environment/solution do you prefer to receive the alerts?	1x within the Video Management System 6x within the SOC 2x on the Physical Access Control System (PACS) Monitor 1x at the access point (e.g. a sound signal, siren, or flashing lights) 0x routed to Police system (for threats/terrorist detected)

5.1.3.6 Anomaly Detection on Passenger Records

The validation participants' replies to the statements on the Anomaly Detection on Passenger Records are summarized in Table 5.16. The overall score of all statements is 5.63 (SD = 2.08) indicating a satisfying agreement, but there are considerable differences between the ratings of individual statements: Two of the statements – "The information in alerts generated by passenger data anomaly detection is useful." (IE05xIDES02) and "The passenger data anomaly detection improves the threat detection." (IE05xIDES05) – received almost perfect scores at 6.83 (SD = 0.41). Meanwhile, the ease of integration (IE05xIDES04) was rated at a lower score of 5.33 with a high standard deviation of SD = 2.08. However, this statement and five others (IE05xIDES03 and IE05xIDES07 trough IE05xIDES10) were replied to only by four or less participants giving them a low expressiveness.

In Table 5.17, the replies to the free text questions are listed. When asked for other kinds of anomalies that could be detected better with the ADPR (IE05xIDET01), the participants suggest the usage for bags that missed an internal scan point (e.g. on the way from the chute to the aircraft). The top benefits listed (IE05xIDET02) are the baggage reconciliation, a clear view of what, where, and when and the alerting capabilities. The issues the participants see (IE05xIDET03) are that not enough information are contained in the alert and the GDPR (General Data Protection Regulation) compliance of the ADPR. The suggestions for use-cases outside of the BHS environment (IE05xIDET04) include remote baggage drop off locations, identification of unattended baggage, and airlines' ground handling operations.

Table 5.16: Results for ADPR - Statements (some statements shortened compared to D6.2)

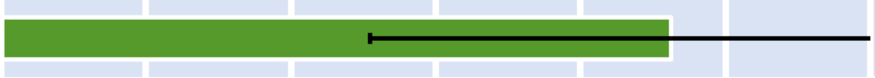
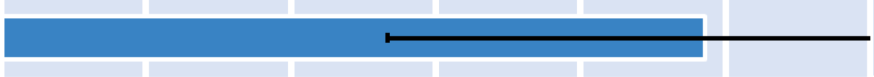
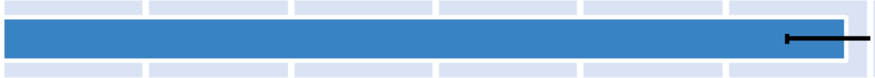
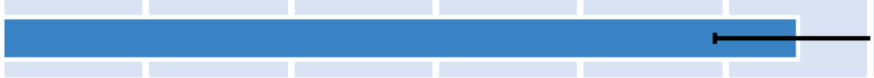
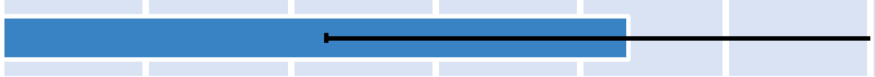
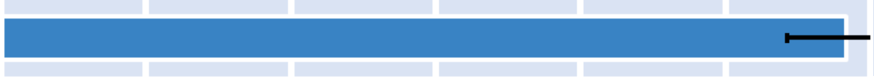
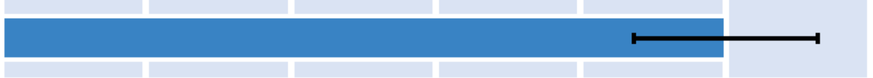
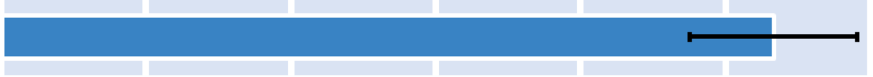
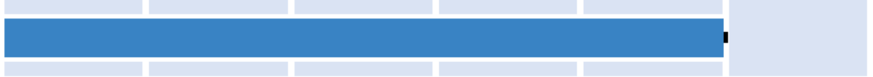
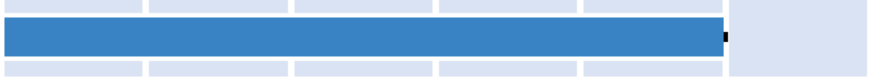
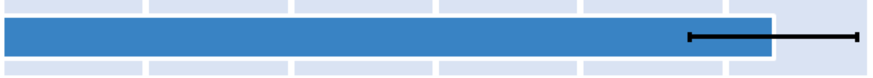
Ref	Question	1 2 3 4 5 6 7 Completely disagree Neutral Completely agree	No. of replies
Statements	Overall		
IE05xIDES01	The information in alerts generated by passenger data anomaly detection is easy to understand.		7
IE05xIDES02	The information in alerts generated by passenger data anomaly detection is useful.		6
IE05xIDES03	The passenger data anomaly detection is useful for my day-to-day work.		4
IE05xIDES04	The passenger data anomaly detection is easy to integrate into my existing system.		3
IE05xIDES05	The passenger data anomaly detection improves the threat detection.		6
IE05xIDES06	I am interested in more anomaly detection functions like the use of other watch lists or a business rules engine.		6
IE05xIDES07	The baggage registration service is easy to understand.		3
IE05xIDES08	The baggage registration service is easy to use.		3
IE05xIDES09	The baggage registration service is useful in my day-to-day work.		2
IE05xIDES10	The baggage registration service is accurate enough to be used in day-to-day operations.		3

Table 5.17: Results for ADPR - Free text questions

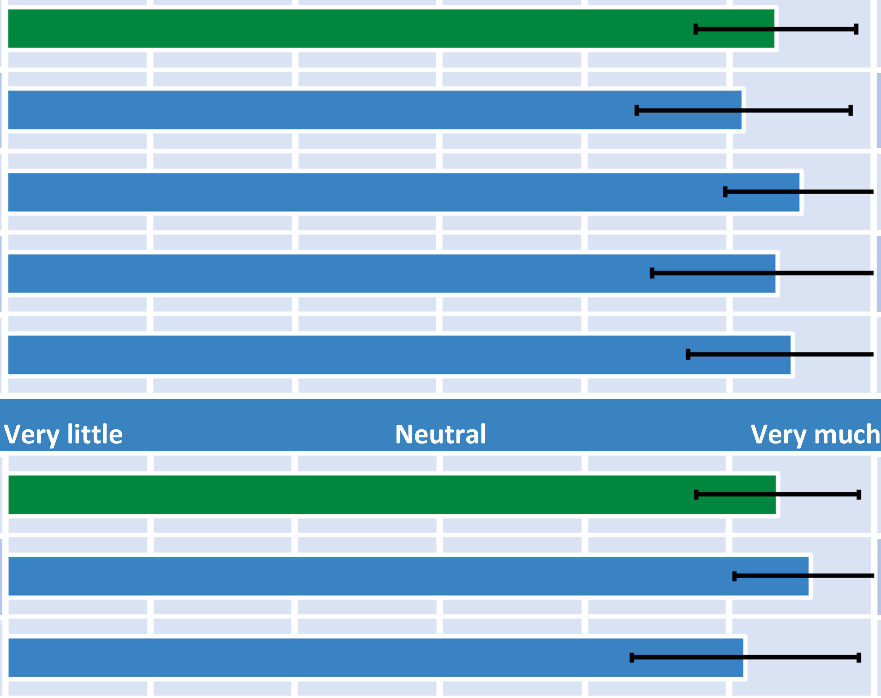
Ref	Question	Reply
Free text questions		
IE05xIDET01	Can you think of other kinds of anomalies that could better be detected with this tool?	• For bags that missed an internal scan point (e.g. on their way from the chute to the aircraft).
IE05xIDET02	What are the top three benefits of using a service like the baggage registration service?	Top 1: • Baggage reconciliation. • Clear view of what, where, and when. Top 2: • Alerting capabilities. Top 3: • *None mentioned.*
IE05xIDET03	Do you see any issues with using a service like the baggage registration service?	• More information on the raised alarm highly appreciated. • GDPR related issues.
IE05xIDET04	Do you think that the baggage registration service is useful outside of the BHS environment? If yes, where?	• For unattended bags. • In IT department to detect anomalies regarding IT infrastructure and BHS infrastructure. • For remote baggage drop off locations, security services, or airlines' ground handling operations.

5.1.3.7 Secured ATM Services

In Table 5.18, the results for the statements and how-questions on the Secured ATM Services are presented. The overall evaluation of the statements and the results for all individual statements are above a value of six and on the very positive side of the rating scale. The lowest agreement was recorded for the statement “The possibility of the Incident Management System to adjust the Threat Level of the ATM Service is useful.” (IE06xFQSS01) at a score of 6.10 (SD = 0.74). A similar pattern is visible for the how-questions. Here, the lowest rating is seen for the question “How much added value is generated by correlation of different alerts (e.g., DOS + physical door intrusion)?” (IE06xFQSH02) with a score of 6.11 (SD = 0.78). The maximum standard deviation across all statements and how-questions is small at 0.87, pointing towards a homogenous answering pattern.

In response to the free text question on whether there is a need for more alert types, the participants didn't wish for more alert types, but highlighted that there should be few alerts with precise information in order to quickly identify the underlying problem.

Table 5.18: Results for Secured ATM Services - Statements and How-questions



Ref	Question	1 Completely disagree	2	3	4 Neutral	5	6	7 Completely agree	No. of replies
Statements	Overall								
IE06xFQSS01	The possibility of the Incident Management System to adjust the Threat Level of the ATM Service is useful.								10
IE06xFQSS02	The correlated alert is received early enough to provide sufficient time to react.								10
IE06xFQSS03	The alerts are improving my detection of attacks compared to my current system.								9
IE06xFQSS04	The alerts are improving my time to detect attacks compared to my current system.								9
		Very little			Neutral			Very much	
How-questions	Overall								
IE06xFQSH01	How useful is the provision of individual alerts (e.g. for Brute Force Attack, or DOS Attack)?								9
IE06xFQSH02	How much added value is generated by correlation of different alerts (e.g., DOS + physical door intrusion)?								9

Table 5.19: Results for Secured ATM Services - Free text question

Ref	Question	Reply
Free text question		
IE06xFQST01	Which additional alerts do you think would be useful in the context of ATM Services?	• No need for additional alerts. • Alerts must be few and precise in order for the operator to understand exactly what the problem is.

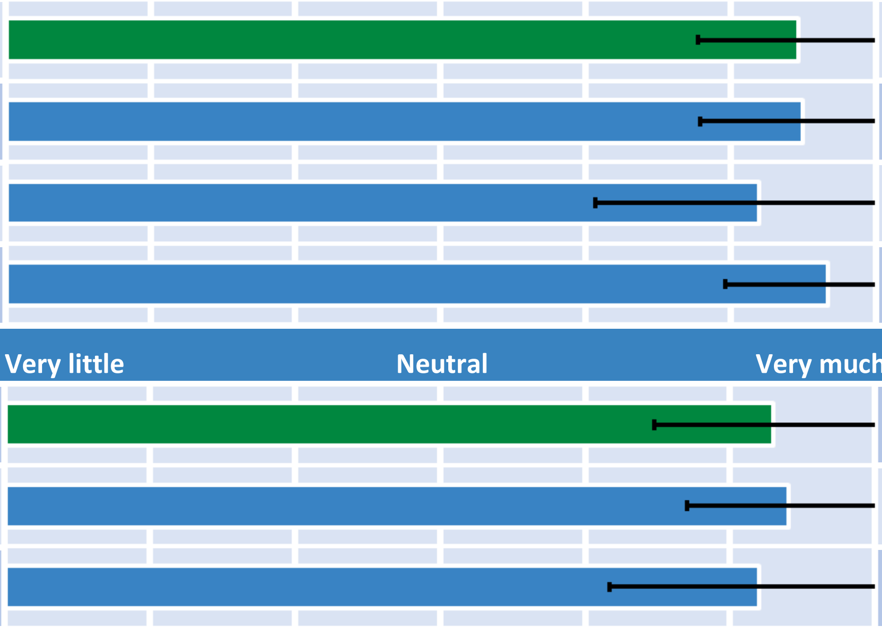
5.1.3.8 Traffic Management Intrusion and Compliance System

In the following Table 5.20, the results for the statements and how-questions on the TraMICS are presented. Compared to the planning laid out in D6.2, the statement "The single alerts are received early enough for an appropriate reaction." (IE07xDLRS02) was removed as it is no longer applicable in the final implementation of the TraMICS's alerts in the IMP. For the same reason, the statements IE07xDLRS01 and IE07xDLRS03 were slightly modified.

As can be seen from the table, the TraMICS received an overall very good evaluation, both for the statements (6.47, SD = 0.69) and for the how-questions (6.30, SD = 0.82). The un-correlated single alerts are experienced as very useful (IE07xDLRH01) as is the correlated security situation indicator (IE07xDLRH02) and the combination of single alerts and security situation indicator (IE07xDLRS01). Further, the participants find the correlated security situation indicator to be provided early enough to identify a potential coordinated attack (IE07xDLRS03). Throughout all statements and how-questions, the standard deviation is quite small – the maximum SD is 1.13 for IE07xDLRS03 – and indicates a homogenous answering pattern given that the validation participants are used to three very different work environments with different expectations of the tool.

Table 5.20: Results for TraMICS - Statements and how-questions

Ref	Question	1 Completely disagree · 2 · 3 · 4 Neutral · 5 · 6 · 7 Completely agree	No. of replies
Statements	Overall		
IE07xDLRS01	The combination of TraMICS single alerts and the TraMICS security situation indicator is useful.		10
IE07xDLRS03	The TraMICS security situation indicator is received early enough to identify a potential coordinated attack.		10
IE07xDLRS04	The TraMICS information is useful in the context of Airport Operations/Security.		9
		Very little · Neutral · Very much	
How-questions	Overall		
IE07xDLRH01	How useful are the un-correlated single alerts?		10
IE07xDLRH02	How useful is the TraMICS correlated security situation indicator?		10



In addition to the statements and how-questions presented above, two free text questions on the TraMICS were answered by the validation participants. The responses are summarized in Table 5.21 below. The answers show that no additional single alerts are wished for and the only area for improvement is one entire week being covered by the correlated security situation indicator compared to currently 5 minutes.

Table 5.21: Results for TraMICS - Free text questions

Ref	Question	Reply
Free text questions		
IE07xDLRT01	Which alerts are missing? If there are none, please write "None".	• None. (5x)
IE07xDLRT02	Which timeframe shall be used to derive the correlated security situation indicator? If you would like to have multiple correlated security situation indicators over different timeframes, please add multiple answers to the text field.	• Summary for an entire week (24/7).

5.1.3.9 Business Process-based Intrusion Detection System

In the following Table 5.22, the results for the statements on the Business Process-based Intrusion Detection System are displayed. The overall rating of the BP-IDS is on the positive side of the rating scale at a score of 5.50 (SD = 1.13). There is little variation between the results for individual statements. The agreement with the best rated statement – "The BP-IDS alerts are informative enough to pinpoint cyber-attacks." (IE08INOVS03, 5.86, SD = 1.07) – is close to that of the lowest rated statement – "The possibility to receive BP-IDS alerts via Kafka, Syslog, or email is compatible with the current SOC." (IE08INOVS02, 5.33, SD = 1.21). The standard deviation ranges between 1.07 for IE08INOVS03 and 1.21 for IE08INOVS02 as can be expected for the heterogenous group of participants.

In Table 5.23, the validation participants' replies to the free text question and the dropdown question are presented. As can be seen, none of the participants needs more information in the BP-IDS's alerts to identify the cyber-attack. The preferred way to receive the alerts is through Syslog.

Table 5.22: Results for BP-IDS - Statements (some statements shortened compared to D6.2)

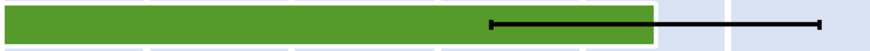
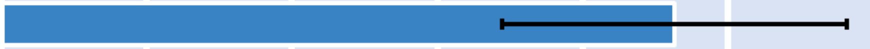
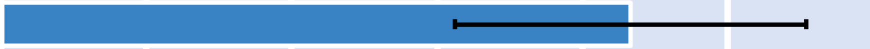
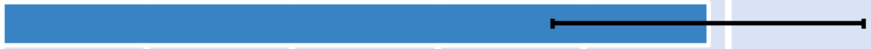
Ref	Question	1 Completely disagree 2 3 4 Neutral 5 6 7 Completely agree	No. of replies
Statements	Overall		
IE08INOVS01	I think that deploying BP-IDS would increase airport infrastructure security compared to the current situation.		8
IE08INOVS02	The possibility to receive BP-IDS alerts via Kafka, syslog, or email is compatible with the current SOC.		6
IE08INOVS03	The BP-IDS alerts are informative enough to pinpoint cyber-attacks.		7

Table 5.23: Results for BP-IDS - Free text question and dropdown question

Ref	Question	Reply
Free text question		
IE08INOVT01	What information is missing from the BP-IDS alert to identify the cyber-attack?	*No replies.*
Dropdown question		
IE08INOVD01	Which BP-IDS alert format is preferred?	1x Kafka 5x Syslog 1x E-mail

5.1.3.10 Malware Analyser

The results for the statements and the free text question on the Malware Analyser are presented in Table 5.24 and Table 5.25. Both statements were rated above a score of six and with standard deviations of SD = 0.64 (IE08xACSS01) and SD = 0.74 (IE08xACSS02) indicating a high agreement and a homogenous answering pattern. None of the participants wished for additional status types (IE08xACST01).

Table 5.24: Results for Malware Analyser - Statements

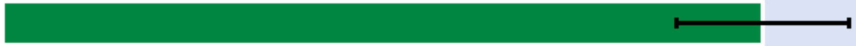
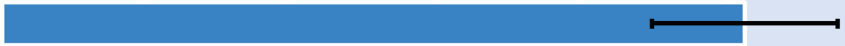
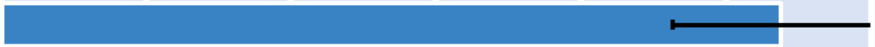
Ref	Question	1 2 3 4 5 6 7 Completely disagree Neutral Completely agree	No. of replies
Statements	Overall		
IE08xACSS01	The report of an analysed file provides easily understandable.		8
IE08xACSS02	The report of an analysed file provides useful information.		8

Table 5.25: Results for Malware Analyser - Free text question

Ref	Question	Reply
Free text question		
IE08xACST01	In addition to the low, medium, high, and severe status of a file, would you like to have additional status types. If yes, which?	• No. (4x) • No, the status alert system is very solid and understandable.

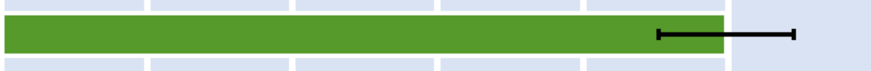
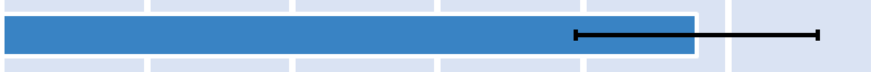
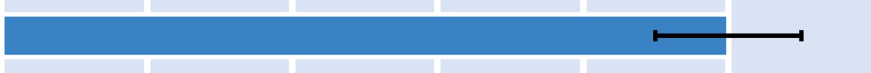
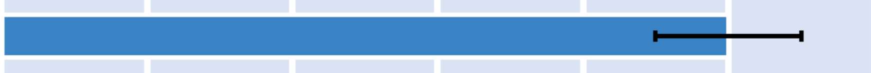
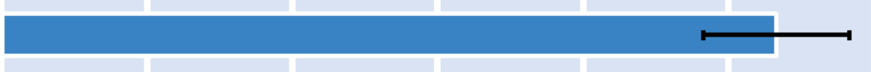
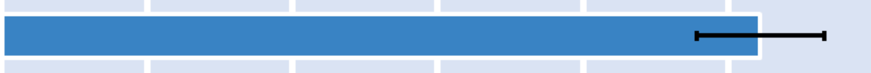
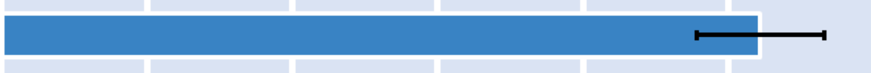
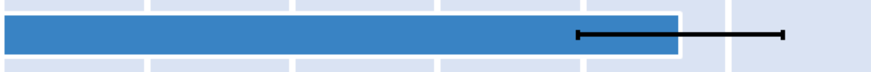
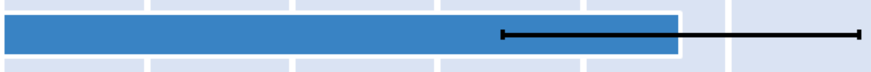
5.1.3.11 ALCAD

For the ALCAD, no bespoke questions were formulated.

5.1.3.12 Correlation Engine

The validation participants' replies for the statements on the Correlation Engine are summarized in Table 5.26 below. In general, they highly agree with the statements as indicated by an overall score of 5.99 (SD = 0.47). The highest agreement was recorded for the timeliness of the alerts (IE09xACSS04), the added value of the correlated alerts raised by the Correlation Engine (IE09xACSS05), and the trust in the raised alerts being accurate (IE09xACSS06). While still sufficiently high, the validation participants agreed the least with the alerts and rules being easily understandable (IE09xACSS01 and IE09xACSS07) as well as the events that trigged alerts being easy to see (IE09xACSS08). The standard deviation is overall quite small – only the SD for IE09xACSS08 is above 1.00 – indicating a homogenous answering pattern, especially when considering that the participants originate from three airports with different work environments.

Table 5.26: Results for Correlation Engine - Statements (some statements shortened compared to D6.2)

Ref	Question	1 Completely disagree 2 3 4 Neutral 5 6 7 Completely agree	No. of replies
Statements	Overall		
IE09xACSS01	The alerts generated by the Correlation Engine are easily understandable.		9
IE09xACSS02	The alerts generated by the Correlation Engine give enough information about the possible threat.		9
IE09xACSS03	The cyber-physical alerts generated by the Correlation Engine are relevant.		9
IE09xACSS04	The alerts generated by the Correlation Engine are received in a timely manner.		9
IE09xACSS05	The alerts generated by the CE have added value compared to the events coming from the other IEs.		9
IE09xACSS06	I trust the alerts generated by the Correlation Engine to be accurate.		9
IE09xACSS07	The rules are easily understandable.		9
IE09xACSS08	It is easy to see the events that trigged alerts from the Correlation Engine.		9

5.1.3.13 Investigation Tool

In Table 5.27, the participants' agreement to the statements on the SMS-I are presented separated by a) after the first exercise (pre-evaluation) and b) after all exercises (post-evaluation). Overall, the participants highly agree with the statements in the pre-evaluation (6.49, SD = 0.32) as well as the post-evaluation (5.84, SD = 0.62), albeit with a lower score. The same general trend can also be seen for the individual statements: The pre-evaluation always is at or above a score of six while the post-evaluation is lower, but still on the positive side of the rating scale. The most agreed to statements of the post-evaluation are that the SMS-I improves the efficiency and organization of the SOC (IE10ISEPS06), that the displayed graphics, metrics, and probabilities are trusted (IE10ISEPS07), and that the dashboard displays critical information (IE10ISEPS08) which all are rated at or above a score of six. The lowest agreement in the post-evaluation was recorded for the user friendliness of the interface at a still satisfying score of 5.43 (SD = 0.79). The standard deviation is quite small throughout all statements at a maximum value of SD = 0.98 for IE10ISEPS05.

To the free text question, only one reply was recorded highlighting the importance of the percentage metrics for the analysis of the presented data (see Table 5.28).

Table 5.27: Results for SMS-I - Statements

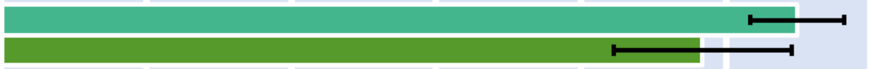
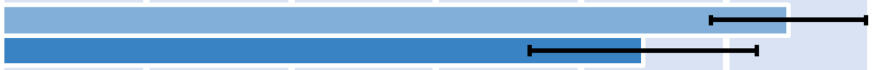
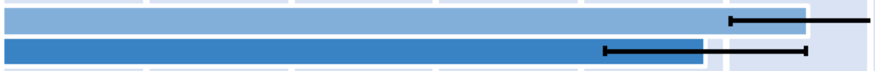
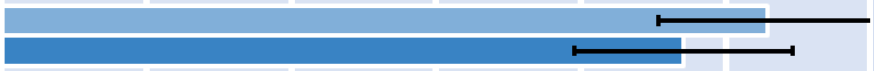
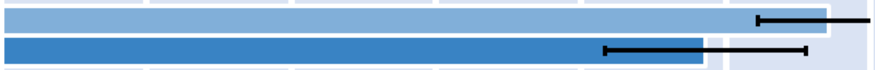
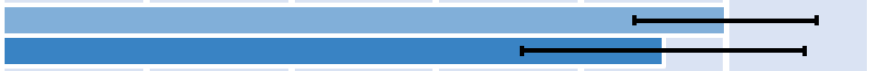
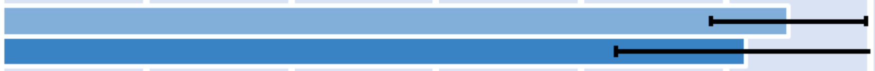
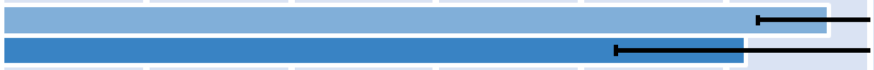
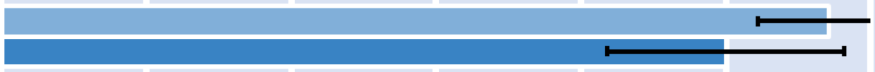
Ref	Question	1 Completely disagree 2 3 4 Neutral 5 6 7 Completely agree	No. of replies
Statements	Overall Pre Post		
IE10ISEPS01	The interface is user friendly.		7 7
IE10ISEPS02	The dashboards display useful information.		7 7
IE10ISEPS03	The dashboards simplify the analysis of open incidents.		7 7
IE10ISEPS04	The dashboards bring awareness to suspicious alerts or events.		7 7
IE10ISEPS05	The statistics and probabilities derived from machine learning are helpful during the decision making process.		6 7
IE10ISEPS06	The Investigation Tool improves the efficiency and organization of the SOC.		7 7
IE10ISEPS07	I trust the graphics, metrics, and probabilities displayed.		7 7
IE10ISEPS08	The dashboards display critical information.		7 7

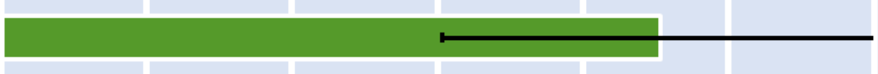
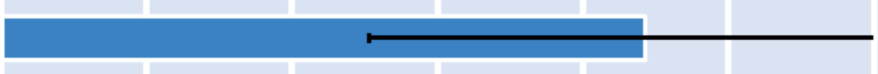
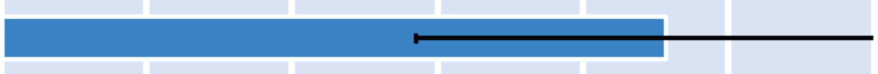
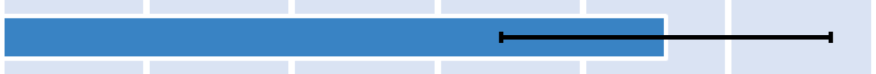
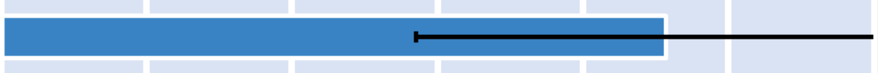
Table 5.28: Results for SMS-I - Free text question

Ref	Question	Reply
Free text question		
IE10ISEPT01	Which graphics or metrics are useful and/or essential to analyse the data?	• Percentage metrics.

5.1.3.14 Business Impact Assessment

The results for the statements on the BIA are depicted in Table 5.29. Throughout the overall score and the individual statements, an almost identical average agreement score – ranging from 5.43 for IE11INOVS01 to 5.57 for the other statements – can be observed. This indicates that the BIA is useful (IE11INOVS01), easy to use (IE11INOVS03) and that business processes and assets impacted by a threat (IE11INOVS02 and IE11INOVS04) are well understood. The relatively high standard deviation – the maximum is SD = 1.90 for IE11INOVS01 – points towards a heterogenous answering pattern which can be traced back to the diverse group of participants, familiar with three different work environments, that answered the questions.

Table 5.29: Results for BIA - Statements

Ref	Question	1 2 3 4 5 6 7 Completely disagree Neutral Completely agree	No. of replies
Statements	Overall		
IE11INOVS01	The BIA simulations are useful to predict the impact of cyber-attacks.		7
IE11INOVS02	BIA allows me to understand which business processes could be impacted by a threat.		7
IE11INOVS03	It is easy to run a BIA simulation and visualize the results.		7
IE11INOVS04	The BIA allows me to understand which assets could be impacted by a threat.		7

The participants’ replies to the two dropdown questions are summarized in Table 5.30. As can be seen, none of the browsers is clearly preferred to access the BIA (IE11INOVD01). Instead, the replies are evenly distributed across the “Chrome”, “Firefox”, and “Edge” browser options. Similarly, none of the BIA features is unanimously agreed to be the most useful to identify the threat propagation (IE11INOVD02). The most votes were recorded for the impact propagation path (named five times), followed by the description of the impacted process (named four times), and the ability to filter the results (named twice). None of the participants found the function to export the results useful to identify the threat propagation.

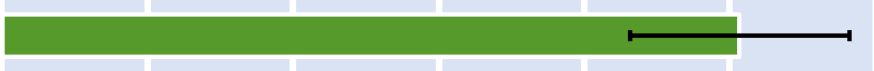
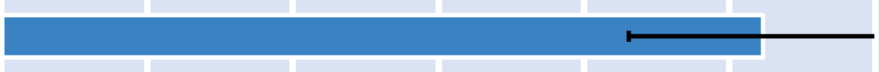
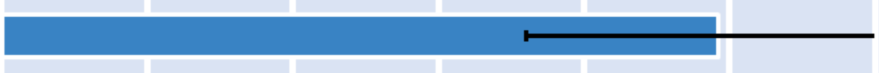
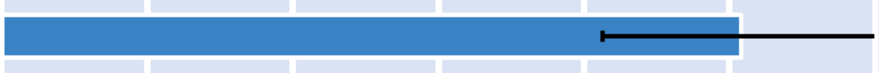
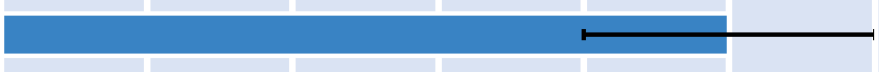
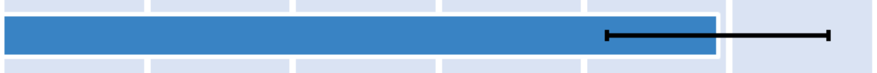
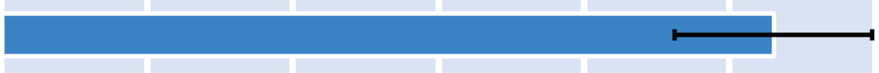
Table 5.30: Results for BIA - Dropdown questions

Ref	Question	Reply
Dropdown questions		
IE11INOVD01	Which browser is preferred to access BIA?	3x Chrome 3x Firefox 2x Edge 0x Internet Explorer
IE11INOVD02	Which BIA feature is the most useful to identify the threat propagation at your airport?	5x Impact propagation path 2x Filter results using graph view 4x Show description of the impacted process 0x Exporting BIA results

5.1.3.15 Impact Propagation Simulation

The validation participants' agreement to the statements on the IPS are presented in Table 5.31. Overall, there is a high agreement with the statements at a summarized score of 6.07 (SD = 0.75). As for the Business Impact Assessment, there is little variation in the agreement to the individual statements: All statements are rated around a score of six which is a very satisfying result. The participants agree the most with the IPS being a better tool than the impact propagation support currently in use at the airport (IE11xFHGS06, 6.30, SD = 0.68). While the understandability of the Network Model (IE11xFHGS02) and the mitigation options being well defined (IE11xFHGS05) received the lowest agreement at a score of 5.92, which is still a satisfying result. The standard deviation lies between SD = 0.68 for IE11xFHGS06 and SD = 1.32 for IE11xFHGS02, which is a normal range for the heterogenous group of participants asked.

Table 5.31: Results for IPS - Statements

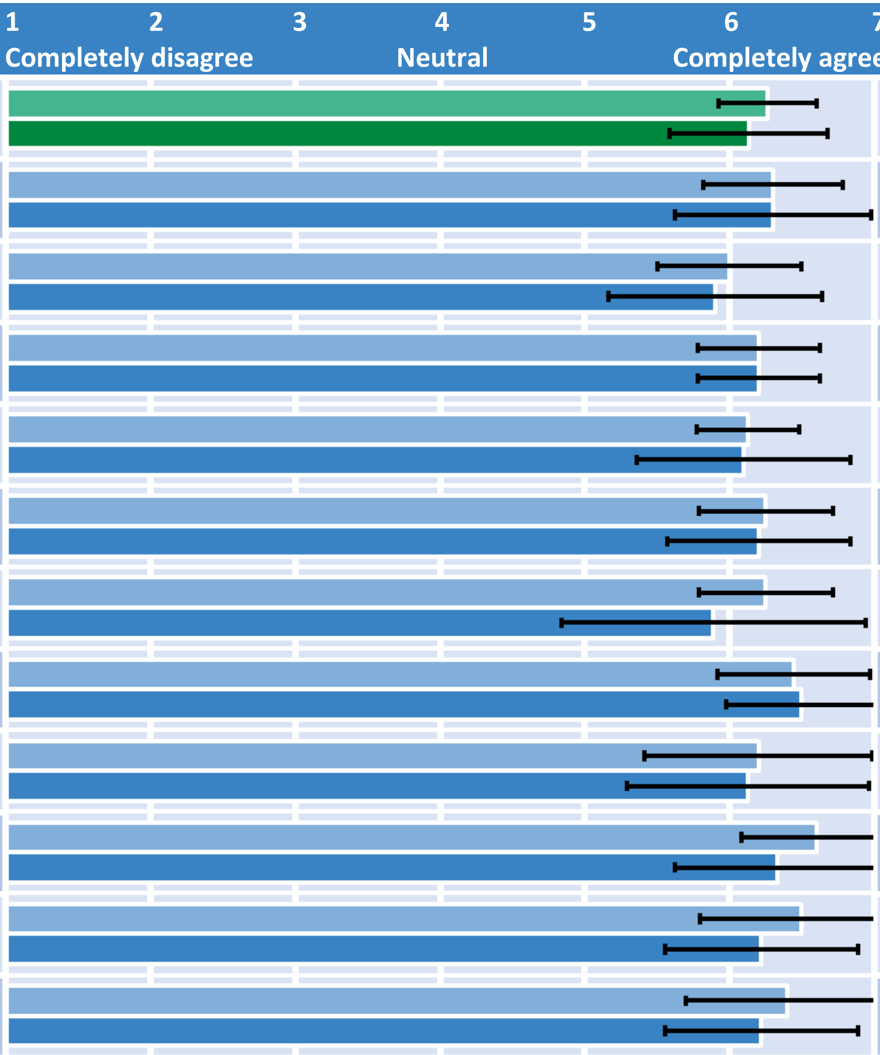
Ref	Question	1 Completely disagree 2 3 4 Neutral 5 6 7 Completely agree	No. of replies
Statements	Overall		
IE11xFHGS01	The Impact Propagation Simulation provides useful decision support.		13
IE11xFHGS02	The Network Model is easy to understand.		13
IE11xFHGS03	The Agent-Based Model provides additional detailed insights compared to the Network Model.		13
IE11xFHGS04	I would implement the Impact Propagation Simulation to improve my airport operation.		11
IE11xFHGS05	The mitigation options are well defined.		13
IE11xFHGS06	The Impact Propagation Simulation is a better tool than the existing, if any, impact propagation support.		10

5.1.3.16 Incident Management Portal

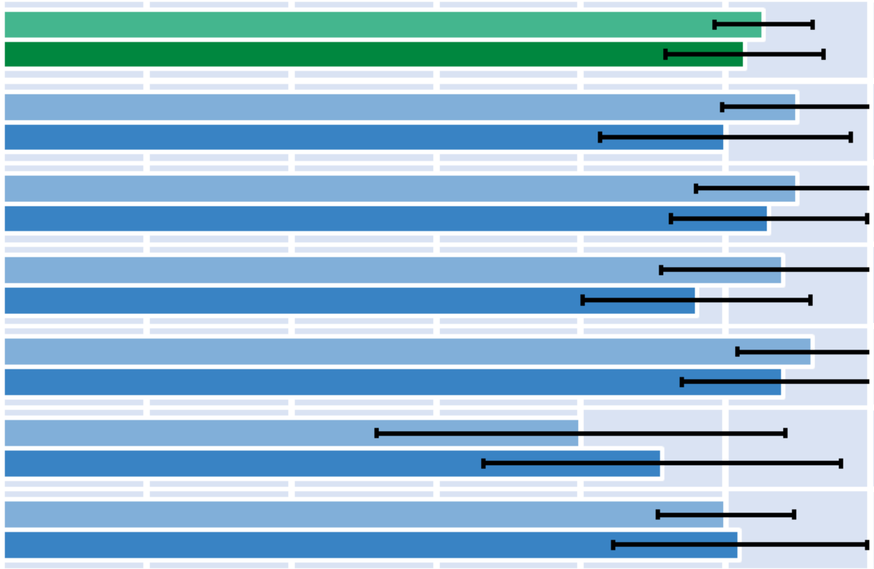
The results for the statements on the central interaction system for the SOC operator, the Incident Management Portal, are summarized in Table 5.32. Overall, there is a very high agreement with the statements after the first exercise (pre-evaluation, 6.26, SD = 0.34) as well as after all exercises (post-evaluation, 6.13, SD = 0.55). The scores for individual statements are all quite similar and lie around a value of six. There also is little variation between the pre-assessments and post-assessments. This all indicates that the IMP's GUI is well designed (IE12xACSS01, IE12xACSS03) and easy to use (IE12xACSS04 - IE12xACSS06, IE12xACSS13, IE12xACSS17). Furthermore, the IMP is found to be a great improvement compared to the operators' current situation (IE12xACSS09 - IE12xACSS12, IE12xACSS14). A relatively low, still sufficient, agreement was recorded for the number of alerts and incidents raised being on an acceptable level (IE12xACSS16) at a score of 5.00 (SD = 1.41) in the pre-evaluation that increased to 5.56 (SD = 1.24) in the post-evaluation. This increase of the agreement after handling all scenarios could be attributed to a high variation of the number of alerts raised in each of the five threat scenarios giving the participants a too negative impression after seeing only one scenario (i.e. in the pre-evaluation). This can also explain the relatively high standard deviation for this statement whereas it is quite small for the other statements.

Finally, the only additional feature requested (IE12xACST01, see Table 5.33) is the ability to have the current status of the alert visible, even if it has been escalated to the AOC.

Table 5.32: Results for IMP - Statements (some statements shortened compared to D6.2)



Ref	Question		No. of replies
Statements	Overall	Pre Post	
IE12xACSS01	The alert received are easily understandable.		10 10
IE12xACSS02	The alert received have enough information about the possible threat.		9 10
IE12xACSS03	The interface is user friendly.		10 10
IE12xACSS04	It's easy to go to the source of the alert and see the events in the Correlation Engine (graylog) from the IMP.		8 10
IE12xACSS05	It's easy to see the impact propagation of an alert by switching to the Impact Propagation Simulation.		8 10
IE12xACSS06	It's easy to see the business impact of an alert by switching to the Business Impact Assessment.		8 9
IE12xACSS07	The Incident Management Portal is useful.		9 10
IE12xACSS08	I would like to use the Incident Management Portal in my day-to-day work.		10 8
IE12xACSS09	The Incident Management Portal has added value compared to my current situation.		10 9
IE12xACSS10	The Incident Management Portal increases my situation awareness compared to my current situation.		10 9
IE12xACSS11	The Incident Management Portal reduces response times to alerts compared to my current situation.		10 9



Ref	Question		1 Completely disagree	2	3	4 Neutral	5	6	7 Completely agree	No. of replies
	Overall	Pre Post								
IE12xACSS12	The Incident Management Portal improves my efficiency compared to my current situation.									10 9
IE12xACSS13	It's intuitive to convert an alert into an incident and thereby send it to the AOC.									10 10
IE12xACSS14	The IMP improves my communication with the AOC compared to my current situation.									10 10
IE12xACSS15	The ability to close an incident is useful.									10 10
IE12xACSS16	The number of alerts and incidents does not increase my workload compared to my current situation.									9 9
IE12xACSS17	It's easy to filter the alerts and incidents.									10 10

Table 5.33: Results for IMP - Free text question

Ref	Question	Reply
Free text question		
IE12xACST01	I would like to have the following additional features:	• None. (2x) • Have current status of alert visible, even if it has been escalated to AOC.

5.1.3.17 Crisis Alerting System

In the following Table 5.34, the results for the statements on the CAS are presented. Overall, the validation participants highly agree with the statements, both in the pre-evaluation (6.55, SD = 0.43) and the post-evaluation (6.24, SD = 0.49). Also, for the individual statements, very high agreements were recorded, up to a complete agreement with the statement "The CAS is useful." (IE13xSATS05, 7.00, SD = 0.00) in the pre-evaluation. The lowest scores can be observed for the statements referencing improvements in the collaboration inside the AOC (IE13xSATS02) and with the SOC (IE13xSATS03) as well as the notification of passengers (IE13xSATS04). However, these are still very satisfying agreement scores. The standard deviation ranges from very small (SD = 0.00 for IE13xSATS05, pre-evaluation) to quite high (SD = 1.55, IE13xSATS03, pre-evaluation) which can be attributed to the homogenous group of operators that participated in the simulation validations.

The single additional feature requested (IE13xSATT01, see Table 5.35) is the ability to communicate back to the SOC (currently, information is only passed from the SOC to the AOC). This also is in line with the previous observation for the statement IE13xSATS03.

Table 5.34: Results for CAS - Statements (some statements shortened compared to D6.2)

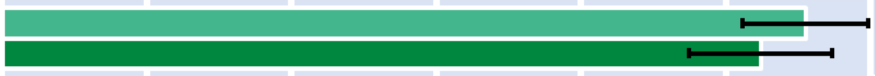
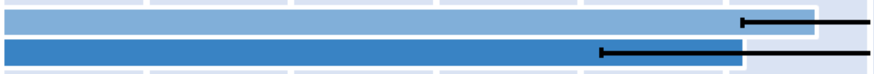
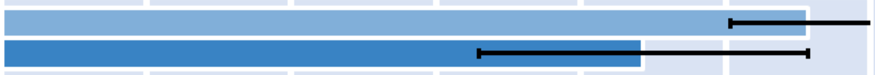
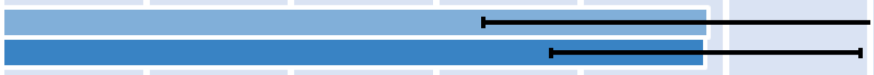
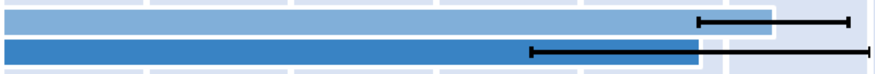
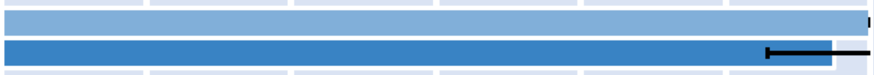
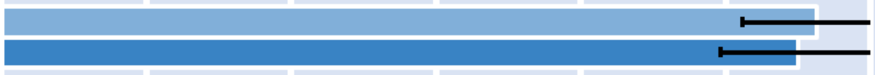
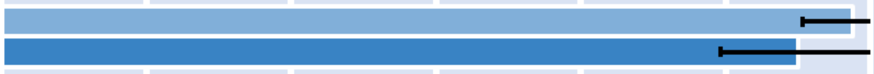
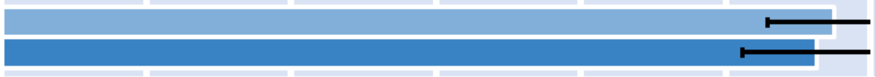
Ref	Question	1 Completely disagree 2 3 4 Neutral 5 6 7 Completely agree	No. of replies
Statements	Overall		
IE13xSATS01	The CAS improves the collaboration between the AOC and LEAs compared to my current situation.		8 8
IE13xSATS02	The CAS improves the collaboration inside the AOC compared to my current situation.		7 7
IE13xSATS03	The CAS improves the collaboration between the AOC and the SOC compared to my current situation.		8 7
IE13xSATS04	The CAS improves the notification of passengers affected by a specific incident compared to my current situation.		6 6
IE13xSATS05	The CAS is useful.		7 8
IE13xSATS06	The way that the CAS collects and visualizes the operational information from multiple sources is useful.		8 8
IE13xSATS07	CAS provides a user-friendly and intuitive graphical user interface.		8 8
IE13xSATS08	CAS informs AOC operators about the current incidents (that are related to the airport) and their possible impact.		8 8

Table 5.35: Results for CAS - Free text question

Ref	Question	Reply
Free text question		
IE13xSATT01	I would like to have the following additional features:	• None. (2x) • Two-point voice communication for the provision of clarifications between teams and acknowledgement of notification reception between teams. • Sending of SMS to and from SOC. • Possibility of sending messages back to SOC.

5.1.3.18 CyberRange

In the following Table 5.36 and Table 5.37, the validation participants' replies to the questions on the CyberRange are presented. Since the participants highly agree that the CyberRange is realistic enough for the simulation of the scenarios (IE14xACSS01), the free text question asking for necessary improvements was not displayed to any participant.

Table 5.36: Results for CyberRange - Statements

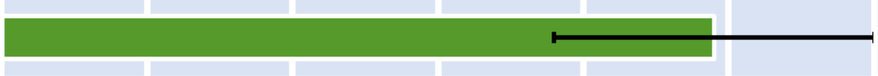
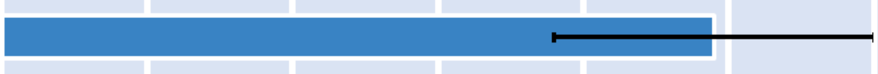
Ref	Question	1	2	3	4	5	6	7	No. of
		Completely disagree			Neutral			Completely agree	replies
Statements	Overall								
IE14xACSS01	The replication of the airport environment is realistic enough for the simulation of the scenarios.								10

Table 5.37: Results for CyberRange - Free text question

Ref	Question	Reply
Free text question		
IE14xACST01	What is needed to increase the realism of the airport environment?	*No participant disagreed with the statement.*

5.1.3.19 Baggage Handling System

Equal to the questions on the CyberRange, the only statement answered for the Digital Twin of the BHS (see Table 5.38) aimed at the realism of the emulation (IExxxALSS01). As the validation participants highly agree that the emulation of the BHS was realistic enough (5.88, SD = 1.00), they were not presented with the free text question asking for necessary improvements (IExxxALST01, see Table 5.39).

Table 5.38: Results for BHS - Statements

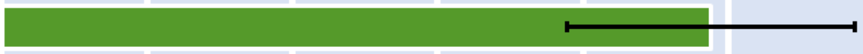
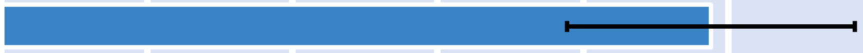
Ref	Question	1 Completely disagree 2 3 4 Neutral 5 6 7 Completely agree	No. of replies
Statements	Overall		
IExxxALSS01	The simulation of the Baggage Handling System is realistic enough for the simulated scenarios.		8

Table 5.39: Results for BHS - Free text question

Ref	Question	Reply
Free text question		
IExxxALST01	What is needed to increase the realism of the Baggage Handling System?	*No participant disagreed with the statement.*

5.2 Key Performance Indicators

Following the presentation of the subjective results in the previous section, the objective results of the simulation validation are summarized in this section in the form of Key Performance Indicators. The KPIs to be calculated were laid out in Table 4.13 of D6.2 (1) and determined based on logs recorded during the simulation validation and data gathered in pre- or post-validation experiments. The individual methods used for each SATIE Tool are described in the following sections and the results are summarized in Table 5.40 below. In deviation to the validation plan outlined in D6.2 (1), some of the KPIs (marked with “N/A” in the table) were no longer applicable or could not be calculated due to insufficient data.

Table 5.40: Summary of validation-related KPIs defined in D6.2 (1) (CO = These results are confidential and therefore reported in deliverable D1.4 (12); N/A = KPI could not be calculated)

KPI	Definition	Unit	ComSEC	UAC	ADPR	Secured ATM Services	TraMICS	BP-IDS	Malware Analyser	ALCAD	Correlation Engine	SMS-I	BIA	IPS	IMP	CAS
(Incident / Intrusion / Anomaly / Threat) Detection Rate	$\frac{\text{Correct alerts}}{\text{Potential alerts (incl. undetected)}}$	%	100	See section 5.2.5	CO	N/A	100	CO	N/A	N/A	N/A				100	
False Positive Rate	$\frac{\text{False positive alerts}}{\text{All raised alerts}}$	%	0		CO	N/A		CO	N/A	0	0				0	
Equal Error Rate	*Defined in section 1.4 of D4.2* (4)	%					3.87									
Latency	Time from occurrence of intrusion / anomaly / threat until being displayed in the IMP/CAS	s							<300							
Time until Security Situation Rating Update (TraMICS)	Time between the current and the previous update of the security situation rating	s					60									
Computational Time for Simulation	Time required to process new alert and display result	s											11	15		
Time to Synchronize	Time required to present new information	s										<90				0.5

KPI	Definition	Unit	ComSEC	UAC	ADPR	Secured ATM Services	TraMICS	BP-IDS	Malware Analyser	ALCAD	Correlation Engine	SMS-I	BIA	IPS	IMP	CAS
Time to Qualify New Alerts		s										<20				
Time to Respond	Time from occurrence of incident until initiation of response (marking as incident, forward to first responders, …)	s													368	8
Automatic Decision Support Suggestions	$\frac{\text{Alerts with decision support}}{\text{Total alerts}}$	%													N/A	100
Automatic Mitigation Support Suggestions	$\frac{\text{Alerts with mitigation support}}{\text{Total alerts}}$	%													N/A	100

5.2.1 Risk Integrated Service

There were no validation specific KPIs to be calculated for RIS as the risk assessment was not dynamic during the scenarios. General, not validation specific KPIs will be reported in the SATIE project’s final report, deliverable D1.4 (12).

5.2.2 Vulnerability Intelligence Platform

There were no validation specific KPIs to be calculated for VIP as the vulnerability assessment was not dynamic during the scenarios. General, not validation specific KPIs will be reported in the SATIE project’s final report, deliverable D1.4 (12).

5.2.3 Gestion Libre de Parc Informatique

There were no validation specific KPIs to be calculated for GLPI. General, not validation specific KPIs will be reported in the SATIE project's final report, deliverable D1.4 (12).

5.2.4 Secured Communication on the BHS and Business Process-based Intrusion Detection System

The BP-IDS and ComSEC were evaluated using the Scenario #4. Specifically, the evaluation used a testbed with three virtual airport systems represented in the simulation platform (the FIMS [Flight Information Management System], the AODB and BHS) provided by Alstef[2]. The evaluation assessed the KPIs of the ComSEC and BP-IDS by validating BHS service operations. The Key Performance Indicators for the BP-IDS are confidential and therefore reported in the final report, deliverable D1.4 (12).

Table 5.41 shows the detection results for ComSEC to identify integrity and replay anomalies. Integrity anomalies are packets that had their data changed while in transit between the sender and the receiver. Replay anomalies are packets that were sent more than once to the recipient (retransmitted). ComSEC monitored 18.736.351 packets and raised a total of 14876 alerts. From the raised alerts, 220 were related with integrity problems, while 14656 were related with retransmission of network packets. During the evaluation ComSEC had 0 false negatives, this shows that ComSEC detected all anomalies and that it is a very accurate solution for assessing the integrity of communications. This is due to ComSEC being deterministic when assessing integrity. For each packet sent from a machine ComSEC is connected, it will send a control packet with a signature of the packet. The non-correspondence of the signature or absence of the control packet on a receiving ComSEC, will always generate an alert. Regarding false positives, ComSEC shows a false positive rate (FPR) of 3% for detecting integrity problems, and a 0.88% for detecting packet retransmission. Regarding integrity detection, this FPR is related with data loss during the transmission of control packets between BHS machines. The control packets are UDP packets, which is a connectionless protocol, and therefore have no guarantee of delivery, ordering, or duplicate protection, however taking into account the reliability of current networks, a high UDP packet loss rate is unlikely (so ComSEC will display little FPR).

Table 5.41: ComSEC integrity detection results

Alert type	Total alerts	Correct Alerts	False negatives	False positives	Accuracy	False Positive Rate
Integrity	220	213	0	7	100%	3%
Uniqueness	14527	14527	0	0	100%	0%
Both	14747	14740	0	7	100%	0%

[2] https://www.alstef.com/Baggage-handling-and-screening

The Key Performance Indicators for the Business Process-based Intrusion Detection System are confidential and will therefore be reported in deliverable D1.4 (12).

5.2.5 Unified Access Control

The Unified Access Control solution is primarily revolving around the face recognition from Augmented Vision. This face recognition is currently performed with standard IP cameras. In the context and use case of SATIE, it is impossible to determine the accuracy of the system as it is the combination of two biometric identification systems. More importantly, the face recognition accuracy is subject to multiple factors that do not reside only in the system such as:

- Lighting conditions: Ceiling lights vs wall-mounted lamp, difference of lighting between days and nights or between yearly seasons and weather conditions.
- Quality of the enrolment photo.
- Camera resolution, mounting heights and angle and image distortion (e.g. fisheye).
- Behaviour of the employee: The attitude of the user will have a determinant factor in the true identification rate, as face angle (horizontal or vertical), speed of walking, face expression (smiling, talking, etc.), and face attributes (sun-glasses, face mask, hat, etc.) will all have an impact on the biometric score generated.

Nonetheless, Augmented Vision in SATIE is set with a biometric threshold of 2500. This means that any comparison between faces with a score below 2500 will not generate an alert (higher scores indicate a better biometric match). This biometric score is calculated by IDEMIA’s algorithm and the value 2500 represents a theorical value for a False Acceptance Rate (FAR) of 10^{-2} or 0,01%.

In addition, the Augmented Vision algorithm is regularly submitted to external laboratories for performance evaluation under precise conditions and a large dataset. In Figure 5.1 below, the results of accuracy tests performed by the National Institute of Standards and Technology (NIST) on IDEMIA face recognition algorithms for different dataset over the past years are presented. The scale is showing the False Negative Identification Rate (FNIR) for a fixed False Positive Identification Rate (FPIR) of 0,01%. Results of the latest submissions for 2021 shows that the accuracy of the face recognition algorithm (equalling 1-FNIR) is above 99,99% for three types of datasets.

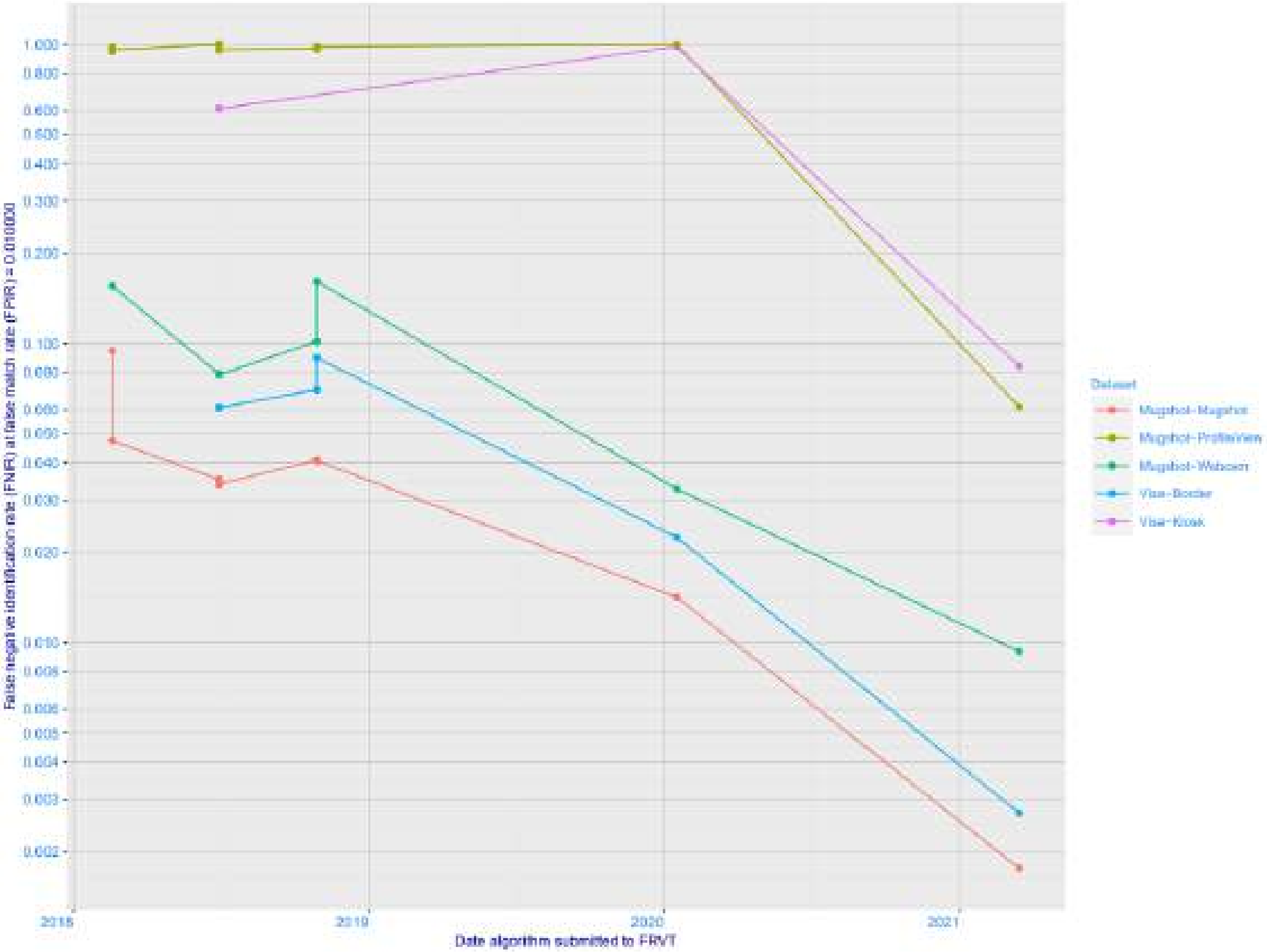


Figure 5.1: Evolution of accuracy for IDEMIA algorithms for three datasets from 2018 to present

5.2.6 Anomaly Detection on Passenger Records

The Key Performance Indicators for the ADPR are confidential and therefore reported in the final report, deliverable D1.4 (12).

5.2.7 Secured ATM Services

As stated in Table 5.40, the following Key Performance Indicators are assigned to the Secured ATM Services:

- (Incident/Intrusion/Anomaly/Threat) Detection Rate.
- False Positive Rate.

The Secured ATM Services in the SATIE Solution provides logging messages to the Correlation Engine, including statistics data about successful and unsuccessful authentication attempts and service access requests. The Correlation Engine takes these statistics data as an input to detect anomalies.

Due to this simulation design, the following has to be stated:

- Incident detection is not performed by Secured ATM Services, but by the Correlation Engine, taking statistics input from Secured ATM Services logging output.
- Incidents are strictly defined by formulas. For example:
  - A “Brute Force Authentication Attack” is defined by the rate of unsuccessful service authentication attempts to the Secured ATM Services being above a certain number per second.
  - A “Denial of Service Attack“ is defined by the rate of successful service access requests to the Secured ATM Services being above a certain number per second.
- Due to this exact definition of attacks, the Correlation Engine was able to detect all attacks, so
  - The Incident Detection Rate was observed to be 100%, as expected.
  - The False Positive Rate was observed to be 0%, as expected.

During the simulation sessions, while playing the Scenario #5, the number of Authentication Attempts and Service Access Requests presented in Table 5.42 have been reported by the Secured ATM Services.

Table 5.42: Secured ATM Services reported figures and detection thresholds

Counter	Normal load	Attack load	Brute Force attack threshold	Denial of Service attack threshold
Authentication Attempt Rate	0 / second	1 / second	4 / minute	N/A
Service Access Request Rate	0/ second	638 / second	N.A.	60 / minute

5.2.8 Traffic Management Intrusion and Compliance System

The definitions and results of the TraMICS's Key Performance Indicators are reported in deliverable D4.2 (4). They have been measured during the tests in the specific simulation environments described as well in deliverable D4.2 (4). The more generic KPI are furthermore included in the summary presented in Table 5.40.

5.2.9 Malware Analyser

Using the log data for the detected malwares from the simulation validation of Scenario #3 and Scenario #5, it was verified that the time until detection was always less than five minutes. The measurement is done by calculating the time between the attack (i.e. the download of the malware) and the time of the reception of the alert by the Correlation Engine. There was insufficient data to reliably calculate a detection rate or a false positive rate.

5.2.10 ALCAD

The KPIs for ALCAD were verified in the simulation platform as part of WP4, please see D4.3 (5) for more details. As verifying the false positives rates requires more data points, verification during a small number of simulation validations yields not much information. Still, it can be said that during the simulation validations, the time until detection was always less than 5 minutes and no false positive alert was raised.

5.2.11 Correlation Engine

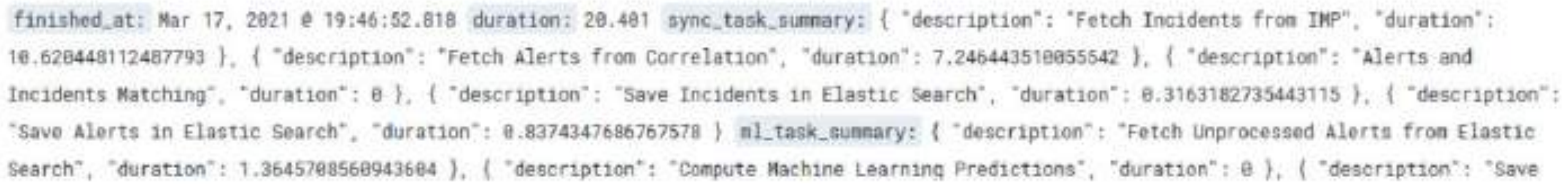
During the simulation validations, no false positive alert was raised. A dedicated detection rate could not be calculated based on the collected data.

5.2.12 Investigation Tool

The "Time to Synchronize" is measured since the Synchronization Mechanism is triggered up until the new event, alert, and incident data is stored in the Elastic Search. This process is composed of several sub-steps: fetching incidents from the IMP, fetching alerts/events from the Correlation Engine, pre-processing and validating all data and, finally, saving all data in the Elastic Search database.

The "Time to Qualify" new alerts is measured since the Machine Learning Engine is triggered up until the Machine Learning results are stored in the Elastic Search. This process is composed of several sub-steps: fetching all unprocessed alerts (by ML) from the Elastic Search, computing the Machine Learning predictions for every unprocessed alert, and storing all results in the Elastic Search database.

The Machine Learning Engine is immediately executed after the Synchronization Mechanism. These processes and their corresponding sub-steps are recorded and stored in the Elastic Search for debugging and auditing purposes. An example for such a log file is depicted in Figure 5.2.



```
finished_at: Mar 17, 2021 @ 19:46:52.818 duration: 20.481 sync_task_summary: { "description": "Fetch Incidents from IMP", "duration":
10.620448112487793 }, { "description": "Fetch Alerts from Correlation", "duration": 7.246443510055542 }, { "description": "Alerts and
Incidents Matching", "duration": 0 }, { "description": "Save Incidents in Elastic Search", "duration": 0.3163182735443115 }, { "description":
"Save Alerts in Elastic Search", "duration": 0.8374347686767578 } ml_task_summary: { "description": "Fetch Unprocessed Alerts from Elastic
Search", "duration": 1.3645708560943604 }, { "description": "Compute Machine Learning Predictions", "duration": 0 }, { "description": "Save
```

Figure 5.2: Example of a synchronization/Machine Learning execution log

Note that these processes are very dependent of external parameters, such as the network latency. However, in the tests performed, the “Time to Synchronize” was always less than 90 seconds, and the “Time to Qualify” was always less than 20 seconds, which is a very acceptable performance of the SMS-I tool.

5.2.13 Business Impact Assessment

Figure 5.3 shows the performance results for BIA. The performance tests, measured the time BIA takes to perform impact assessments in Scenario #4. As can be seen, BIA’s impact assessments can be divided into two main computational parts: setup and impact simulation. The setup part (marked in grey). takes around five seconds and its main objective is to extract the necessary input to perform impact simulations. This involves extracting data from other SATIE Tools. From GLPI REST API, the BIA extracts asset data in around two second (marked in dark blue). From BP-IDS REST, the BIA extracts business process data in around 1 second. The remaining 2 seconds of the setup time is spent on parsing the extracted data and arranging in the BIA knowledge database accepted format. After the setup part is performed, the BIA is ready for performing impact simulations. The impact simulation part takes around 6 seconds (marked in light blue and yellow). This simulation is divided into computational moments, one is displaying the network topology in the BIA homepage which is negligible (38 milliseconds), the second step is performing the impact simulation according to the user’s input and takes around 6 seconds. This results in an acceptable performance of the BIA software, five seconds to start the application and six seconds to perform the simulation.

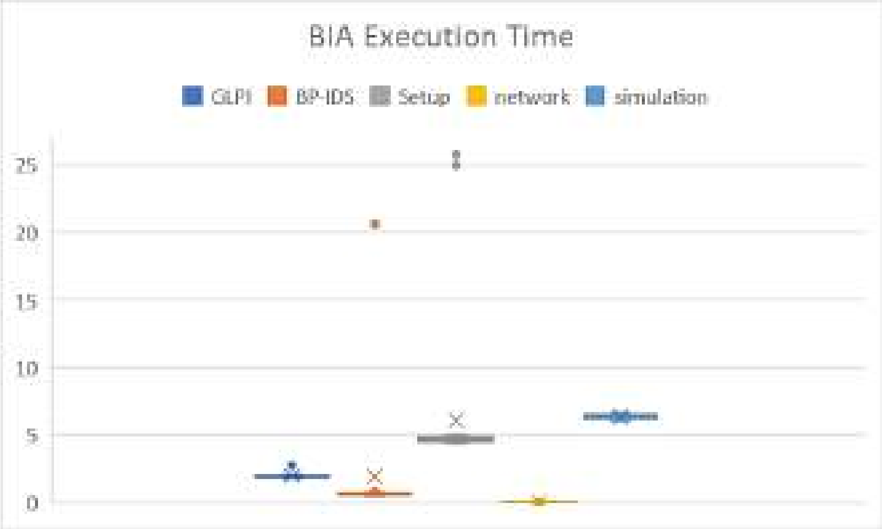


Figure 5.3: BIA computational time

5.2.14 Impact Propagation Simulation

The IPS’s KPI in Table 5.40is defined as the average of the simulation time of the FastNet and of the Network Model (see Table 5.43). The ABM has been excluded from this estimate as it is highly variable and does not contribute to the immediate response to an incident. Further, the simulation time of ABM is dependent on the resources available on the CyberRange which is quite limited for each VM which means that the simulation time is not representative. Also, some algorithms used in the ABM are currently improved to reduce the computation time. The functionalities of all three IPS simulation engines is described in D5.1 (13).

Table 5.43: Average times to respond for the IPS's internal simulation engines

IPS internal simulation engine	Average time to respond
FastNet	0.02 seconds
Network Model	30 seconds
Agent-Based Model (ABM)	100 seconds (highly dependent on the # of time steps)

5.2.15 Incident Management Portal

Using the log files recorded during the simulation validation, it was determined that, during the simulation, all alerts classified as incidents by the operators were real threats. Hence, the detection rate of the IMP is 100% while the false positive rate is 0%.

5.2.16 Crisis Alerting System

In the following Table 5.44, the metrics regarding the CAS functionalities are documented. All interactions of the CAS with the IMP were very fast, due to the web service technology used, resulting in information being received by the CAS in less than 1 second. The first CAS users' actions were performed in less than 10 seconds on average. These actions included

- Alarm inspection,
- Initial notification of public safety agencies,
- Alarm status update, and
- SMS or Email notification of stakeholders.

All the alarms received were supported by decision support and mitigation support suggested actions, according to the AOC operators operating procedures.

Table 5.44: KPIs for CAS functionalities

Actions	Results
Incident send by IMP and received by the CAS	Average time: 0.5 seconds
Time to Synchronize	Average time: 0.5 seconds
First user action on alarm in the CAS	Average time: 8 seconds
Automatic Decision Support Suggestions	Percentage of alarms with decision support suggestions: 100%
Automatic Mitigation Support Suggestions	Percentage of alarms with mitigation support suggestions: 100%

5.2.17 CyberRange

There were no validation specific KPIs to be calculated for the CyberRange. General, not validation specific KPIs will be reported in the SATIE project's final report, deliverable D1.4 (12).

5.2.18 Emulated Baggage Handling System

There were no validation specific KPIs to be calculated for the Digital Twin of the BHS. General, not validation specific KPIs will be reported in the SATIE project's final report, deliverable D1.4 (12).

6 Discussion

In the following the subjective and objective results of the simulation validation reported in the previous chapter 5 are discussed and specific findings are deduced. This chapter is divided into the discussion of the SATIE project's objectives in section 6.1 based on the results of the standard validation questionnaires (see section 5.1.1), the general validation questions (see section 5.1.2), and the KPIs (see section 5.2), the discussion of SATIE Tool-specific findings in section 6.2 deduced from the bespoke validation questions (see section 5.1.3) and the KPIs (see section 5.2), and a summary of all conclusions in section 6.3.

6.1 Validation objectives

As laid out in D6.2 (1), the results of the simulation validation are used to determine how well six of the twelve SATIE Objectives are fulfilled. These objectives are listed in Table 6.1. For the discussion of each objective, different parts of the results are relevant, as defined by the Description of Action (DoA) (14) and shown in the table. In the following sections, the findings for each objective are summarized.

Table 6.1: SATIE Objectives relevant for the simulation validation and associated metrics

Objective	Objective Description	Metric (KPI & Assessment)
O4	Improve **physical threat prevention and detection**, against access to sensitive areas and passenger control	• Detection and false positive rate.
O5	Improve **cyber threat detection** on airports IT and OT networks	• Time until detection. • Spoofing/attack detection rate.
O6	Improve **correlation of cyber and physical threats** to facilitate human analysis and decision-making	• Detection and false positive rate. • Time to qualify an incident. • Time to response and remediation. • Questionnaires and debriefing.
O7	Improve **incident response and impact mitigation** for a reduced and unified time to response	• Time to qualify impact.
O8	Carry out **operational demonstrations** at TRL7 in real conditions at three different international airports	• Questionnaires and debriefing.
O11	Provide **efficient and cost-effective solutions** for airport security	• Questionnaires and debriefing.

6.1.1 Objective O4

In order to determine the improvement in physical threat detection, the KPIs of the physical threat prevention and detection systems, i.e. the Unified Access Control, the Anomaly Detection on Passenger Records, and the TraMICS, have to be analysed. From the results presented in Table 5.40, it can be seen that the detection rates for all three SATIE Tools are satisfyingly high while the false positive rates are very low. Hence, it is deduced that objective O4 is fulfilled.

6.1.2 Objective O5

Similar to the detection of physical threats, the KPIs for the cyber threat prevention and detection systems are used to deduce the improvement in the detection of cyber threats. The relevant SATIE Tools therefore are the ComSEC, the Secured ATM Services, the BP-IDS, the Malware Analyser, and the ALCAD. In light of the results presented in section 5.2, this objective can also be regarded as fulfilled. Even with the limited data collected during the simulation validation and in subsequent tool-individual experiments, high detection rates (e.g. up to 100% for the ComSEC) and very low false positive rates (mostly close to or at 0%) were calculated.

6.1.3 Objective O6

To discuss the improvements made in the correlation of physical and cyber threats, the subjective data derived through the simulation validation questionnaire are used in addition to the objective KPIs. Specifically, the participants' assessment of their mental workload, the results of the general validation questions (in particular GS10 and GS11), the detection rate and false positive rate of the Correlation Engine and the time to respond of the IMP are considered.

The first finding is that the mental workload required to perform various tasks (see section 5.1.1.3) is adequately low. This indicates that the operators were able to easily find the sought information and that they were well understandable as well as that the tools at hand allowed for a low-effort decision making. These findings are supported by the high agreement to the general statements. From the high score for the statements GS10 ("The use of the unified SATIE Solution increases the efficiency compared to my current system(s).") and GS11 ("The use of the unified SATIE Solution increases the efficiency compared to using the unconnected IEs and no CE."), it can furthermore be seen that the unified SATIE Solution is preferred over the current system or even the unconnected SATIE Tools without the information being correlated by the Correlation Engine. It is therefore concluded that the Correlation Engine is an integral part of the SATIE Solution. Together with the satisfying detection rate and false positive rate of the Correlation Engine and the low time to respond, also objective O6 can be regarded as highly fulfilled by the SATIE Solution.

6.1.4 Objective O7

The improvements in incidence response and impact mitigation are provided by the central alerting systems (IMP and CAS) on the one hand and by the SMS-I, BIA, and IPS as supporting systems on the other hand. Hence, discussion of this objective is based on the KPIs of these systems and is complemented by the results of the general validation questions.

As can be seen from Table 5.40, newly received alerts and incidents were quickly processed (within a maximum of 20 seconds of the SMS-I) and the operators also swiftly reacted to new alerts as is evident in the times to respond for the IMP and the CAS. Additionally, all of the alerts displayed in the CAS were accompanied by a simulation of the impact propagation assisting the operator in the impact mitigation. Looking at the subjective opinion of the operators expressed in the agreement to the general validation questions (see Table 5.5), the participants feel that they were able to react quicker to physical and cyber threats compared to their current system (statements GS8 and GS9). In summary, objective O7 is fulfilled by the SATIE Solution.

6.1.5 Objective O8

Currently, this objective cannot be fully discussed as the demonstrations at the Athens, Milan, and Zagreb airports are yet to be carried out and reported on. However, the results collected during the simulation validation are used to determined changes that are necessary for the demonstrations to be successful. The found implications for the demonstrations are reported in chapter 7.

6.1.6 Objective O11

For the discussion of the final objective, the efficiency and cost-effectiveness of the SATIE Solution, the data gathered through the general validation questions of the simulation validation questionnaire are used. As can be seen, the participants feel that they are able to detect and mitigate physical threats and cyber threats faster compared to their current system. Furthermore, when directly asked if they think that the SATIE Solution increases the efficiency compared to their current system (GS10), they replied very positively. The participants also judge the *unified* solution - with the individual tools connected through the Correlation Engine - as more efficient than all of the remaining SATIE Tools on their own. This proves the efficiency of the SATIE Solution and also highlights how integral the Correlation Engine is for the solution to achieve its objectives. The cost-effectiveness of the SATIE Solution is evident in the participants' neutral agreement to statement GS14 ("The solution boosts revenues."). While this may at first seem as an argument against the SATIE Solution, the finding that the revenue is expected to stay the same together with the benefit the solutions provides outlined in the previous sections, results in a higher cost-effectiveness compared to the system currently in place at the airport. Moreover, increasing the revenue of the airport was not one of SATIE's objectives and therefore not specifically considered in the development.

6.2 SATIE Tools

In addition to the findings for the SATIE Solution in general (described in the previous section), conclusions for each individual SATIE Tool are drawn from the results of the bespoke validation questions and the Key Performance Indicators. These are presented in the following sections.

6.2.1 Risk Integrated Service

The answers to the bespoke validation questions for RIS showed an overwhelmingly positive response. The lowest scoring question was about how useful this risk assessment tool is compared to ones already in place at the airport. This indicates that the idea of having a risk assessment tool in the airport is not innovative on its own, nor was that anticipated to be. However, it is a great indication that still the answers were positive, meaning that this tool is more useful.

It requires analysing the other responses to determine where the tool was the most useful and where there may be room for improvement. The second 'worst' responded to question was about using the what-if scenarios to identify countermeasures to take. At first glance it may seem like these what-if scenarios could therefore be improved, the slightly lower responses are most likely due to the fact that these what-if scenarios were not fully demonstrated to the operators and they did not get to use them. This was just a matter of a lack of time, during both the training sessions and the simulation validation. It was important to allow adequate time for the operators to use each tool, and thus it was decided to sacrifice the what-if scenario part of the RIS tool. These what-if scenarios allow one to modify the responses about how well particular security measures are in place to see simulated risk results and therefore determine if the risks to an airport operation would improve as assumed, or whether particular critical assets would become less vulnerable, etc. Therefore, the risk managers can use these simulations to determine how to apply best their time and effort to actually reduce risks in the airport environment. Hence, with these answers, it is not clear whether there really should be improvement in these what-if scenarios or whether there just wasn't adequate time for the operators to try them and thus their evaluation was sacrificed as a result. Strong evidence to suggest the latter is that in the open question about what kind of results are missing, all responders indicated none. Therefore, they could not think of anything that was missing.

The best performing question was about the participants trusting the results to be accurate. This is a great response, because there is no way to prove the accuracy of the results. There is no absolute risk associated with a particular asset or threat, but rather depends highly on the methodology used and how those risks are calculated. Therefore, the trust in the accuracy of the results seems to indicate trust that this methodology is a great way to understand risks in the airport environment.

6.2.2 Vulnerability Intelligence Platform

The VIP's purpose is to gather information on known vulnerabilities associated with the airport's assets so that the operators can easily identify potential points of attack. Therefore, it is important that the shown vulnerabilities are up to date, easy to understand, and that the operators trust the displayed information. As can be seen from the replies to the bespoke validation questions (see section 5.1.3.2), all of these aspects are highly fulfilled by the Vulnerability Intelligence Platform. The tool clearly is fit for purpose and no issues have to be addressed.

6.2.3 Gestion Libre de Parc Informatique

The GLPI is the central system that maintains an inventory of all assets in the airport as well as associated data (such as the vulnerabilities identified by the VIP) and provides these to other tools in the SATIE Solution. Just as with the VIP, it is therefore vital that the information is up-to-date, accurate, and easy to understand. All of this is confirmed by the validation participants (see bespoke validation questions in section 5.1.3.3). It is furthermore concluded from the results, that information in an alert raised to the IMP is sufficient to identify the impacted asset and that accessing the associated information in GLPI directly is highly beneficial, although all immediately necessary information during an attack are also present in the IMP directly. The validation participants also see no need for additional information to be provided by the GLPI.

6.2.4 Secured Communication on the BHS

The ComSEC validation on the simulation platform (section 5.2.4) has shown that ComSEC has 100% accuracy rate, with very little false positives (3%) for identifying security problems related to the BHS communications. In this validation, all BHS systems were protected by ComSEC, totalling seven BHS systems. The devices protected are: one AODB, one sortation unit, two PLCs, one Supervisory Control And Data Acquisition (SCADA) system, one manual coding station, and one HMI. Moreover, ComSEC received positive feedback collected from the bespoke questions, asked to the SOC operators, related to ComSEC monitoring of the BHS (Section 4.10). This shows that the cyber threat detection alarms raised by ComSEC were correctly handled by SOC operators, making it an adequate detection tool for fulfilling objective O5 “Secure IoT communications in the airport BHS for higher confidentiality and integrity level exchanges”.

6.2.5 Unified Access Control

All tests of the Unified Access Control were successfully performed and the results have been in line with the expectations. The accuracy of the face recognition algorithm (equalling 1-FNIR) was calculated as above 99,99%. During the simulation validation participants rated this Innovation Element as one of the systems which stood out. The bespoke validation questions for the Unified Access Control were rated very positive. Especially the tailgating detection received very positive ratings from the participants. The system was rated as rather easy to integrate with existing systems and multiple ideas for areas where the face recognition capabilities may also be employed have been given by participants (e.g. all places that only authorized personnel should be able to access and specifically the gates, passport controls and the AOC access). Additionally, most participants prefer to receive the alerts in the SOC.

6.2.6 Anomaly Detection on Passenger Records

The Key Performance Indicators for the ADPR are confidential and therefore discussed in the final report, deliverable D1.4 (12).

The validation participants' replies to ADPR-specific questions indicated that the information in alerts generated by ADPR is very useful and that the passenger data anomaly detection improves the threat detection. The top benefits listed were the baggage reconciliation, a clear view of what, where, and when and the alerting capabilities of the ADPR. GDPR (General Data Protection Regulation) compliance of the ADPR was one point of discussion. Suggestions for use-cases outside of the BHS environment included remote baggage drop off locations, identification of unattended baggage, and airlines' ground handling operations.

6.2.7 Secured ATM Services

The validation of the Secured ATM Services on the simulation platform has shown that the Secured ATM Services provides useful input to the Correlation Engine, allowing to successfully detect cyber-attacks (section 5.2.7). Moreover, Secured ATM Services received very positive feedback from the bespoke validation questions asked to the SOC operators (section 5.1.3.7): All questions where rated within a score of 5 to 7 (out of a range 1-7), with an average of over 6. This shows that the cyber threat detection alarms originated by Secured ATM Services output were deemed very useful by SOC operators.

6.2.8 Traffic Management Intrusion and Compliance System

In the questionnaires, TraMICS received unanimously positive results with one question-intended suggestion for improvement: to extend the timeframe in which single alerts shall be aggregated to a correlated security situation indicator to a week to possibly better overview the long-term security situation developments and/or post-operations analysis. In general, the tool is useful and accepted by operators. Both single indicators and the correlated security situation indicator are rated highly positive. The results indicate that the TraMICS is on the right track and its concept has proven itself. The remarks will be considered for future improvements to the TraMICS.

6.2.9 Business Process-based Intrusion Detection System

The BP-IDS validation on the simulation platform (see section 5.2.4) has shown that BP-IDS has a 100% accuracy rate, with very little false positives (3%) for detecting cyberthreats on the BHS. This shows that BP-IDS addresses the following objective O5 KPIs related to BP-IDS: Threat detections and false positive rates. Moreover, BP-IDS received positive feedback received from the bespoke questions, asked to the SOC operators, related to BP-IDS monitoring of the BHS (see section 5.1.3.9). This shows that the cyber threat detection alarms raised by BP-IDS were correctly handled by SOC operators, making it an adequate detection tool for fulfilling objective O5 "Improving cyber threat/anomaly detection on the BHS".

6.2.10 Malware Analyser

Using the log data it was verified that the time until detection (time between the attack; i.e. the download of the malware; and the time of the reception of the alert by the Correlation Engine) was always less than five minutes. Analysing the bespoke validation questions, the report of an analysed file provided easily understandable and useful information. Additionally, the simulation validation participants rated this Innovation Element as one of the systems which stood out.

6.2.11 ALCAD

The validation of ALCAD on the simulation platform has shown that ALCAD can provide useful input to the Correlation Engine, allowing to successfully detect cyber-attacks.

6.2.12 Correlation Engine

During the simulation validation, the Correlation Engine performed all tasks it was designed for. It processed in real time various events from several services and detection systems. From a rules-based system, it correlated and detected various threat. The Correlation Engine provided real time alerts to the SOC operator through the Incident Management Portal. During the simulation validation, several events were processed from the SATIE Tools and syslog events from the network and operating systems. These events were processed and alerts were raised to provide useful information to the SOC operators.

6.2.13 Investigation Tool

The SATIE Investigation Tool SMS-I provides SOC operators with the Intelligent Dashboard that presents and contextualizes the security alerts raised by the several SATIE Tools detecting physical and cyber threats. During the test, the SMS-I tool showed to the SOC operators all incidents and which alerts each incident originated from. Moreover, with the Intelligent Dashboard the SOC operators were able to understand the probability of an alert representing an incident. Several other important features of the alerts were also shown, such as the most common source and target IPs and ports. SOC operators were able to interact with the Intelligent Dashboard through their mouse to highlight each feature and focus their investigation.

The SMS-I tool received very positive feedback from SOC operators, which shows that the information provided was accessible and useful for their work. Therefore, it can be said that the SMS-I tool meets the objective O6 previously described.

6.2.14 Business Impact Assessment

Business Impact Assessment validation on the simulation platform focused on determining how an incident can propagate to BHS airport systems. The evaluation has shown that BIA provides fast impact assessment simulations (i.e. within seconds) for identifying several propagation paths that can impact the BHS business processes. During the simulation validation, BIA analysed the network connections within the BHS system (16 network computers connected to two routers), and identified the propagation paths that impacted six BHS business critical processes. Moreover, during the simulation validation, BIA was integrated with three SATIE Tools: the GLPI, the BP-IDS and the IMP. BIA received positive feedback from the bespoke questions, asked to the SOC operators, related to the impact assessments conducted to the BHS (see section 5.1.3.14). This shows that the impact assessment simulations provided by BIA were understandable to SOC operators, making it an adequate tool for fulfilling objective O6 “Improve situational awareness and anticipated decision making with the impact propagation simulation”.

6.2.15 Impact Propagation Simulation

Overall, the validation results for the IPS are very positive and suggest that the system addresses actual end-user needs. The questions presented in section 5.1.3.15 show a high agreement of the operators. Still, for the question “The Network Model is easy to understand” (IE11xFHGS02, Table 5.31) and “The mitigation options are well defined" (IE11xFHGS05, Table 5.31) the agreement is a bit lower. Potentially, this is because it was tried to keep the information limited to not overwhelm the end-user. It is planned to include information panels to better explain the visualized results.

During the development, some previously made assumptions were verified with the end-users, especially for the Agent-based Model, such as waiting times at specific counters, percentages of passengers with online-check-in, and many more. This helped to make the models more realistic and to present valuable results.

During the simulation validation, IPS received all incidents properly and offered visualizations. The feedback received besides the questionnaire was very valuable. The end-users suggested various improvements from which some have been directly implemented (e.g. make the Network Model more interactive, introduce a filter for the asset lists) and others will be addressed in the future development (e.g. develop an offline version of IPS, introduce information panels).

6.2.16 Incident Management Portal

During the simulation validation, the Incident Management Portal helped the operators to easily identify and resolve the threats. The IMP received alerts from the Correlation Engine and displayed all the related information such as e.g. IP address, port, software, operating system, etc. in an understandable way. The operators were able to navigate easily through the different tools to perform their analysis, retrieve vulnerability information from VIP and perform an impact simulation with the Impact Propagation Simulation and Business Impact Assessment.

6.2.17 Crisis Alerting System

During the simulation validation of the SATIE Solution, the CAS performed all the tasks that it was designed for, supporting the AOC operators in their further investigation and response actions. All the incidents that were send from the IMP, were received with almost no delay, and provided the AOC operators with all the required details that they needed in order to proceed with their standard operating procedures. The communication channels that the CAS provides, helped the operators to disseminate important information regarding the alarms, both through SMS and email, as well as the collaboration functionality in order to communicate with public safety agencies. The results of the validation depict the usefulness of such a tool, improving the collaboration between the AOC and other entities like the SOC and the Law-Enforcement Agencies (LEA), compared to the AOCs current situation. At the same time, the CAS GUI was proven to be user-friendly and intuitive, as well as giving the right information to the users during their operations.

6.2.18 CyberRange

On the CyberRange, the airport infrastructure was replicated, to have virtual assets such as the AODB, FIDS, or a Public Announcement system. For the Baggage Handling System, physical assets have been connected, like PLCs, and virtual assets have been replicated in order to have an operational system. Physical elements like cameras or passport readers have been connected to emulate a real airport environment on the CyberRange. All the SATIE Tools are integrated on the CyberRange. This gives it the capacity to play scenarios with cyber and physical aspects directly on the CyberRange and see the result of the detection from an SOC operator's point of view without interfering with real airport operations.

6.2.19 Emulated Baggage Handling System

The Digital Twin of the BHS is designed to emulate the behaviour of a real baggage handling system using a combination of systems actually used in BHS environments and virtual parts (like the actual conveyor belt system). As evident from the results of the bespoke questions presented in section 5.1.3.19, this objective was achieved. The Digital Twin worked well enough to give the participants the impression of an actual BHS system on which the attacks occur.

6.3 Summary

Throughout the previous sections, it has clearly been shown that the SATIE Solution is fit for purpose. The solution sufficiently fulfils the relevant SATIE Objectives as outlined in the DoA and the high agreement to the general validation questions point towards a faster detection of physical threats and cyber threats. Additionally, SATIE's approach of correlating cyber and physical alerts through a Correlation Engine was found to be well suited to combat combined cyber-physical attacks. The effort required by the operators to perform the most important tasks is also adequately low, as can be seen from the results of the modified SHAPE AIM-l questionnaire (see section 5.1.1.3).

In addition to the SATIE Solution in general, the individual SATIE Tools were also found to fulfil the requirements and the participants' expectations. Importantly, the two central interaction systems, the IMP and the CAS, with which the operators interacted the most received very positive replies. Moreover, there were only few suggestions for additional features or modifications.

A summary of all findings for the individual SATIE Tools can be found in tables in Annex 2 and Annex 3. A short result overview is given in Table 6.2, showing that each IE fulfilled its criteria and was rated as fit for purpose.

Table 6.2: Results of the individual IE validations

Innovation Element	IE#	Acceptable?
RIS	1	Yes
VIP	2	Yes
GLPI	2	Yes
ComSEC	3	Yes
Unified Access Control	4	Yes
Anomaly Detection	5	Yes
Secured ATM Services	6	Yes
TraMICS	7	Yes
BP-IDS	8	Yes
M.Analyser	8	Yes
ALCAD	8	Yes
Correlation Engine	9	Yes
SMS-I	10	Yes
BIA	11	Yes
IPS	11	Yes
IMP	12	Yes

Innovation Element	IE#	Acceptable?
CAS	13	Yes
CyberRange	14	Yes
Emulated BHS		Yes

However, the results also point towards several areas for improvements. The first is the overall usability of the SATIE Solution (see SUS score, section 5.1.1.1), which is sufficient, but can be improved for the final implementation. The usability may have been impacted by issues with the simulation environment and attack scenarios during the simulation validation and will probably improve as the operators grow accustomed to the SATIE Solution. This also highlights the need for a sufficient training of future operators and the need for an airport-specific tailoring of the SATIE solution. The second area for improvements is the trust in the solution, assessed using the SATI questionnaire (see section 5.1.1.2). The results of this questionnaire are clearly showing an area for improvement. The participants may already place more trust in the SATIE Solution as they gain more experiences and better understand how it works. The trust score may also have been impacted by the circumstances of the simulation validation, i.e. the fully virtual event via a web conference and limited options for communication between SOC and AOC, that will not be a factor for a system that is implemented at an airport site. Trusting systems is always a matter of understanding systems, transparency of system behaviour, training and experience. By using the system for an extended period of time and connected to real-live systems the operators are familiar with, the trust will raise. The demonstrations of the SATIE project offer this possibility to work under more realistic conditions with the SATIE solution.

Finally, the ease of integration of the SATIE Solution with the airport systems was also identified as a potential issue that should and will be addressed during the preparation of the demonstrations.

Despite the above-mentioned areas for improvement, the simulation validation as a whole showed that the SATIE solution is already quite mature and offers benefits for airport operators and first responders compared to their current systems. It is seen as an innovative solution with a high potential. The chosen threat scenarios have been rated as realistic and relevant and the participants want to use SATIE to add security to their current systems.

7 Implications for demonstrations

In addition to the discussion in the previous chapter, the results of the simulation validation are also analysed for implications for the demonstrations at the Athens, Milan, and Zagreb airports. Even though the SATIE Solution will not be validated by the operators a second time during the demonstrations, a specific focus of the implementation work done at the airports could be placed on issues identified from the simulation validation results.

As already summarized in section 6.3, the SATIE Solution was generally found to be fit for purpose. There are only a few areas for improvements that were identified. One of these is the integration with the existing airport systems. This should be tackled in the preparation of the demonstrations. For the simulation validation, the airport systems needed to be replicated on the CyberRange – or connected to it via VPN in the case of Milan's M-AIS and RMS – which certainly impacted the participants impression of the integration with the SATIE Solution. With the solution now being implemented at the airport sites for the demonstrations, this implementation should be revisited and improved.

Since the airport operators will not be evaluating the SATIE Solution a second time, no additional training is necessary for the demonstrations. Additionally, the demonstrations at the airport sites will be limited to the scenarios associated with the airport – Scenario #1 and Scenario #2 at Athens, Scenario #3 at Milan, and Scenario #4 at Zagreb – and the operators are therefore already very familiar with the airport environment in which the scenario is carried out.

During the demonstrations, the feedback of external stakeholders on the (improved) SATIE Solution will then be collected using a dedicated demonstration questionnaire. This questionnaire will be designed based on the general validation questions (see section 5.1.2) that capture a broad opinion of the SATIE Solution and allows for a comparison of the external stakeholders' assessment gathered in the demonstrations and the airport operators' assessment collected in the simulation validations. The details of the demonstration questionnaire will be included in the three demonstration reports, D6.4 for Zagreb, D6.5 for Athens, and D6.6 for Milan.

8 Conclusion

After the presentation of the test and verification plan and the validation plan in deliverable D6.2 (1), this report represents the next major step in the validation of the SATIE Solution and towards the demonstration of its usefulness, trustworthiness, and acceptance at the Athens, Milan, and Zagreb airports. The deliverable first reported on the deviations compared to the planning summarized in D6.2 (1) that became necessary with the move to a fully virtual simulation validation. Then, the results of the test of the individual SATIE Tools are reported in chapter 4, followed by the data gathered during the simulation validation in chapter 5. These consist of the participants' replies to the three-level simulation validation questionnaire consisting of three standard questionnaires, tailor-made general questions for the SATIE Solution as a whole, and bespoke validation questions on the individual SATIE Tools as well as objective Key Performance Indicators that were determined based on logging data recorded during the simulation validation or in separate experiments.

The results of the simulation validation were subsequently discussed with respect to the fulfilment of the SATIE Solution's objectives and in the context of the individual tools in chapter 6. It has been deduced that the SATIE Solution fulfils all of the validation-related objectives and is highly fit for purpose. Moreover, the individual SATIE Tools were also found to perform according to the operators' expectations. The identified areas for improvements are the usability of the solution and the participants' trust in the solution. These two may already improve as the operators grow more accustomed to how the SATIE Solution handles. One further area for improvement is the integration between the airport systems and the SATIE Solution. Analysing all results, the SATIE solution was very positively evaluated.

Finally, for this deliverable, the implications for the demonstrations at the three airport sites are summarized. While there will be no second evaluation by the operators, the external stakeholders' opinion will be recorded. In light of the very positive results collected during the simulation validations, there are no major changes required to make the demonstrations a success. However, the demonstrations provide the opportunity to improve the integration between the airport systems and the SATIE Solution.

Building onto the foundation laid in this deliverable, the reports on the airport demonstrations (D6.4, D6.5, and D6.6) will present how the analysis of the simulation validation results are reflected in the demonstration approach. Furthermore, the results of the demonstration questionnaire completed by the external stakeholders will be presented, discussed, and compared to the results presented herein.

9 References

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

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

3. **Reuschling, Fabian, et al.** Toolkit to enhance cyber-physical security of Critical Infrastructures in Air Transport. [ed.] John Soldatos, Isabel Praça and Aleksandar Jovanović. *Cyber-Physical Threat Intelligence for Critical Infrastructures Security - Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry.* s.l. : in printing, 2021.

4. **SATIE project.** *D4.2 - Traffic Management Intrusion and Compliance System.* 2020.

5. **SATIE Project.** *D4.3 - Cyber threat detection system.* 2020.

6. **SATIE project.** *D5.4 - Crisis Alerting System.* 2021.

7. **Brooke, J.** SUS - A quick and dirty usability scale. *Usability Evaluation In Industry.* London : Taylor & Francis Ltd., 1996, pp. 189-194.

8. **EUROCONTROL.** SESAR HP Repository: SATI - SHAPE Automation Trust Index. [Online] 22. October 2012. [Cited: 9. July 2020.] https://ext.eurocontrol.int/ehp/?q=node/1594.

9. **Dehn, Doris M.** Assessing the Impact of Automation on the Air Traffic Controler: The SHAPE Questionnaires. *Air Traffic Control Quarterly, Vol. 16(2).* 2008, pp. 127-146.

10. **EUROCONTROL.** SESAR HP Repository: AIM - SHAPE questionnaire for Assessing the Impact of Automation on Mental Workload. [Online] 22 October 2012. [Cited: 01 October 2020.] https://ext.eurocontrol.int/ehp/?q=node/1587.

11. **Bangor, A., Kortum, P. and Miller, J.** Determining What Individual SUS Scores Mean. *Journal of Usability Studies 4 (3).* 2009, pp. 114-123.

12. **SATIE project.** *D1.4 - Final Report (in writing).* 2021.

13. —. *D5.1 - Anticipated impact assessment system.* 2021.

14. **SATIE Project.** *Description of Action.* 2019.

10 Annex 1 – Validation activities' schedules, consent form and NDA

10.1 Schedule of the Zagreb simulation validation

	Time (CET)	Activity	Leader
Morning	9:00 – 9:15	Welcome	Project representative
	9:15 – 9:35	Details about the validation activities	Validation exercise leader
	9:35 – 9:45	Log into CyberRange	Technical exercise leader
	9:45 – 10:15	Review of each tool on CyberRange (5 min each) **SOC**: ACS, RIS, SMS-I, BIA, IPS **AOC**: IPS, CAS	Trainers (in respective rooms)
	10:15 – 10:30	Coffee break	--
	10:30 – 12:20	**Exercise 1 (Sc#4)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	12:20 – 13:00	**Exercise 2 (Sc#5)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader

	13:00 – 13:55	Lunch break	--
Afternoon	13:55 – 14:00	Buffer time / gathering in main room	Validation exercise leader
	14:00 – 14:45	**Exercise 3 (Sc#2)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	14:45 – 15:45	**Exercise 4 (Sc#1)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	15:45 – 16:15	**Exercise 5 (Sc#3)**: Handle the scenario, return to the main room	Validation exercise leader
	16:15 – 16:45	**Exercise 6**: RIS validation, answer the questionnaire	IE developer
	16:45 – 17:15	Final debriefing & impressions about SATIE	Validation exercise leader, IE developers
	17:15 – 17:30	Recap and end	Project representative

10.2 Schedule of the Athens simulation validation

	Time (CET)	Activity	Leader
Morning	9:00 – 9:15	Welcome	Project representative
	9:15 – 9:35	Details about the validation activities	Validation exercise leader
	9:35 – 9:45	Log into CyberRange	Technical exercise leader
	9:45 – 10:15	Review of each tool on CyberRange (5 min each) **SOC**: ACS, RIS, SMS-I, BIA, IPS **AOC**: IPS, CAS	Trainers (in respective room)
	10:15 – 11:15	**1st Exercise (Sc#1)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	11:15 – 12:25	Lunch break	--
Afternoon	12:25 – 12:30	Buffer time / gathering in main room	Validation exercise leader
	12:30 – 13:30	**2nd Exercise (Sc#2)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	13:30 – 14:30	**3rd Exercise (Sc#3)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	14:30 – 14:45	Coffee break	
	14:45 – 15:40	**4th Exercise (Sc#4)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader

	15:40 – 16:10	**5th Exercise (part I)**: Sc #5, handle the scenario, return to the main room	Validation exercise leader
	16:10 – 16:40	**5th Exercise (part II):** RIS validation, answer the questionnaire	IE developer
	16:40 – 17:00	Final debriefing & impressions	Validation exercise leader, IE developers

10.3 Schedule of the Milan simulation validation

Day 1

	Time (CET)	Activity	Leader
Morning	10:00 – 10:15	Welcome	Project representative
	10:15 – 10:35	Details about the validation activities	Validation exercise leader
	10:35 – 10:45	Log into CyberRange	Technical exercise leader
	10:45 – 11:15	Review of each tool on CyberRange (5 min each) **SOC**: ACS, RIS, SMS-I, BIA, IPS **AOC**: IPS, CAS	Trainers (in respective room)
	11:15 – 11:30	Coffee break	--
	11:30 – 12:30	**Exercise 1 (Sc#3)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	12:30 – 13:30		Validation exercise leader

		Exercise 2 (Sc#4): Handle the scenario, answer the questionnaire, return to the main room	
	13:30 – 14:25	Lunch break	--
Afternoon	14:25 – 14:30	Buffer time / gathering in main room	Validation exercise leader
	14:30 – 15:30	**Exercise 3 (Sc#1)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	15:30 – 16:00	Recap of Day 1	Project representative

Day 2

	Time (CET)	Activity	Leader
Morning	9:30 – 9:50	Welcome, address any issues from yesterday	Project representative
	9:50 – 10:00	Log into CyberRange	Technical exercise leader
	10:00 – 11:00	**Exercise 4 (Sc#5)**: Handle the scenario, answer the questionnaire, return to the main room	Validation exercise leader
	11:00 – 11:15	Coffee break	--
	11:15 – 12:15	**Exercise 5 (Sc#2)**: Handle the scenario, return to the main room	Validation exercise leader

	12:15 – 12:45	**Exercise 6**: RIS validation, answer the questionnaire	IE developer
	12:45 – 13:15	Final debriefing, impressions about SATIE, address any questions	Validation exercise leader, IE developers
	13:15 – 13:30	Recap and end	Tim

10.4 Consent form and NDA

10.4.1 Information sheet

The SATIE Project

The SATIE project is funded by the European Commission’s Research Executive Agency (REA), under its Horizon 2020 Framework Programme for Research and Technological Development. It aims to build a security toolkit in order to protect critical air transport infrastructures against combined cyber-physical threats. Over a 30-month time frame, the SATIE consortium will develop, test, validate and demonstrate in operational conditions 14 innovative elements which will optimise airport security.

SATIE: Simulation Validation for the SATIE Tools

The SATIE simulation validation is aimed at providing participants with sufficient knowledge of the SATIE systems and subsystems to be used during demonstrations and simulations. This ensures that all participants are familiarised with the functioning of the systems beforehand.

The personal data that will be gathered

Before the simulation, your first and last name, as well as email address will be/were collected. This data will be used to provide you with access to the CyberRange simulation platform on which the training and simulations are carried out.

During the simulation, there will be no data recorded. You may be asked to share your screen, but no screen recording will take place.

The SATIE Project
During the SATIE related exercises, multiple data will be recorded to aid in validating the concepts presented in the SATIE solution. This data will be: Objective performance data (e.g. in the form of log files), subjective questionnaire data, comments, remarks and general feedback. The information collected from questionnaires, as well as some comments, remarks, and general feedback will be first pseudonymized and later anonymized during pre-processing to comply with data protection regulations.
How to withdraw from the simulation validations exercise?
Participation is entirely voluntary. The participant can withdraw from the exercise at any moment by informing the Project Coordinator of their wish to withdraw from the exercise.
Who will be responsible for the information once the Project is completed?
The collection, storage, protection, retention and destruction of personal data will be the responsibility of the data collecting and processing partners, whose DPO details are included in the information sheet. To facilitate the exercise of data rights, the Project Coordinator Tim Stelkens-Kobsch acts as the point of contact for the DPOs and all requests should be sent to Tim.Stelkens-Kobsch@dlr.de.

The SATIE Project

Who will have access to the information?

Apart from the participant (data subject), the respective data controllers (see below) will have access to the participant's personal data. The data controller will delete any personal data latest after ten years.

Data collected	Data controller
Full names and e-mail addresses	Airbus Cybersecurity SAS
Subjective data (questionnaire data, comments, remarks, general feedback)	Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)
Objective data (e.g. in the form of log files)	Developer of the system collecting the data.

Your personal data will not be shared outside of the SATIE project.

The Data Subject's Rights

The participant is granted, free of charge, access to all data concerning them and, as appropriate the right of rectification, erasure or blocking of data, in particular because of the incomplete or inaccurate nature of the data. The data subject also has the right of notification of rectifications to third parties to whom the data have been disclosed.

10.4.2 List of DPOs in the SATIE project

Below is the information for the Data Protection Officer provided by the relevant partners. As different partners will be collecting and processing different data for the simulation validation exercises, several organizations and DPOs are involved. In case you want to exercise your data rights a single point of contact is provided above as acting DPO for the simulation validation exercises. The list below is provided just as a reference.

Company	DPO Name	Contact details
Airbus Cybersecurity SAS	[redacted]	[redacted]@airbus.com
	[redacted]	[redacted]@airbus.com
Alstef Automation	[redacted]	[redacted]@alstef.com
Athens International Airport S.A.	[redacted]	[redacted]@aia.gr
Deutsches Zentrum für Luft- und Raumfahrt	[redacted]	[redacted]@dlr.de
Eticas Research and Innovation	[redacted]	[redacted]@eticasfoundation.com
Fraunhofer Institut für Kurzzeitdynamik, Ernst-Mach-Institut	[redacted]	[redacted]@zv.fraunhofer.de
Frequentis AG	[redacted]	[redacted]@frequentis.com
Idemia Identity and Security France	[redacted]	[redacted]@idemia.com
INOV INESC Inovação – Instituto de Novas Tecnologias	[redacted]	[redacted]@inov.pt
Instituto Superior de Engenharia do Porto	[redacted]	[redacted]@isep.ipp.pt
ITTI Sp. z o.o.	[redacted]	[redacted]@itti.com.pl
Kentro Meleton Asfaleias	[redacted]	[redacted]@kemea-research.gr
Ustav Informatiky, Slovenska Akademia Vied	[redacted]	[redacted]@savba.sk
Satways - Proionta Kai Ypiresies Tilematikis Diktyakon Kai Tilepikinoniakon Efarmogon Etairia Periorismenis Efthinis Epe	[redacted]	[redacted]@satways.net

Company	DPO Name	Contact details
Società peAzioni esercizi Aeroportuali	[redacted]	[redacted]@seamilano.eu
Teclib Spain S.L	[redacted]	[redacted]@teclib.com
Zagreb Airport	[redacted]	[redacted]@zag.aero

10.4.3 Consent form

The SATIE project is funded by the European Commission's Research Executive Agency (REA), under its Horizon 2020 Framework Programme for Research and Technological Development. It aims to build a security toolkit in order to protect critical air transport infrastructures against combined cyber-physical threats. Over a 30-month time frame, the SATIE consortium will develop, test, validate and demonstrate in operational conditions 14 innovative elements which will optimise airport security.

The following form is intended to record your consent as a participant to take part in the SATIE simulation activities and the processing of your personal data which has been explained in the information sheet provided to you by the project coordinator.

CONSENT	YES	NO
I hereby confirm that I freely consent to my participation in the SATIE simulation activities. The purpose of this activity has been explained to me in writing and I am fully informed about the way in which my personal data is going to be processed. I am participating voluntarily and understand that I can withdraw from the activities at any time without any penalty or prejudice. I freely consent to the processing of my personal data for the purpose of participating in this SATIE activity. I understand that my personal data will not be processed outside the SATIE project.	□	□

CONSENT	YES	NO
I understand that in the unlikely event that the research leads to findings regarding criminal or harmful activities, the Exercise Leader, or SATIE's Project Management Board in case the Exercise Leader is unable to provide an opinion, shall be made aware of this and decide on whether or not to pass this on to the relevant authorities, depending on the finding and national legal requirements. I understand that my feedback will remain anonymous, and that should I not wish to answer any particular question(s), I am free to decline without any penalty or prejudice. I understand that my answers to any questionnaire will remain anonymous, and that should I not wish to answer any particular question(s), I am free to decline without any penalty or prejudice. I have been informed that the length of the personal data retention period will be of up to ten years after the end of the project. I have the right to request access to my personal data, and to have it rectified or deleted at any time by contacting the Project Coordinator Tim Stelkens-Kobsch at tim.stelkens-kobsch@dlr.de. I acknowledge that once the Project Coordinator or Exercise Leader receives notification that I chose to withdraw my consent, my information will no		

CONSENT	YES	NO
longer be processed for the purposes I originally agreed to, unless there are other legitimate bases for doing so in the law. I understand that the personal information included in this form (name and surname) will be kept by DLR for a maximum of ten years after the end of the project, in a secure environment according to data protection guidelines. It will be permanently destroyed or anonymized up to ten years after the end of the project. A copy of the information sheet will be given to the signee (participant).		
I will not receive any compensation or incentive for having taken part in this exercise.	□	□
Some picture/video could be taken during the exercise and may be published digitally or in print for communication and dissemination purposes. I give authorization to use my image only for these purposes. Note: Choosing NO does not limit the participation in this exercise.	□	□
Some audio and screen recordings of the virtual meeting could be taken during the exercise and may be used for data analysis and exercise evaluation purposes. I give authorization to use my recordings only for these purposes. Note: Choosing NO does not limit the participation in this exercise.	□	□

The personal information included in this form (name and surname) will be kept by the Project Coordinator for a maximum of five years after the end of the project, in a secure environment according to data protection guidelines. It will be permanently destroyed or anonymized five years after the end of the project.

A copy of the information sheet and this (signed) consent form will be given to the signee and a copy will be kept by Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR) for their record.

Print name (participant) ………………………………………………….

Signature (participant) : ……………………………………………………..

Date : …………………………………………………..

10.4.4 Non-Disclosure Agreement

NDA	YES	NO
I hereby confirm that I shall keep all information confidential related to the above-mentioned simulation validation exercises.	□	□
I shall use all reasonable care, but in no event a lesser degree of care than I use to protect my own confidential and proprietary information of similar importance, to prevent the unauthorized use, disclosure, publication or dissemination of confidential information.	□	□
I shall not transmit, show or communicate to third parties, any documents or any confidential information supplied during the exercises, whether it is connected with or produced during the simulation validation exercise.	□	□
I hereby undertake to return to the exercise leader all documentation that would generally be in my possession and that is in any way related to the activity of the simulation validation exercise.	□	□

________________ ________ ____

Name of Participant Date Signature

11 Annex 2 – List of technical and integration tests

11.1 CyberRange

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
CR_L1	Log in	Access the application inserting the username and password and clicking "Sign in"	Workzone SATIE display	The SATIE workzone is displayed	OK
CR_D1	WZ-05	On the left bar, Infrastructure, Template, Operating Systems/ Drag and drop one system	System deploy on CyberRange	The system is deployed	OK
CR_D2	WZ-05	On the left bar, Infrastructure, Template, Networks/ Drag and drop LAN	LAN deploy on CyberRange	The LAN is deployed	OK
CR_D3	WZ-05	Double click on a VM	Terminal or UI display	The terminal or UI are displayed	OK
CR_S1	WZ-05	On the left bar, Actions and scenarios, scenarios, choose one scenario	The scenario is played	The scenario is played	OK

11.2 Emulated Baggage Handling System (BHS)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
SCADA_ SAC_1	SCADA Client: Error History	No error related to the communication between PLC and BAGWARE are displayed	PLCs are communicating with BAGWARE	Communication between PLCs and BAGWARE is ok	OK
SCADA_ SAC_2	SCADA Client: Headband, Error History	Communication indicator is alive. No error related to the communication between PLC and SCADA are displayed	PLCs are communication with SCADA	Communication between PLCs and SCADA is ok	OK
SCADA_3D_1	SCADA Client: Error History, Error Acknowledgement	No error related to the communication between PLC and Emulate3D are displayed	PLCs are communication with Emulate3D	Communication between PLCs and Emulate3D is ok	OK
SCADA_3D_2	SCADA Client: Error History, Error Acknowledgement	No error related to the Emulate3D environment	Baggage flow is not blocked	Emulate3D is working normally, the baggage is sorted	OK
BAGWARE_1	Under user account: Type "taches" (French for "tasks")	No error detected, no missing tasks	BAGWARE is running and communicating in standard condition	No missing tasks, BAGWARE is working properly	OK
BAGWARE _VIEW_1	BAGWARE Client: Info Bar	No link is missing, no process is missing	BAGWARE is running and communicating in standard condition	The links and processes are all there. BAGWARE is functioning normally.	OK
BAGWARE _VIEW_2	BAGWARE Client: Flight Tab	Flights are displayed	BAGWARE is sorting bags according to Baggage Source Message (BSM)	Bags are properly sorted and flights well displayed	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
AODB_1	Under user account: Type “taches” (French for tasks)	No error detected, no missing tasks	BSM generator is running and communicating in standard condition	No missing tasks, AODB is working properly and generate BSM messages	OK

11.3 Secured ATM Services

The described technical tests assume the following settings:

- Secured ATM Services are deployed and running.
- SWIM Client is available and ready to interact with Secured ATM Services.
- ALCAD is deployed and running.
- Correlation Engine is deployed and running.
- Communication infrastructure (e.g., Kafka broker) is up and running.

In the following Table, the “SETTING” column indicates the components to be used to trigger the test case and to observe the results.

TEST CASE ID	SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
ATM_SVC_1	SWIM Client	User requests flight plan data from Secured ATM Service, using valid credentials.	User is able to request Flight Plan data from Secured ATM Services	SWIM Client could successfully request Flight Plan Data from Secured ATM Services	OK
ATM_SVC_2	SWIM Client	User requests weather data from Secured ATM Service, using valid credentials	User is able to request weather data from Secured ATM Services	SWIM Client could successfully request weather data from Secured ATM Services	OK

TEST CASE ID	SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
ATM_SVC_3	SWIM Client	User requests NOTAM data from Secured ATM Service, using valid credentials	User is able to request NOTAM data from Secured ATM Services	SWIM Client could successfully request NOTAM messages from Secured ATM Services	OK
ATM_SVC_4	SWIM Client	User tries to access Secured ATM Services, using invalid credentials.	Service access is denied	Without using valid credentials, the access to Secured ATM Services is denied	OK
ATM_LOG_1	Correlation Engine	Secured ATM Services are running normally, without the need of specific events.	Correlation Engine receives periodic log messages from Secured ATM Services (e.g., one message every 30 seconds)	Correlation Engine receives periodic log messages from Secured ATM Services: one message every 30 seconds	OK
ATM_LOG_2	Correlation Engine	Secured ATM Services are running normally, without the need of specific events.	Log messages from Secured ATM Services include the following information items: • Security Threat Level • Number of Service Requests • Number of invalid authentication requests	Log messages from Secured ATM Services include the following information items: • Security Threat Level • Number of Service Requests • Number of invalid authentication requests	OK
ATM_LOG_3	ALCAD	Secured ATM Services are running normally, without the need of specific events.	ALCAD receives NetFlow data from Secured ATM Services server.	ALCAD receives NetFlow data from Secured ATM Services server	OK

TEST CASE ID	SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
ATM_LOG_4	SWIM Client / Correlation Engine	User interacts via SWIM Client by requesting various ATM data (FPL, Weather, NOTAM).	Log messages received by Correlation Engine include the number of service requests issued during the last logging period.	After interacting via SWIM Client, the log data received by the CE include the number of service requests.	OK
ATM_LOG_5	SWIM Client / Correlation Engine	User tries to authenticate with invalid credentials via SWIM Client.	Log messages received by Correlation Engine include the number of failed authentication requests encountered during the last logging period.	After interacting via SWIM Client, the log data received by the CE include the number of failed authentications.	OK
ATM_LOG_6	Incident Management Portal / Correlation Engine	User at the Incident Management Portal sets a new value of the Security Threat Level.	Log messages received by Correlation Engine in the next logging cycle include the new value of the Security Threat Level.	After setting the Security Threat Level via Incident Management Portal, the log data received by the CE include the new value of the Security Threat Level.	OK
ATM_HRD_1	Incident Management Portal	User at the Incident Management Portal sets a new value of the Security Threat Level.	Secured ATM Services accept the command for setting the Security Threat Level.	Secured ATM Services accept the command for setting the Security Threat Level.	OK
ATM_HRD_2	Incident Management Portal / SWIM Client	User at the Incident Management Portal sets the Security Threat Level to "Low." User interacts via SWIM Client by requesting various ATM data (FPL, Weather, NOTAM).	Under "Low" Security Threat Level, Secured ATM Services act less restrictive in accepting new Service Requests: All service requests with valid credentials from SWIM Client are accepted.	Under "Low" Security Threat Level all service requests with valid credentials from SWIM Client are accepted.	OK

TEST CASE ID	SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
ATM_HRD_3	Incident Management Portal/ SWIM Client	User at the Incident Management Portal sets the Security Threat Level to "High." User interacts via SWIM Client by requesting various ATM data (FPL, Weather, NOTAM).	Under "High" Security Threat Level, Secured ATM Services act more restrictive in accepting new Service Requests: Now only a smaller number of service requests is accepted.	Under "High" Security Threat Level only a subset of service requests from SWIM Client are accepted. .	OK

11.4 Traffic Management Intrusion and Compliance System (TraMICS)

According to the DoA, TraMICS was tested within T4.2 and the tests as well as the results of its verification are described and documented in D4.2 (4); where the following table originates from.

TEST CASE ID	NAME	STATUS (OK, NOT)
SpV.1	Single-target speaker verification	OK
SpV.2	Speaker authorization (multitarget-group speaker verification)	OK
SpV.3	Radio channel speaker verification	OK
SD.1	Stress detection	OK
CMCD.1	Detection of deviation from assigned route	OK
CMCD.2	No route deviation alerts after being back on route	OK
CMCD.3	Detection of multiple deviations from a planned route	OK
CMCD.4	Opposite traffic	OK

TEST CASE ID	NAME	STATUS (OK, NOT)
CMCD.5	Opposite traffic at a crossing	OK
CMCD.6	Two AC merge into a taxiway without stopping	OK
CMCD.7	Two AC merge into a taxiway with stopping	OK
CMCD.8	Two AC merge into a taxiway with stopping behind a stop bar	OK
CMCD.9	Two AC at a crossing with disjoined routes	OK
CMCD.10	Two AC at a runway holding point	OK
CMCD.11	Two AC are moving on the same taxiway and the subsequent is faster	OK
CMCD.12	Two AC are moving on the same taxiway and the preceding stops	OK
CMCD.13	Route deviation with opposite heading	OK
CMCD.14	Hold clearance was given but AC does not stop	OK
CMCD.15	AC stopped, but continues taxi without continue taxi clearance	OK
UB.1	AC pushing without pushback clearance	OK
UB.2	AC taxiing without taxi clearance	OK
UB.3	Wrong clearance order	OK
UB.4	Pushback clearance at rollout position	OK
UB.5	Pushback with taxi clearance	OK
CORE.1	Message reception from SpV module	OK
CORE.2	Unauthorized speaker leads to a red security situation indicator	OK
CORE.3	Long lasting route deviation leads to a yellow/red security situation indicator	OK
CORE.4	Multiple route deviations of one AC lead to a yellow security situation indicator	OK
CORE.5	Route deviations of several AC lead to a red security situation indicator	OK
CORE.6	Conflict leads to a yellow security situation indicator	OK

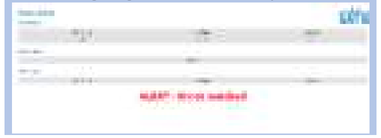
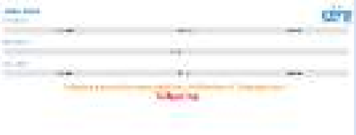
TEST CASE ID	NAME	STATUS (OK, NOT)
CORE.7	Conflicts lead to a red security situation indicator	OK
CORE.8	Unauthorized speaker and route deviation	OK
CORE.9	Unauthorized speaker, route deviation and conflict	OK
CORE.10	Route deviation and conflict lead to a yellow security situation indicator	OK
CORE.11	Change from a yellow to a green security situation indicator	OK
CORE.12	Change from a red to a green security situation indicator	OK
CORE.13	Change from a red to a yellow to a green security situation indicator	OK
SYL.1	Verification of message creation and recording	OK
SYL.2	Verification of message reception at the Correlation Engine	OK

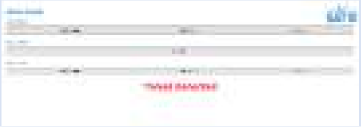
11.5 Anomaly Detection on Passenger Records (ADPR)

The results of Anomaly Detection on Passenger Records are confidential and will therefore be reported in deliverable D1.4 (12).

11.6 Unified Access Control (UAC)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
UAC_REG_1	Person authorized registration	Register face into Augmented Vision and card (or fingerprint) into MorphoWave device to create an authorized user (for both “employee” and “executives” status).	Registration is completed. Fingerprint and face are properly identified.	New users can be registered into both systems (Augmented Vision & MorphoWave) as an authorized person, either an	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
				"employee" or an "executive". User record can be visualized, modified, and deleted in Augmented Vision and Morphowave interface.	
UAC_REG_2	Person threat registration	Register face into Augmented Vision Alert watch list to create a new threat	Registration is completed. Face is properly identified	New user can be registered into Augmented Vision as a "threat" in the alert watchlist. User record can be visualized, modified, and deleted in Augmented Vision.	OK
UAC_AC_1	Access control	Previously authorized person tries to access a restricted area with its fingerprint (or card)	Access is granted, an "access granted" event is sent to the SOC with registered person and card info	Access Granted message generated by UAC.	OK
UAC_AC_2	Access control	Previously authorized person tries to access a restricted area with a stolen or copied card	Access is denied, an alert "ID not match" is sent to the SOC with registered person and camera location	"Alert - ID not matched" message generated by UAC 	OK
UAC_AC_3	Access control – Tailgating activated	Previously authorized person (with employee status) try to access a restricted area while unknown individual is hiding behind	Access is denied, an alert "Tailgating detected" is sent to the SOC with registered person and camera location	"Tailgating" message generated by UAC. 	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
UAC_AC_4	Access control – Tailgating activated	Previously authorized person (with executive status) try to access a restricted area while unknown individual is hiding behind	Access is granted, an “accompanied access” event is sent to the SOC with registered person, card info and camera location.	“Accompanied Access granted” message generated by UAC.	OK
UAC _SURV_1	Surveillance	A known threat is detected in the field of view of the camera (irrelevant to access intent)	Access is denied, a “threat detected” event is sent to the SOC with registered threat information and camera location	“Threat detected” message generated by UAC. 	OK

11.7 Business Process-Based Intrusion Detection System (BP-IDS)

The results of Business Process-based Intrusion Detection System are confidential and will therefore be reported in deliverable D1.4 (12).

11.8 Malware Analyser

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
MA_L1	Login page	Access the application inserting the username and password and clicking "Sign in"	Home page of the application	The home page is displayed.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
MA_P1	Search Page	Add filter for example "Operating System" "Windows 7"	All analyse file with the specific filter are displayed	A list of files is displayed.	OK
MA_F1	Submit page	Submit a file	The file is analysed	An analysis is running.	OK
MA_R1	Report page	Click on a file to see the report	All the information including the risk are displayed	A report is displayed, the risk is visible.	OK
MA_R1	Report page	Click on Export PDF	A report File in PDF is download	A report in PDF format is generated and saved locally.	OK
MA_S1	/etc./suricata/suricata.yml	Suricata extract file in the Surion path monitored	File sent to Malware Analyser	Files are extracted from the network and sent to the Malware Analyser.	OK
MA_S2	/etc./surion/surion.conf	File send to Malware Analyser with Surion	Report received and send to Kafka	A message is available in Kafka.	OK
MA_S3	/etc./rsyslog.d/kafka.conf	Report send to Kafka	Report received by external systems	The message is displayed in the Correlation Engine.	OK

11.9 ALCAD

The table below describes the following technical tests:

- ALCAD is deployed and running.
- ALCAD communicates with other systems properly (ATM services, Correlation Engine, other).
- ALCAD is running and marking / detecting selected types of attacks (e.g. port scan) correctly as anomalies.

TEST CASE ID	PAGE/ SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
ALCAD _CONF_1	Configuration tests	The Netflow data is sent by external system to ALCAD collector.	The data is received from external system by collector.	The data was received from external system by collector. The details can be found in deliverable D4.3.	OK
ALCAD _CONF_2	Calculation test	Monitored system is scanned using e.g. nmap.	The port scan is marked as anomaly.	The port scan was marked as anomaly. The details can be found in D4.3 deliverable.	OK
ALCAD _CONF_3	Configuration test	Event is sent to internal kafka broker and visualized	Event is visualized in ALCAD UI	Event was properly visualized in ALCAD UI.	OK
ALCAD _CALC_1	Configuration test	Event is sent to external kafka broker and visualized	Event is received in external system.	Event was received in external system.	OK

11.10 Secured Communication on the BHS (ComSEC)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
ComSEC _TRACE_1	Wireshark on BHS network	ComSEC is bridging network traffic	Network traffic should be found for BAGWARE (ComSEC2), SCADA(ComSEC5), PLCs (ComSEC3 and 4), AODB (ComSEC1), and BAGWARE View (ComSEC6).	By performing network traffic inspection on the simulation platform, it was possible to validate that ComSEC is bridging the network traffic between BHS devices.	OK
ComSEC _TRACE_2	Wireshark on BHS	ComSEC is generating network packet digital signatures	ComSEC digital signatures should be found for BAGWARE (ComSEC2), SCADA(ComSEC5), PLCs(ComSEC3	By performing network traffic inspection on the simulation platform, it was possible to	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
			and 4), AODB (ComSEC1), and BAGWARE View (ComSEC6)..	validate that ComSEC is constructing digital signatures of all BHS network traffic.	
ComSEC _TRACE_3	Alert in the ComSEC database	ComSEC detected the incident	ComSEC detected the incident and has registered in its internal database.	By connecting to internal database, it was possible to inspect all ComSEC alerts.	OK
ComSEC _INT_1	Apache Kafka topic ComSEC	ComSEC has forwarded the alert to Correlation Engine	Kafka should have the event.	By connecting to Apache Kafka, it was possible to inspect that ComSEC contained events.	OK
ComSEC _INT_2	Apache Kafka topic ComSEC	ComSEC is connected to Correlation Engine	Kafka should have at least one event	By connecting to Apache Kafka, it was possible to inspect that ComSEC is connected to Apache Kafka.	OK

11.11 Business Impact Assessment (BIA)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
BIA_TRACE_1	BIA webpage	BIA is online.	A threat propagation graph is displayed.	By using the SOC operator it was possible to connect to BIA. Under this connection, it was possible to perform threat propagation.	OK
BIA_INT_1	IMP redirection button	BIA is reachable from IMP.	BIA homepage is displayed.	Using the IMP, it was possible to connect to BIA	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
				through the Impact Assessment button.	
BIA_INT_2	BP-IDS REST_API webpage	BIA is able to load BP-IDS business process information.	A JSON object with BP-IDS is displayed.	By connecting to the endpoint of the BP-IDS REST API, it was possible to retrieve the JSON object.	OK
BIA_INT_3	GLPI REST_API webpage	BIA is able to load GLPI inventory information.	A JSON object with GLPI information is displayed.	By connecting to the endpoint of the GLPI REST API, it was possible to retrieve the JSON object.	OK

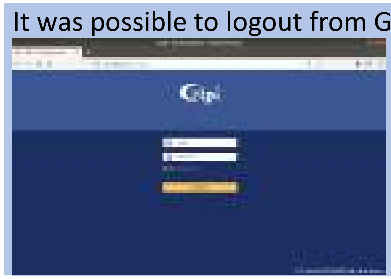
11.12 Correlation Engine

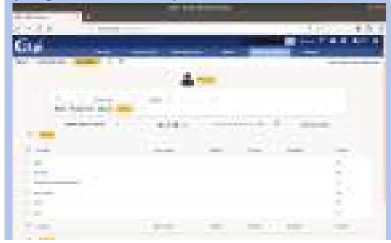
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
CE_L1	Log in	Access the application inserting the username and password and clicking "Sign in"	Main page of the Application, at the Top Right you can see your profile with the username	Main page of the Application.	OK
CE_L2	Log in	Log-out of the application and re-access it inserting the username and password.	Operation went successfully.	Operation went successfully.	OK
CE_P1	Search Page	Access the search page	User is able to see the events received	The events are displayed.	OK
CE_P2	Alerts page	Access the alerts page/ Show all alerts	User is able to see all the alert resolved or not	The alerts are displayed.	OK

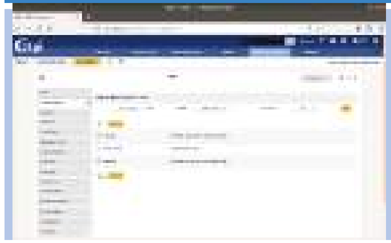
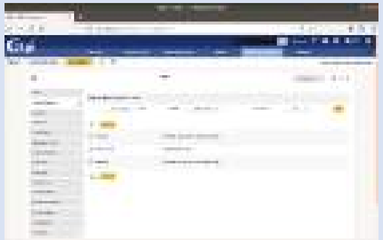
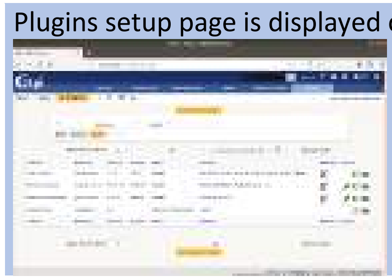
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
CE_INPUT_1	System INPUT/ Show received messages on ALCAD Input	Input configure to receive events from ALCAD	New events received from the ALCAD system	ALCAD events displayed.	OK
CE_INPUT_2	System INPUT/ Show received messages on BP-IDS Input	Input configure to receive events from BP-IDS	New events received from the BP-IDS system	BP-IDS events displayed.	OK
CE _INPUT_3	System INPUT/ Show received messages on ComSEC Input	Input configure to receive events from ComSEC	New events received from the ComSEC system	ComSEC events displayed.	OK
CE _INPUT_4	System INPUT/ Show received messages on TraMICS Input	Input configure to receive events from TraMICS	New events received from the TraMICS system	TraMICS events displayed.	OK
CE _INPUT_5	System INPUT/ Show received messages on SWIM ATM Services Input	Input configure to receive events from SWIM ATM Services	New events received from the SWIM ATM Services system	SWIM ATM events displayed.	OK
CE _INPUT_6	System INPUT/ Show received messages on Surion Input	Input configure to receive events from Malware Analyser	New events received from the Malware Analyser system	Malware Analyser events displayed.	OK
CE _INPUT_7	System INPUT/ Show received messages on Passenger anomaly detection Input	Input configure to receive events from Passenger anomaly detection	New events received from the Passenger anomaly detection system	Passenger Anomaly Detection system events displayed.	OK
CE _INPUT_8	System INPUT/ Show received messages on Unified Access Control Input	Input configure to receive events from Unified access control	New events received from the Unified Access Control system	Unified Access Control system events displayed.	OK
CE_COM_1	System / Configurations GLPI Configuration	The configuration is filled up	Click on Test Button Green banner “Success” is displayed	Green banner “Success” is displayed.	OK
CE_COM_2	System / Configurations VIP Configuration	The configuration is filled up	Click on Test Button Green banner “Success” is displayed	Green banner “Success” is displayed.	OK

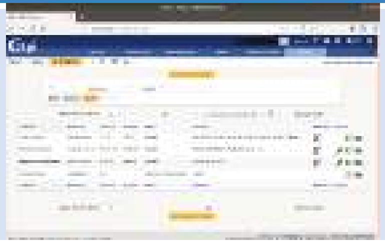
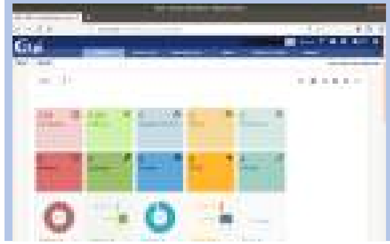
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
CE _ENRICH_1	Search	The Correlation Engine is able to request information from GLPI	SATIE events enriched with GLPI information	SATIE events are enriched.	OK
CE _ENRICH_2	Search	The Correlation Engine is able to request information from VIP	Specific SATIE events enriched with VIP infromation	SATIE events are enriched.	OK
CE_ALERT_1	Alerts	Alert rules defined	Alert triggered when specific events received	Alerts are triggered.	OK

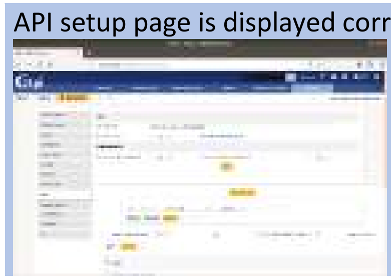
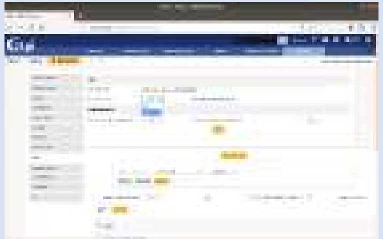
11.13 Gestion Libre de Parc Informatique (GLPI)

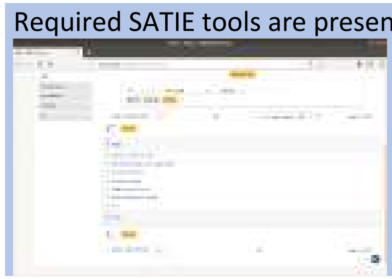
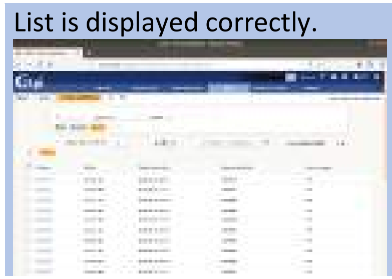
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
GLPI _LOGIN_1	Login page	Access the application home URL, fill "Username" and "Password" fields and click "Post"	The home page is displayed with the global dashboard	It was possible to login to GLPI.	OK
GLPI _LOGIN_2	Any page	Click the exit button on the upper right of the window	The login page is displayed	It was possible to logout from GLPI. 	OK

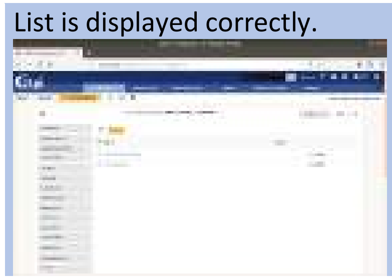
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
GLPI _LOGIN_3	Any page	Click the 'My settings' button on the upper right of the window	The main user settings page is displayed	It was possible to access the settings page correctly.	OK
GLPI _LOGIN_4	Any page	Click Administration -> Users	The Users administration page is displayed	It was possible to access the administration page correctly. 	OK
GLPI _LOGIN_5	Users administration page	Click 'glpi' entry in the list	The 'glpi' User details is displayed	User details are correct.	OK
GLPI _LOGIN_6	'glpi' User details page	Click 'Authorizations' tab on the left	The 'glpi' user authorizations are displayed	User authorizations are correct.	OK

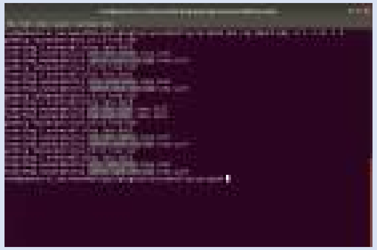
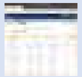
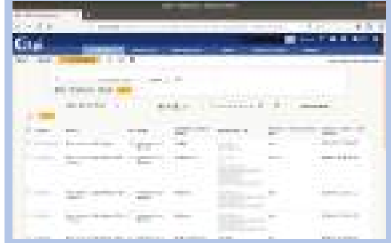
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
					
GLPI _LOGIN_7	'glpi' user authorizations page	No action	The 'Root entity' entry in the list shows that 'glpi' user has 'Super-Admin' authorization	It was checked that user has required authorization. 	OK
GLPI _PLUGIN_1	Any page	Click/Right upper menu -> Setup -> Plugins	The plugins Setup page is displayed, showing all installed plugins	Plugins setup page is displayed correctly. 	OK
GLPI _PLUGIN_2	Plugins Setup page	No action	The "FusionInventory" plugin is installed and enabled	Required plugin is ok.	OK

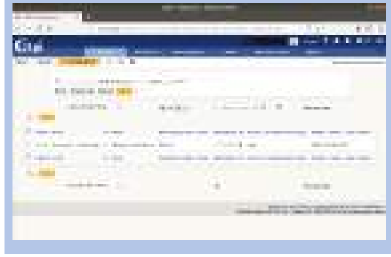
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
					
GLPI _ASSETS_1	Any page	Click Assets upper menu	The assets dashboard is displayed, showing all inventoried assets by categories	The assets dashboard contains all required information. 	OK
GLPI _ASSETS_2	Any page	Click Assets upper menu -> Computers	The inventoried computers are displayed in a list.	List is displayed correctly. 	OK
GLPI _ASSETS_3	Computers list	Click list first entry	The corresponding computer is displayed, showing detailed inventory data with left tabs 'Computer', 'Operating systems', Software	Computer is displayed correctly.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
GLPI_API_1	Any page	Click upper right button 'My settings'	The 'My settings' page is displayed and an API token is set	API page is displayed correctly.	OK
GLPI_API_2	Any page	Click menu Setup -> General, then 'API' tabs on the left	The API setup page is displayed	API setup page is displayed correctly. 	OK
GLPI_API_3	API setup page	No action	'Enable Rest API' dropdown must be set to 'Yes'	Dropdown is correctly set to ‘Yes’. 	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
GLPI_API_4	API setup page	No action	API client list must contain entries for SATIE tools	Required SATIE tools are present. 	OK
GLPI_API_5	API setup page	Click on second list entry	The corresponding API client entry is displayed and an 'app_token' is set	The token is set correctly.	OK
GLPI_VULN_1	Any page	Click Right upper menu -> Tools ->Vulnerabilities	The list of vulnerabilities imported from VIP is displayed	List is displayed correctly. 	OK
GLPI_VULN_2	BHS Computers list	Click on last entry	The computer is displayed, showing detailed inventory data with the left tab 'Vulnerabilities' containing a number	The tab contains a number.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
GLPI_VULN_3	Previous computer entry	Click on 'Vulnerabilities' left tab	The list of vulnerabilities affecting computer is displayed	List is displayed correctly. 	OK
GLPI_VULN_4	Previous vulnerabilities list	Click on list first entry	The details of the corresponding vulnerability are displayed	Details are displayed correctly.	OK
GLPI_I_VIP_1	Vulnerability plugin scripts directory	Launch the vip_import.php script	GLPI is able to connect to VIP web service and a success return code is returned by the script	Script connects to VIP and is able to download vulnerabilities.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
GLPI_I_VIP_2	Vulnerability plugin scripts directory	Launch the vip_import.php script	GLPI is able to import vulnerability data from VIP and a success return code is returned by the script	Script connects to VIP, is able to download vulnerabilities and to import them into GLPI.  	OK
GLPI _I_BHS_1	Computers list	In search panel, click second dropdown, enter 'fusion', select 'FusionInventory tag', click third dropdown, select 'contains', in right field, enter 'bhs', click 'Search'	The inventoried computers of the BHS are displayed in a list	By searching in inventoried assets, it was possible to find BHS machines. 	OK
GLPI _I_BHS_2	Computers list after having searched 'FusionInventory tag' containing 'bhs'	Click first list entry, then 'Computer' tab on the left, then scroll to 'FusionInventory' section	The last contact date is displayed and must be less than 24 hours from current time	By accessing BHS computer entry, it was possible to check that FusionInventory Agent was working properly.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
GLPI _I_ATM_1	Computers list	In search panel, click second dropdown, enter 'fusion', select 'FusionInventory tag', click third dropdown, select 'contains', in right field, enter 'swim', click 'Search'	The inventoried computers of the Secured ATM Services are displayed in a list	By searching in inventoried assets it was possible to find Secured ATM Services machines. 	OK
GLPI _I_ATM_2	Computers list after having searched 'FusionInventory tag' containing 'swim'	Click first list entry, then 'Operating systems' tab on the left	The operating system of the computer is displayed	By accessing computer entry, it was possible to check the operating system version.	OK

11.14 Vulnerability Intelligence Platform (VIP)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
VIP_C_L1	login	Access the application inserting the username and password and clicking "submit"	See the first collect page with data	Collect page with list of vulnerabilities.	OK
VIP_C_L2	logout	Click on the logout item in the menu	See the login page	Login page.	OK
VIP_C_S1	Administration > scanner	Select the NIST scanner, click on the standalone scan button of the toolbar.	A popup is open with a message. After some minutes, the scan should be finished. Refresh the page. The status of the NIST scanner has to be ok and its date has to be modified.	Popup with a message: “The command has been created. It will be processed as soon as possible”. Refresh after some minutes, the date is updated and the status is OK.	OK
VIP_C_V1	Public data > vulnerabilities	All vulnerabilities are provided in a paginated list	Vulnerabilities should be displayed.	List of vulnerabilities displayed.	OK
VIP_C_V2	Rest > vulnerabilities	curl -k -u <login>:<password> https://<vip-collect> /collect/rest/vulnerabilities	A JSON containing vulnerabilities	Curl command returned the vulnerabilities in a JSON.	OK
VIP_M_L1	login	Access the application inserting the username and password and clicking "submit"	See the first collect page with data	Management page with list of open tickets.	OK
VIP_M_L2	logout	Click on the logout item in the menu	See the login page	Login page.	OK
VIP_M_L3	Menu > profile	Click on the change password button. Complete the expected fields to change password	See a success message. Logout and login to check the new password.	Success message, new password is working.	OK
VIP_M_U1	Administration > users	All users are provided in a list	Users should be displayed.	List of users.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
VIP_M_U2	Administration > users	Click on create user button. Complete the expected fields. Click on create button.	The new user should be present in the users list.	New user in the list.	OK
VIP_M_O1	Administration > organizations	All organizations are provided in a list	Organizations should be displayed	List of organizations.	OK
VIP_M_O2	Administration > organizations	Click on create organization button. Complete expected fields. Click on create button.	The new organization should be present in the organizations list.	New organization in the list.	OK
VIP_M_O3	Administration > organizations > users	Select a user to add and click on the add user button	The user should be displayed in the organization user list.	User added to the organization.	OK
VIP_M_P1	Administration > organizations > projects	All projects of an organization are provided in a list	Projects of the organization should be displayed	List of projects of the organization.	OK
VIP_M_P2	Administration > organizations > projects	Click on the create project button. Complete expected fields. Click on create button.	The new project should be present in the projects list.	New project in the list.	OK
VIP_M_P3	Administration > organizations > projects > project	Show project detail	The project detail page of the selected project should be displayed.	Page with details of the projects.	OK
VIP_M_P4	Administration > organizations > projects > project > users	Select a user to add and click on the add user button	The user should be displayed in the project user list.	User present in the list.	OK
VIP_M_P5	Administration > organizations > projects > project > components	Click on the create component button. Complete the expected fields. Click on the create button.	The new component should be present in the component list.	New component in the component list.	OK
VIP _M_GLPI1	Administration > organizations > projects > project	Click on the GLPI synchronization button.	A message should be displayed. After some minutes, synchronization should be completed. Refresh the page to see the synchronized list of components.	Click on Run synchronisation, message displayed: “The synchronisation will be processed in few minutes”. After some minutes and a	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
				page refresh, the list of components is updated.	
VIP_M_CO1	Administration > Collect	Click on the collect synchronization item or execute curl command	After some minutes, last vulnerabilities from collect should be present in the database. curl -k -u <login>:<password> https://<vip-mgt>/mgt/rest/advisories?sort=-publish_date& limit=10	Click on collect synchronisation. “Vulnerability synchronisation with vip-collect will be processed in few minutes”. Curl command returns list of vulnerabilities in JSON format.	OK
VIP_M_A1	Administration > organizations > projects > project	Click on the launch analysis button.	A message should be displayed. After some minutes, analysis should be finished. The last analysis date of the project should be updated. New tickets on the project could be displayed (only if new vulnerabilities are in the database).	Click on “Run Analysis”, message displayed: “The analysis will be processed in few minutes”. The last analysis date of the project is updated.	OK
VIP_M_T1	tickets	All new and pending tickets of all projects are provided in a list	All new and pending tickets should be displayed	List of all pending tickets.	OK
VIP_M_T2	Projects > project > tickets	All tickets of a project are provided in a list	All tickets of a project should be displayed	List of tickets of the project.	OK
VIP_M_T3	Projects > project > tickets > ticket	Project has to have users. Open a new ticket detail. Click on the set pending button. Select the user and confirm.	The status and the assigned fields of the ticket should have changed.	Status changed to pending, Assignment changed to the user selected.	OK
VIP_M_T4	Projects > project > tickets > ticket	Open a pending ticket detail. Click on the set fix button.	The status field of the ticket should have changed.	Status is set to “PROCESSED”.	OK
VIP_M_T5	Projects > project > tickets > ticket	Open a pending ticket detail. Click on the set irrelevant button.	The status field of the ticket should have changed.	Status value is set to “IRRELEVANT“.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
VIP_M_T6	Rest > tickets	curl -k -u <login>:<password> https://<vip-mgt>/mgt/rest/tickets	A JSON containing tickets	Curl command returns a JSON with the tickets.	OK

11.15 Risk Integrated Service (RIS)

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
RIS_L1	Log in	Access the application inserting the username and password and clicking "Sign in".	See the enabled profiles (SATIE Project Owner) for the reference company.	The enabled profiles are seen.	OK
RIS_L2	Log in	Log-out of the application and re-access it inserting the username and password.	Operation went successfully.	Operation was successful.	OK
RIS_L3	Log in	Select the relevant profile.	After there should be the menu to select the project and scenario.	There is a menu to select the project and scenario.	OK
RIS_L4	Log in	Select the project and scenario pressing the button "Select."	After there should be a menu on the left with the following selections: -HOME -PROJECT -INTERMEDIARY REPORTS	There is a menu with the necessary selections.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
			-FINAL REPORTS -REPOSITORY		
RIS_L5	Log in	Select the option "Change Password" on the right of the top bar. Fill out the password fields and save.	Password will be saved successfully.	The password is saved.	OK
RIS_L6	Log in	Select the option "Logout" from the top bar on the right.	The user will be brought to the page to insert credentials for access.	Page successfully loaded.	OK
RIS_P1	PROJECT -> Project Settings	Access the project setting pages	A sub-menu opens underneath Project Settings with the following options: - Processes/Services - Asset Classes - Business Attributes - Threat Probabilities - Risk Matrix & Appetite - Scenario Configuration	The sub-menu opens.	OK
RIS_P2	PROJECT -> Project Settings -> Processes/Services	Access the processes to add (using the button "Create") and change existing ones (with the button "Edit").	Can successfully change or add processes.	Processes are modifiable.	OK
RIS_P3	PROJECT -> Project Settings -> Asset Classes	See the instantiated asset classes and	Can move asset classes between the "Asset Classes	Asset classes are able to be included or excluded.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
		optionally add or remove classes.	Available" and the "Asset Classes Selected" lists.		
RIS_P4	PROJECT -> Project Settings -> Business Attributes	Can see the instantiated business attributes and change which ones are instantiated.	Can move business attributes between the "Business Attributes Available" and "Business Attributes Selected" lists.	Business attributes are able to be included or excluded.	OK
RIS_P5	PROJECT -> Project Settings -> Threat Probabilities	See and change the probabilities of threats.	Double-click under the Probability column, select a different probability, and press "Save".	The probabilities are modifiable.	OK
RIS_P6	PROJECT -> Project Settings -> Scenario Configuration	Can freeze a scenario	From the Risk Processing menu, the Run Process button will be active.	The Run Process button is available.	OK
RIS_P7	PROJECT -> Project Settings -> Scenario Configuration	Unfreeze a scenario	Many of the menus will become read-only (e.g. Asset Inventory, Checklist Compiling).	The menu selection changes.	OK
RIS_P8	PROJECT -> Scenario Settings -> Checklist Scope	Can add or remove control objectives (security standards being analysed).	Control objectives should be able to move between the "Domains Instantiation" and "Checklist Instantiated" lists.	Control domains can be instantiated or not.	OK
RIS_P9	PROJECT -> Assets -> Asset Inventory	Access the Asset Inventory page and be able to edit the asset inventory.	Operation was successful; updated details are saved.	Asset details are editable.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
RIS_P10	PROJECT -> Assets -> Asset Inventory	Access the Asset Inventory page and create a new asset with the configuration wizard (general information, impacts, dependencies, threat probabilities).	Operation was successful through the configuration wizard.	New asset is creatable.	OK
RIS_P11	PROJECT -> Assets -> Asset Inventory	Extract the asset inventory as a CSV.	Extract was successful; a CSV file was downloaded.	Extract was successful.	OK
RIS_P12	PROJECT -> Checklist -> Compiling	Access the Compiling page of the Checklist, the control panel filters the list of questions accordingly after pressing the button "Go."	The questions visualized are filtered according to the selection.	Questions are visible and filterable.	OK
RIS_P13	PROJECT -> Risk Processing	Access the Risk Processing page.	The current scenario should be visualized with an active button to "Freeze" the scenario and once that has been selected, then to "Go to Process Page."	The scenario is visible, along with the Freeze button.	OK
RIS_P14	PROJECT -> Risk Processing -> Jobs & Reports	View current and past jobs.	Can see the current scenario with an active button next to it "Run Process."	The current scenario is visible with the Run Process button.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
RIS_R1	Intermediary Reports -> Risk Distribution	View results.	See a histogram with bars and a table below of assets and risk values. If a bar is clicked on, the table below is filtered according to that risk value.	A histogram is visible. Clicking on a bar filters the table below.	OK
RIS_R2	Intermediary Reports -> Process Risk Sheet	View results.	See a vertical histogram and table with sub-operations as labels and overall risk values.	There is a vertical histogram.	OK
RIS_R3	Intermediary Reports -> Asset Risk Sheet	View results according to assets.	There should be a pull-down menu with a list of assets; when one is selected, risk values, criticality, and biggest threat information is displayed.	There is a pull-down menu with assets, which changes the results shown.	OK
RIS_R4	Intermediary Reports -> Threat Risk Sheet	View results according to threats.	View a table with threats and risk values. If the arrow next to a threat is selected, the impacted assets are then displayed.	A table is visible. Dialog boxes appear after clicking on the arrow.	OK
RIS_R5	Final Reports -> All About Assets	Access the page and see the results.	See a histogram with values and a bar graph.	A histogram and bar graph are visible.	OK
RIS_R6	Final Reports -> All About Assets -> Overview	Access the page and see the results.	When the sections are expanded, tables should be visible with risk values for each line.	Tables with risk values are visible.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
RIS_R7	Final Reports -> All About Assets -> Process In-depth	Access the page and see the results.	There should be a bar graph and table visible. If a process filter is selected on the top of the page, the table should filter accordingly.	There is a bar graph and table visible. The table is filterable.	OK
RIS_R8	Final Reports -> All About Assets -> Asset In-depth	Access the page and see the results.	See a histogram with values, a horizontal bar graph with varying colours, and below a table with asset names and risk values. If parts of the upper graphs are clicked on, the table should filter accordingly. If the button "Analyse" next to an asset is clicked, the page should redirect to one called "Asset Risk Sheet."	A histogram is visible which is filterable.	OK
RIS_R9	Final Reports -> All About Assets -> System In-depth	Access the page and see the results.	See a histogram and table below.	A histogram and table are visible.	OK
RIS_R10	Final Reports -> All About Assets -> Trends	Access the page and see the results.	See a plot with at least one data point.	A plot with one datapoint is visible.	OK
RIS_R11	Final Reports -> All About Assets -> Asset Comparison	Access the page and see the results.	It is possible to select an asset from a pull-down menu next to "Asset Selected" along with at least one scenario in the menus for "Scenario #1" and "Scenario #2." After these	Assets are available in two pull-down menus and their risk values are shown.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
			selections are made, risk and criticality information should appear.		
RIS_R12	Final Reports -> All About Assets -> Scenario Comparison	Access the page and see the results.	See two pull-down menus in the area "Scenario Selection" where it is possible to select from at least one scenario. After a scenario is selected, a histogram appears.	The scenario is available in two pull-down menus and the results are displayed.	OK
RIS_R13	Final Reports -> All About Risk	Access the page and see the results.	There should be two figures visible with multiple circles representing how many risks are at that criticality and risk value.	There are two bubble charts.	OK
RIS_R14	Final Reports -> All About Risk -> Risk Breakdown	Access the page and see the results.	See a bubble plot (figure with multiple circles) and a table listing assets and their risk values. If the button under "Analyse" is clicked for an asset, the page should be redirected to one titled "Asset Risk Sheet."	There is a bubble plot and table of risk values.	OK
RIS_R15	Final Reports -> All About Risk -> Managed Risks	Access the page and see the results.	See a bubble plot (figure with multiple circles) and a histogram below. If a process and sub-process are selected and the button "Go" pressed at the top, both figures	There is a bubble plot and histogram.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
			should be filtered accordingly.		
RIS_R16	Final Reports -> All About Risk -> Threats In-depth	Access the page and see the results.	There should be a bar graph and a table below it with threats and risk values for each threat. If a bar is clicked on, a pop-up window should list assets and risk values. Similarly, if the number in the table under "Number of Affected Assets" is selected, the same pop-up window should appear.	There is a bar graph and table with threats and risk values.	OK
RIS_R17	Final Reports -> All About Risk -> Vulnerabilities In-depth	Access the page and see the results.	There should be a bar graph and a table below with the same information: threat names and risk levels. If a bar is clicked on, a pop-up window should display a list of assets and risk values. If the number in the table under "Number of Affected Assets" is selected, the same pop-up window should appear.	There is a bar graph and table with vulnerabilities and risk values.	OK
RIS_R18	Final Reports -> Top Results	Access the page and see the results.	See two horizontal bar graphs with	There are two horizontal bar graphs.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
RIS_R19	Final Reports -> Top Results -> Worst 10 Controls	Access the page and see the results.	View two histograms with ascending values for the controls and of the objectives with the lowest application levels. Below are large icons of those controls, which when clicked on, show a description and the relevant questions used to evaluate that control.	A histogram is visible with dialog boxes that appear after clicking on a threat.	OK
RIS_R20	Final Reports -> Top Results -> Worst 10 Vulnerabilities	Access the page and see the results.	See a histogram with descending exposure levels for vulnerabilities. Below are large icons of those vulnerabilities, which when clicked on, show a description of the vulnerability and the relevant controls and questions used to evaluate the vulnerability.	A histogram is visible with dialog boxes that appear after clicking on a vulnerability.	OK
RIS_R21	Final Reports -> Top Results -> Worst 10 Assets	Access the page and see the results.	View a histogram, which can be filtered, of the overall risks per sub-operation.	A histogram is visible and filterable.	OK
RIS_G_AR1	Airport Operator	Click the button “Request GLPI Asset Inventory” and receive the JSONs.	Receive an “Asset messages received successfully” message and no error messages.	Message received correctly.	OK

TEST CASE ID	PAGE	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
RIS_G_AU1	Airport Operator	Click the “Update Asset Inventory” button.	Receive a “Inventory Updated” message and no error messages.	Assets are updated successfully.	OK
RIS_G_VR1	Airport Operator	Click the “Request GLPI Vulnerability Updates” button and receive the JSONs.	Receive a “Vulnerability messages received successfully” message and no error messages.	N.A.	--
RIS_G_VU1	Airport Operator	Click the “Update Vulnerability Exposure” button.	Receive a “Vulnerability Exposure updated successfully” message and no error messages.	N.A.	--

11.16 Incident Management Portal (IMP)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IMP_L1	Log in	Access the application inserting the username and password and clicking "Submit"	Main page of the application, at the Top Right you can see your profile with the username	Main page of the application.	OK
IMP_L2	Log in	Log-out of the application and re-access it inserting the username and password.	Operation went successfully.	Operation went successfully.	OK
IMP_L3	Log in	Select the option "Change Password" on the right of the top	Password will be saved successfully.	New password is saved successfully.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
		bar. Fill out the password fields and Submit.			
IMP_L4	Log in	Select the option "Logout" from the top bar on the right.	The user will be brought to the page to insert credentials for access.	Page to insert credential.	OK
IMP_L5	Log in	Access the application inserting the username new password and clicking "Submit"	Main page of the application	Main page of the application.	OK
IMP P1	Dashboard	Access the dashboard page	Number of open alert and incident for each severity and total. Graphical that show the history of alert and incident.	Dashboard page is displayed.	OK
IMP P2	Alerts and incident	Click on Alerts and Incident on the left vertical bar	List of alert and incidents	List of alert and incidents displayed.	OK
IMP P3	Alerts and incident	List of alert and incidents, Filter on severity “High” and status “Opened”	See only the event with severity “High” and status “Opened”	The list show only the events High and Opened.	OK
IMP P4	Alerts and incident	Click on that title of an alert	Detail page of the alert, in the equipment part you can see the Source and Target	Page with the details of the alert.	OK
IMP_P5	Alerts and incident	on the right of the top bar, click on My assignment	The page of alerts and incidents is display filter with only the alerts and incidents assigned to the operator	The alert displayed are all assign to the operator.	OK
IMP _ALERT1	Alerts and incident	Click right on an alert, Convert to incident	The alert is converted to an incident	An incident is created with the alert.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IMP _ALERT2	Alerts and incident	Select several alerts, click right, Convert to incident	The alerts are converted to an incident	An incident is created with all the alerts.	OK
IMP _ALERT3	Alerts and incident	Click right on an alert, Close	The alert is closed	Status of the alert is closed.	OK
IMP _ALERT4	Alerts and incident	Click right on an alert, Reopen	The alert is reopened	Status of the alert is reopened.	OK
IMP _ALERT5	Alerts and incident	Select several alerts or incident, Click right, Close	The alerts are closed	Status of the alerts are closed.	OK
IMP _ALERT6	Alerts and incident	Click right on an alert, Assign	You can select operator and submit. The name of the operator is in the fields “Operators”	Alert is assigned to an operator.	OK
IMP _ALERT7	Alerts and incident	Click right on an alert assign to the operator, Remove assignment	The operator is no longer assigned to the alert or incident (The name in the fields Operators is removed)	Alert is no longer assigned.	OK
IMP _ALERT8	Alerts and incident	Click right on an alert, Export	A CSV file is downloaded	A CSV file is downloaded.	OK
IMP _ALERT9	Alerts and incident	Click right on an alert, Edit, Requalified Severity	The severity of the alert as changed	The severity of the alert is changed.	OK
IMP_ALERT10	Alerts and incident	Click right on an alert that was requalified, Reinitialize severity	The severity of the alert is the default one	The severity of the alert is the default one.	OK
IMP_VIP1	Alerts and incident/detail page of an alert	An alert with an artefact of application type. Right click on the application artefact, external actions, get vulnerability from VIP	A popup with the result, the result can be saved in the analysis of the alert	The analysis contains the information about the vulnerability.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IMP_SEND1	Alerts and incident	On the alert classify on Incident, right click, external action, send incident	A popup with a final status OK.	A popup with a final status OK.	OK
IMP_LINK1	Alerts and incident	Right click on an alert, external action, Open Graylog Alert	A web page of the Correlation Engine is open that shows the alert.	A web page of the Correlation Engine is open that shows the alert.	OK
IMP_LINK2	Alerts and incident	Right click on an alert, external action, Open Graylog Event	A web page of the Correlation Engine is open that shows the events of the alert.	A web page of the Correlation Engine is open that shows the events of the alert.	OK
IMP_LINK3	Alerts and incident	Right click on an alert, external action, Open Impact Assessment	A web page of the Impact assessment is opened.	A web page of the Impact assessment is opened.	OK
IMP_LINK4	Alerts and incident	Right click on an incident, external action, Open Impact Propagation	A web page of the Impact assessment is opened for the incident.	A web page of the Impact assessment is opened for the incident.	OK

11.17 Single-Sign-On (SSO) Solution

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
SSO_L1	https://<sso_server>:8443/auth	Connect to the SSO login page	The login page is displayed on the browser	Login page displayed.	OK
SSO_L2	https://<sso_server>:8443/auth	Log in with username and password	The login page display 'is authenticated'	Page with a "Green tick" and text: "is authenticated".	OK
SSO_L3	https://<sso_server>:8443/auth	Log in with wrong username and / or password	The login page display 'An error occurred	Error page.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
			Invalid credentials’		
SSO_L4	https://<sso_server>:8443/auth/chooseschema.jsp?sourceURL=https%3A%2F%2F<manager_server>%3A8443%2F manager%2Floginsso	Log in with username and password to Cymid Manager through SSO authentication	The user is redirected to the manager and its authorized view is displayed	Manager page, view with the SATIE application displayed.	OK
SSO_L5	https://<manager_server:8443>/manager/portal or portal icon, represented by a computer screen	Log in to an application through SSO authentication. SSO_L4 should be performed before this test	The user is log in the application.	Test with Cymerius application. We are automatically log in to the application.	OK
SSO_L6	https://<sso_server>:8443/signandgo	Log in with administrator user to the SSO server web interface	The SSO server web interface is displayed	The SSO server web interface is displayed.	OK
SSO_C1	https://<manager_server>:8443/manager/administration/applications or administration icon represented by a gear and verticals bars -> applications	Log in to Cymid Manager with an administrator account and access the applications page	The configured applications are displayed	The configured applications are displayed.	OK
SSO_C2	https://<manager_server>:8443/manager/administration/detail/<application_uid> or administration icon represented by a gear and verticals bars -> applications -> <application_name>	Log in to Cymid Manager with an administrator account and access an application configuration page	The configuration of the application is displayed	Configuration displayed (Title, address, …).	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
SSO_C3	https://<manager_server>:8443/manager/administration/applications/detail/<application_uid> or administration icon represented by a gear and verticals bars -> applications -> <application_name>	Log in to Cymid Manager with an administrator account and update an application configuration Modify a field and click on 'update'.	The configuration of the application is updated and the list of the configured applications is displayed.	Configuration updated.	OK
SSO_C4	https://<manager_server>:8443/manager/administration/applications or administration icon represented by a gear and verticals bars -> applications	Log in to Cymid Manager with an administrator account and delete an application. Click on the trash for the desired application.	The application is deleted and doesn't appear in the list of the configured application anymore.	Application deleted.	OK
SSO_C5	https://<manager_server>:8443/manager/administration/profiles or administration icon represented by a gear and verticals bars -> profiles	Log in to Cymid Manager with an administrator account and access the profiles page	The configured profiles are displayed	The configured profiles are displayed.	OK
SSO_C6	https://<manager_server>:8443/manager/administration/profiles/detail/<profile_uid> > or administration icon represented by a gear and	Log in to Cymid Manager with an administrator account and access a profile configuration page	The configuration of the profile is displayed	The configuration of the profile is displayed.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
	verticals bars -> profiles -> <profile_name>				
SSO_C7	https://<manager_server>:8443/manager/administration/profiles/detail/<profile_uid> or administration icon represented by a gear and verticals bars -> profiles -> <profile_name>	Log in to Cymid Manager with an administrator account and update a profile configuration Modify a field and click on 'update'.	The configuration of the profile is updated and the list of the configured profile is displayed.	The configuration of the profile is updated and the list of the configured profile is displayed.	OK
SSO_C8	https://<manager_server>:8443/manager/administration/profiles or administration icon represented by a gear and verticals bars -> profiles	Log in to Cymid Manager with an administrator account and delete a profile. Click on the trash for the desired profile.	The profile is deleted and doesn't appear in the list of the configured profile anymore.	The profile is deleted.	OK
SSO_C9	https://<manager_server>:8443/manager/administration/users or administration icon represented by a gear and verticals bars -> Advanced Search	Log in to Cymid Manager with an administrator account and access the users page	The configured users are displayed	The configured users are displayed.	OK
SSO_C10	https://<manager_server>:8443/manager/administration/users/detail/<user_uid> or	Log in to Cymid Manager with an administrator account and access a user configuration page	The configuration of the user is displayed	The configuration of the user is displayed.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
	administration icon represented by a gear and verticals bars -> Advanced Search -> <user_name>				
SSO_C11	https://<manager_server>:8443/manager/administration/users/detail/<user_uid> or administration icon represented by a gear and verticals bars -> Advanced Search -> <user_name>	Log in to Cymid Manager with an administrator account and update a user configuration Modify a field and click on 'update'.	The configuration of the user is updated and the list of the configured users is displayed.	The configuration of the user is updated and the list of the configured users is displayed.	OK
SSO_C12	https://<manager_server>:8443/manager/administration/users/detail/<user_uid> or administration icon represented by a gear and verticals bars -> Advanced Search -> <user_name>	Log in to Cymid Manager with an administrator account and add a profile to a user. Click on the 'Profiles' list and check the profile to add then click on update.	The profile is added to the user.	The profile is added to the user.	OK
SSO_C13	https://<manager_server>:8443/manager/administration/users/detail/<user_uid> or administration icon represented by a gear and verticals bars -> Advanced Search -> <user_name>	Log in to Cymid Manager with an administrator account and add a specific right to a user. Click on the 'Access Rights' list and check the right to add then click on update.	The right is added to the user.	The right is added to the user.	OK
SSO_C14	https://<manager_server>:8443/manager/administration/users	Log in to Cymid Manager with an administrator account and update a user password	The password update interface is displayed.	Password successfully changed; the user can log in with his new password.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
	or administration icon represented by a gear and verticals bars -> Advanced Search	Click on the password icon represented by a key. Enter the new password twice and click on update. Try test SSO_L4 with the updated user.	The user can log in with his new password		
SSO_C15	https://<manager_server>:8443/manager/configuration/resources or configuration icon represented by a hammer and a wrench -> resources	Log in to Cymid Manager with an administrator account and access the resources page	The configured resources are displayed	The configured resources are displayed.	OK
SSO_C16	https://<manager_server>:8443/manager/configuration/resources/detail/<resource_uid> or configuration icon represented by a hammer and a wrench -> resources -> <resource_name>	Log in to Cymid Manager with an administrator account and access a resource configuration page	The configuration of the resource is displayed	The configuration of the resource is displayed.	OK
SSO_C17	https://<manager_server>:8443/manager/configuration/resources/detail/<resource_uid> or configuration icon represented by a hammer and a wrench -> resources -> <resource_name>	Log in to Cymid Manager with an administrator account and update a resource configuration Modify a field and click on 'update'.	The configuration of the resource is updated and the list of the configured resources is displayed.	The configuration of the resource is updated and the list of the configured resources is displayed.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
SSO_C18	https://<manager_server>:8443/manager/configuration/resources or configuration icon represented by a hammer and a wrench -> resources	Log in to Cymid Manager with an administrator account and delete a resource. Click on the trash for the desired resource.	The resource is deleted and doesn't appear in the list of the configured resource anymore.	The resource is deleted and doesn't appear in the list of the configured resource anymore.	OK
SSO_C19	https://<manager_server>:8443/manager/configuration/rights or configuration icon represented by a hammer and a wrench -> rights	Log in to Cymid Manager with an administrator account and access the rights page	The configured rights are displayed	The configured rights are displayed.	OK
SSO_C20	https://<manager_server>:8443/manager/configuration/rights/detail/<right_uid> or configuration icon represented by a hammer and a wrench -> rights -> <right_name>	Log in to Cymid Manager with an administrator account and access a right configuration page	The configuration of the right is displayed	The configuration of the right is displayed.	OK
SSO_C21	https://<manager_server>:8443/manager/configuration/rights/detail/<right_uid> or configuration icon represented by a hammer and a wrench -> rights -> <right_name>	Log in to Cymid Manager with an administrator account and update a right configuration Modify a field and click on 'update'.	The configuration of the right is updated and the list of the configured right is displayed.	The configuration of the right is updated and the list of the configured right is displayed.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
SSO_C22	https://<manager_server>:8443/manager/configuration/rights/detail/<right_uid> or configuration icon represented by a hammer and a wrench -> rights -> <right_name>	Log in to Cymid Manager with an administrator account and delete a right. Click on the trash for the desired right.	The right is deleted and doesn't appear in the list of the configured rights anymore.	The right is deleted and doesn't appear in the list of the configured rights anymore.	OK
SSO_A1	https://<manager_server>:8443/manager	Log in to Cymid Manager with an administrator account	The configured applications are displayed On the top right the following icons are visible: • Administration - represented by a gear and verticals bars • Configuration - represented by a hammer and a wrench • Portal - represented by a computer screen • Logout - represented by a user picture On the left panel under 'Consultation' the following selection is displayed: • Applications • Gateways • Devices • Organizations • Profiles • User Templates	All panels displayed and icons available.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
SSO_A2	https://<manager_server>:8443/manager/configuration/ or configuration icon represented by a hammer and a wrench	Log in to Cymid Manager with an administrator account and try to access the configuration page. Click on the Configuration icon	The configured resources are displayed On the top right the following icons are visible: • Administration - represented by a gear and verticals bars • Configuration - represented by a hammer and a wrench • Portal - represented by a computer screen • Logout - represented by a user picture On the left panel under 'Model Administration' the following selection is displayed: • Resources types • Rights • Applications • Organizations User Templates	All panels displayed and icons available.	OK
SSO_A3	https://<manager_server>:8443/manager/portal or portal icon represented by a computer screen	Log in to Cymid Manager with an administrator account and try to access the portal page. Click on the portal icon	The configured applications for the administrator user are displayed. On the top right the following icons are visible: • Administration - represented by a gear and verticals bars • Configuration - represented by a hammer and a wrench • Portal - represented by a computer screen	All panels displayed and icons available.	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
			- Logout - represented by a user picture On the left panel under 'Consultation' the following selection is displayed: My applications		
SSO_A4	https://<manager_server>:8443/manager/administration/applications or administration icon represented by a gear and verticals bars -> applications	Log in to Cymid Manager with an administrator account and try to access the applications page. Click on the administration icon then on Applications.	The configured applications are displayed.	The configured applications are displayed.	OK
SSO_A5	https://<manager_server>:8443/manager/administration/profiles or administration icon represented by a gear and verticals bars -> profiles	Log in to Cymid Manager with an administrator account and try to access the profiles page. Click on the administration icon then on Profiles.	The configured profiles are displayed.	The configured profiles are displayed.	OK
SSO_A6	https://<manager_server>:8443/manager/administration/users or administration icon represented by a gear and verticals bars -> Advanced Search	Log in to Cymid Manager with an administrator account and try to access the users page. Click on the administration icon then on Advanced Search.	The configured users are displayed.	The configured users are displayed.	OK
SSO_A7	https://<manager_server>:8443/manager	Log in to Cymid Manager with an operator account	The configured applications for the operator user are displayed.	Top right 2 icons, Portal and logout. On the left panel under	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
			On the top right the following icons are visible: • Portal - represented by a computer screen • Logout - represented by a user picture And the following icons should NOT be visible: • Administration - represented by a gear and verticals bars • Configuration - represented by a hammer and a wrench On the left panel under 'Consultation' the following selection is displayed: My application	'Consultation' the following selection is displayed: My application.	
SSO_A8	https://<manager_server>:8443/manager/<any other url but the portal>	Log in to Cymid Manager with an operator account and try to access another page than the portal	The portal page is displayed	Redirection to the portal page.	OK
SSO_R1	https://<manager_server>:8443/manager/portal	Click on Graylog icon	The Graylog application is opened	The Graylog application is opened.	OK
SSO_R2	https://<manager_server>:8443/manager/portal	Click on Cymerius icon	The IMP (Cymerius application) is opened	The IMP (Cymerius application) is opened.	OK
SSO_R3	https://<manager_server>:8443/manager/portal	Click on Orion icon	The Orion application is opened	The Orion application is opened.	OK
SSO_R4	https://<manager_server>:8443/manager/portal	Click on Impact Propagation icon	The Impact Propagation application is opened	The main page of the IPS is opened.	OK

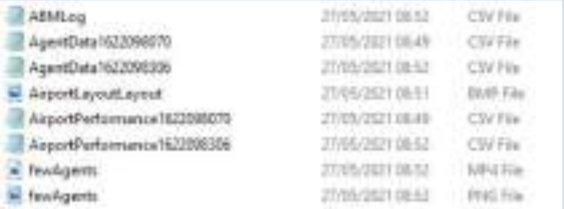
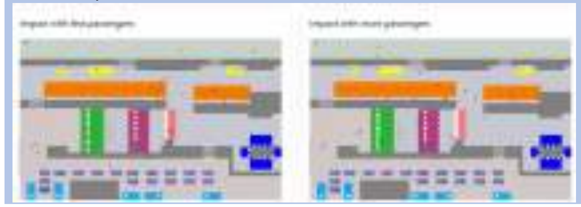
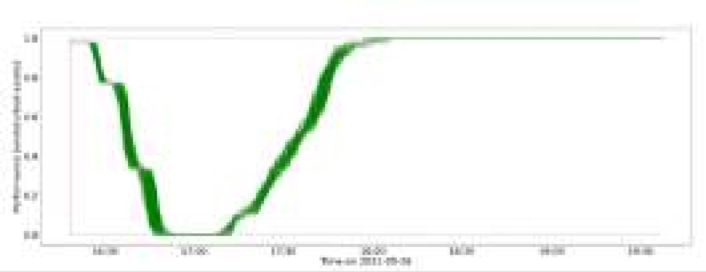
11.18 Investigation Tool (SMS-I)

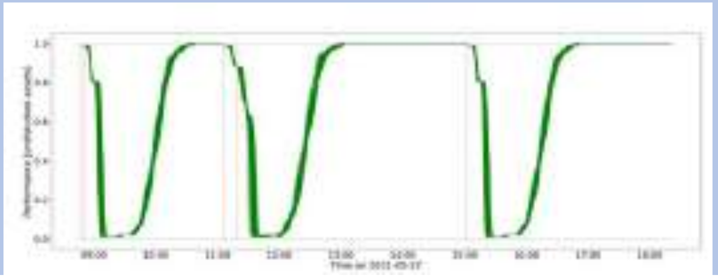
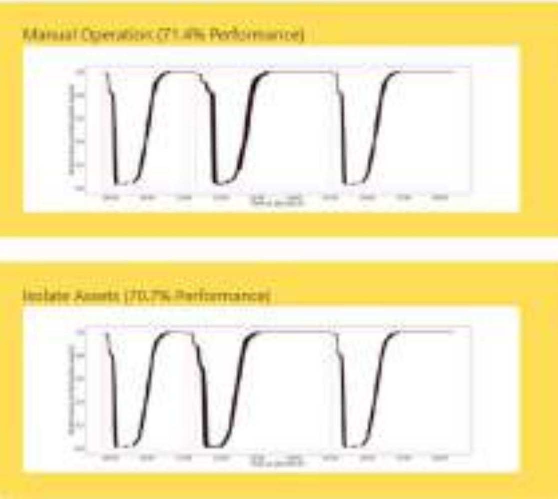
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
SMS-I_L_1	Log in	Access the application inserting the username and password and clicking "Sign in"	View Menus and details of SMS-I	The user is successfully logged in and has access to all View Menus and details of SMS-I.	OK
SMS-I_L_2	Log In	Log-out of the application and access again by inserting the username and password.	The operation went successfully	The user is successfully logged out and is redirected to the login page. When he enters his credentials, he is able to log in successfully.	OK
SMS-I _DASH_1	Dashboards	Click in dashboards and visualize the dashboard options.	View all dashboards options	When the user clicks in “Main Dashboard”, he is able to view all the available dashboard options.	OK
SMS-I _DASH_2	Dashboards	Select any dashboard option.	View the corresponding dashboard	When the user selects any dashboard option (e.g. Alerts Dashboard), the appropriate page is displayed.	OK
SMS-I _ALERT_1	Alerts	Select “Alerts” button.	View latest alerts list	When the user clicks either on “Open Alerts” or “Closed Alerts”, he is able to see the latest alerts list.	OK
SMS-I _ALERT_2	Alerts	Select “Alert Details”.	View the alert details	Clicking on any alert card of the list allows the user to visualize the details of the selected alert.	OK
SMS-I_ML_1	Machine Learning	In “Alert Details” the Machine Learning classification suggestion should be displayed.	View the ML results	In the alert details, the user is able to see the Machine Learning classification	OK

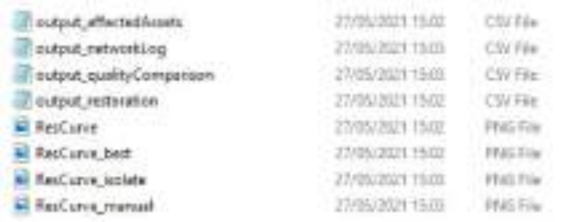
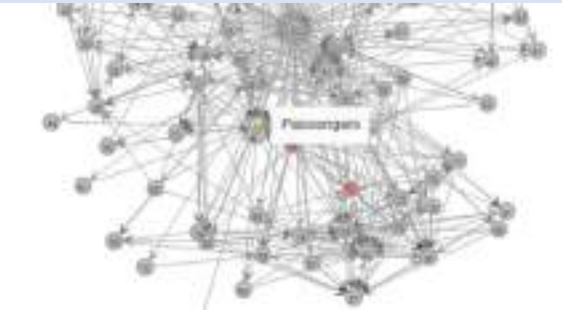
TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
				suggestion under the section “Is Incident”.	
SMS-I _SYNC_1	Synchronization	Data synchronization is triggered by time (e.g. every 10 minutes) or by clicking “Download Latest”	The Elastic Search database is updated	When the synchronization mechanism is triggered by a remote API call (e.g. a scheduled task), event, alert, and incident related data is fetched from both the IMP and the Correlation Engine, pre-processed, and stored in Elastic Search.	OK
SMS-I _SYNC_1	Synchronization	After synchronization, the SMS-I should produce logs with a summary related to the operation	New log records are produced.	After the synchronization mechanism is executed, the logs with the operation summary are saved in the Elastic Search.	OK

11.19 Impact Propagation Simulation (IPS)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IPS_ABM_1	Varying agent arrival (spawn) rate	ABM executed in Python on VM.	Longer queues (Q) for larger spawn rates (SR).	SR = 1/7 -> 0 to 5 passengers in Q of security check SR = 1/20 -> 0 to 1 passenger in Q of security check	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IPS_ABM_2	Varying number of simulation time steps	ABM executed in Python on VM.	Longer simulation time for more time steps.	1000 time steps -> 120 s 500 time steps -> 21 s	OK
IPS_ABM_3	Output files	ABM executed in Python on VM.	ABMLog.csv AgentData*.csv AirportPerformance*.csv AirportLayoutLayout.bmp fewAgents.mp4 fewAgents.png	All files were properly produced:  ABMLog 27/05/2021 08:52 CSV File AgentData1622098070 27/05/2021 08:49 CSV File AgentData1622098306 27/05/2021 08:52 CSV File AirportLayoutLayout 27/05/2021 08:51 BMP File AirportPerformance1622098070 27/05/2021 08:49 CSV File AirportPerformance1622098306 27/05/2021 08:52 CSV File fewAgents 27/05/2021 08:52 MP4 File fewAgents 27/05/2021 08:52 PNG File	OK
IPS_ABM_4	Simulate impact of predefined incident in ABM with different number of agents.	ABM executed in Python on VM.	Observe and visualize the impact.	The impact in the ABM is presented in videos which are created for two different numbers of agents to start the simulation (25 and 35): 	OK
IPS_NET_1	Start simulation with one randomly placed incident acting on one node.	NET executed in Python on VM.	Observe and visualize the impact propagation.	The incident is presented in the performance plot as vertical red line. The performance drops due to the incident: 	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IPS_NET_2	Start simulation with several placed incidents with time delay.	NET executed in Python on VM.	Observe and visualize the impact propagation.	The series of incidents is presented in the performance plot as vertical red lines: 	OK
IPS_NET_3	Test predefined mitigation options for a specified incident.	NET executed in Python on VM. Mitigation options implemented.	Observe and visualize the impact propagation for different mitigation options.	Two mitigation options (manual operation and isolate assets) are compared with two plots: 	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IPS_NET_4	Output files	NET executed in Python on VM.	output_affectedAssets.csv output_networkLog.csv output_qualityComparison.csv output_restoration.csv ResCurve.png ResCurve_best.png ResCurve_isolate.png ResCurve_manual.png	All files were properly produced:  output_affectedAssets 27/05/2021 15:02 CSV File output_networkLog 27/05/2021 15:03 CSV File output_qualityComparison 27/05/2021 15:03 CSV File output_restoration 27/05/2021 15:02 CSV File ResCurve 27/05/2021 15:02 PNG File ResCurve_best 27/05/2021 15:02 PNG File ResCurve_isolate 27/05/2021 15:03 PNG File ResCurve_manual 27/05/2021 15:03 PNG File	OK
IPS_HY_1	Receive incident that directly triggers ABM from NET.	NET triggered by received incident. Connection to IMP. Interface between NET and ABM.	Locate the indicated asset in the network and ABM.	Passengers are identified as an asset that network and ABM have in common: 	OK
IPS_HY_2	*removed*				

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
IPS_HY_3	Provide access to the results of HY_1 and interpret the visualization.	NET triggered by received incident. Connection to IMP. Interface between NET and ABM. Connection to CAS and IMP to provide results to user.	The results are correctly displayed in CAS and IMP.	This test has been successfully performed during the simulations.	OK
IPS_CON_1	Receive incident from Incident Management Portal (IMP) to test impact propagation.	NET triggered by received incident. Connection to IMP and consistent asset inventory.	Locate the indicated asset in the network. Observe and visualize the impact propagation.	This test has been successfully performed during the simulations.	OK
IPS_CON_2	Send a dummy post request to CAS with the message ID “xyz”.	Incident and simulated results are able to be forwarded to CAS.	JSON with entries: “messageId”:”xyz”,”response”:”FORWARDED”	Connection to CAS is completed as expected.	OK

11.20 Crisis Alerting System (CAS)

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
CAS _LOGIN_1	Login page	User inserts his credentials (username/password).	User has access to the main CAS UI. The functionalities and information that are provided are in accordance with the user's access rights and role.	The users managed to log into the CAS and what they had access to was according to their roles.	OK
CAS_INT_1	"Alarms Management" perspective	User is logged in. The "Alarms Management" perspective is selected.	User has access to the list of the active alarms. This list contains alarms that are either created manually by the CAS operators or received by the SOC (SATIE Tool Incident Management Portal). The alarms that are received by the SOC are highlighted with a specific icon.	User has access to the list of the active alarms. This list contains alarms that are either created manually by the CAS operators or received by the SOC (SATIE Tool Incident Management Portal). The alarms, created by incidents that are received by the SOC are marked with the IMP incident id.	OK
CAS_INT_2	"Alarms Management" perspective	User is logged in. The "Alarms Management" perspective is selected and user selects a specific incident from the list of active alarms.	Information related to the impact propagation of the selected alarm is depicted to user. This information is received by the SOC (SATIE Tool Impact Propagation Simulation).	Information related to the impact propagation of the selected alarm, regarding an IMP incident is depicted to user. This information is received by the SOC (SATIE Tool Impact Propagation Simulation).	OK
CAS_INT_3	"Alarms Management" and "Collaboration" perspectives	User is logged in. The "Alarms Management" or the	User has access to the list of operational information that is	Information from the SOC is visible through the Details	OK

TEST CASE ID	PAGE/SETTING	CONDITION	EXPECTED RESULTS	OBTAINED RESULTS	STATUS (OK, NOT)
		“Collaboration” perspective is selected.	collected by the security and safety systems of the airports and the SOC in the “Alarms” perspective. Information is also presented on a specialized map view in the “Collaboration” perspective.	view. The map is used to present information regarding the collaboration of the AOC with the public safety agencies.	
CAS _SHARE_1	“Collaboration” perspective	User is logged in. The “Collaboration” perspective is selected.	User is able to exchange information (operational information, locations on the map, and text and multimedia messages) with the involved actors, responders, and safety agencies.	The AOC operator exchanges information with public safety agencies through the collaboration perspective. All information exchanged can also visible on the map, if selected by the user.	OK
CAS _SHARE_2	“Alarms Management” perspective	User is logged in. The “Alarms Management” perspective is selected.	User is able to send notifications and alerts the passengers and the public in the vicinity of installations.	The notifications can be sent as emails or SMS messages to lists of recipients.	OK

12 Annex 3 – Detailed results of validation questionnaire

12.1 Standard validation questionnaires

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
System Usability Scale						
Statements	Pre Post	**57.50** **47.50**	**80.00** **92.5**	**67.17** **61.83**	**2.02** **11.04**	**15** **15**
SUS01	I think that I would like to use this solution frequently.	4.00 3.00	5.00 5.00	4.20 3.87	0.41 0.64	15 15
SUS02	I found the solution unnecessarily complex.	2.00 2.00	4.00 4.00	2.40 2.53	0.63 0.74	15 15
SUS03	I thought the solution was easy to use.	2.00 2.00	5.00 5.00	3.87 3.67	0.83 0.72	15 15
SUS04	I think that I would need the support of a technical person to be able to use this solution.	1.00 1.00	3.00 4.00	2.33 3.00	0.72 1.00	15 15
SUS05	I found the various functions in this solution were well integrated.	2.00 2.00	5.00 5.00	4.07 4.00	0.88 0.76	15 15
SUS06	I thought there was too much inconsistency in this solution.	1.00 1.00	5.00 4.00	2.33 2.53	1.18 0.83	15 15
SUS07	I would imagine that most people would learn to use this solution very quickly.	2.00 3.00	4.00 4.00	3.53 3.40	0.64 0.50	15 15

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
SUS08	I found the solution very cumbersome/awkward to use.	1.00 1.00	4.00 4.00	2.33 2.40	0.82 0.91	15 15
SUS09	I felt very confident using the solution.	3.00 3.00	5.00 5.00	3.73 3.67	0.59 0.82	15 15
SUS10	I needed to learn a lot of things before I could get going with this solution.	1.00 1.00	4.00 5.00	3.13 3.40	0.99 0.98	15 15
State-Trait Anxiety Inventory (SITA)						
Statements (In the previous working period, I felt that …)	Pre Post	**3.00** **2.00**	**5.67** **6.00**	**4.32** **3.63**	**0.80** **1.33**	**15** **15**
SITA01	... the solution was useful.	3.00 2.00	6.00 6.00	4.53 3.80	1.12 1.52	15 15
SITA02	... the solution was reliable.	3.00 2.00	6.00 6.00	4.53 3.67	1.87 1.45	15 15
SITA03	... the solution worked accurately.	3.00 2.00	6.00 6.00	4.73 3.67	1.1 1.34	15 15
SITA04	... the solution was understandable.	0.00 2.00	6.00 6.00	3.67 3.47	1.91 1.36	15 15
SITA05	... the solution worked robustly (e.g. it did not freeze or crash).	2.00 2.00	6.00 6.00	3.93 3.60	1.58 1.45	15 15
SITA06	... I was confident when working with the solution.	3.00 2.00	6.00 6.00	4.53 3.60	1.06 1.45	**15** **15**

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
Workload						
Statements	Pre Post	**2.25** **1.93**	**4.56** **5.57**	**3.47** **3.32**	**0.70** **0.91**	**15** **15**
Workload01	... gather and interpret information?	2.00 2.00	6.00 6.00	3.87 3.40	1.10 0.99	14 15
Workload02	... integrate information from various sources to form a picture?	2.00 2.00	6.00 6.00	3.77 3.60	1.01 1.12	13 15
Workload03	... anticipate the future situation?	2.00 2.00	5.00 6.00	3.33 3.40	0.89 1.06	12 15
Workload04	... verify information sources?	2.00 2.00	5.00 6.00	3.57 3.73	0.85 1.03	14 15
Workload05	... recall necessary information?	1.00 1.00	4.00 6.00	3.08 3.33	0.95 1.29	13 15
Workload06	... access relevant information?	2.00 2.00	6.00 5.00	3.57 3.40	1.28 0.83	14 15.
Workload07	... manage information?	2.00 1.00	5.00 6.00	3.64 3.20	0.75 1.21	14 15
Workload08	... identify potential threats (e.g. via VuMS)?	3.00 2.00	4.00 7.00	3.60 3.53	0.52 1.25	10 15
Workload09	... recognize an attack (e.g. via the alerts)?	2.00 2.00	7.00 5.00	3.33 2.93	1.83 1.03	12 15
Workload10	... understand all information displayed by the system?	1.00 2.00	7.00 6.00	4.00 3.47	1.60 1.13	15 15

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
Workload11	… evaluate the consequences of an plan (e.g. via IPS)?	3.00 2.00	6.00 5.00	4.11 3.25	1.27 0.97	9 12
Workload12	… generate mitigation options?	1.00 2.00	5.00 6.00	3.45 3.38	1.13 1.19	11 13
Workload13	… prioritize alerts, security and safety response and recovery actions?	2.00 1.00	4.00 6.00	3.20 3.20	0.68 1.15	15 15
Workload14	… share information with other parties (e.g. SOC, AOC, first responders, general public)?	1.00 1.00	6.00 4.00	2.53 2.67	1.19 0.90	15 15

12.2 General validation questions

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
General validation						
Statements	Pre Post	**5.22** **4.33**	**6.82** **6.72**	**6.04** **5.84**	**0.47** **0.62**	**15** **15**
Gen01	The solution is overall a significant improvement compared to your current security-monitoring system.	4.00 4.00	7.00 7.00	6.27 6.00	0.88 0.88	15 15
Gen02	The solution is acceptable as a way to monitor and raise security alerts.	4.00 5.00	7.00 7.00	6.33 6.00	0.82 0.56	15 15
Gen03	The solution provides accurate and up-to-date information.	6.00 5.00	7.00 7.00	6.47 6.07	0.52 0.83	15 15

Ref		Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
	Gen04	It is intuitive to interact with the solution.	4.00 4.00	7.00 7.00	5.73 5.80	0.80 1.08	15 15
	Gen05	The solution provides all relevant information.	5.00 4.00	7.00 7.00	6.36 5.92	0.63 0.95	14 15
	Gen06	The solution enables a faster detection of cyber threats compared to your current situation.	5.00 4.00	7.00 7.00	6.40 6.08	0.74 0.86	15 15
	Gen07	The solution enables a faster detection of physical threats compared to your current situation.	5.00 4.00	7.00 7.00	6.15 6.21	0.69 0.89	13 15
	Gen08	The solution enables a faster response to cyber threats compared to your current situation.	6.00 3.00	7.00 7.00	6.53 5.71	0.52 1.20	15 15
	Gen09	The solution enables a faster response to physical threats compared to your current situation.	5.00 4.00	7.00 7.00	6.38 6.14	0.65 0.77	13 15
	Gen10	The use of the unified SATIE solution increases the efficiency compared to your current situation.	4.00 4.00	7.00 7.00	6.27 5.79	0.88 1.12	15 15
	Gen11	The use of the unified SATIE solution increases the efficiency compared to using the unconnected Innovation Elements (Incident Management Portal, Crisis Alerting System, etc.) and no Correlation Engine.	5.00 4.00	7.00 7.00	6.60 6.17	0.63 1.12	15 15
	Gen12	It is easy to integrate the solution with the necessary airport systems.	3.00 3.00	7.00 7.00	5.14 4.73	1.23 1.56	14 15
	Gen13	The solution is innovative compared to others on the market.	4.00 4.00	7.00 7.00	5.54 6.00	1.33 1.00	13 15
	Gen14	The solution boosts revenues.	2.00 1.00	7.00 6.00	4.62 4.17	1.66 2.23	13 15

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
Gen15	I wish to secure my system using the SATIE solution.	4.00 4.00	7.00 7.00	5.36 5.78	1.01 1.09	14 15
Gen16	I think that the attack could have happened under the presented circumstances.	2.00 3.00	7.00 7.00	5.73 5.67	1.44 0.98	15 15
Gen17	I understood the flow of events in the attack.	5.00 5.00	7.00 7.00	6.20 6.07	0.56 0.70	15 15
Gen18	The simulation on the CyberRange worked flawlessly.	3.00 4.00	7.00 7.00	6.13 5.93	1.13 0.96	15 15

12.3 Bespoke validation questions

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
Risk Integrated Service (RIS)						
Statements	Overall	**5.00**	**6.83**	**5.91**	**0.63**	**11**
IE01xNISS01	I trust the results to be accurate.	6.00	7.00	6.27	0.47	11
IE01xNISS02	The interface is user friendly.	4.00	7.00	6.20	1.03	10
IE01xNISS03	RIS displays the results in a useful format.	5.00	7.00	6.00	0.82	10
IE01xNISS04	I understand how to interpret the risk values of assets.	5.00	7.00	5.73	0.79	11
IE01xNISS05	I understand how to interpret the risks associated with threats.	5.00	7.00	5.82	0.87	11

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE01xNISS06	The "what-if" scenarios help identify the best countermeasures to take.	4.00	7.00	5.38	0.92	8
How-Question	Overall	**4.00**	**7.00**	**5.67**	**1.21**	**6**
IE01xNISH01	How much more useful is this risk assessment approach compared to the one currently in place?	4.00	7.00	5.67	1.21	6
Vulnerability Intelligence Platform (VIP)						
Statements	Overall	**5.00**	**6.75**	**6.00**	**0.69**	**6**
IE02xACSS01	The information about the Common Vulnerabilities and Exposures (CVE) is easily understandable.	5.00	6.00	5.83	0.41	6
IE02xACSS02	I trusted the list of vulnerabilities (Common Vulnerabilities and Exposures) to be up to date.	5.00	7.00	6.17	0.75	6
IE02xACSS03	The information about possible impacted assets is easily understandable.	5.00	7.00	6.00	0.89	6
IE02xACSS04	I trusted the list of vulnerabilities (Common Vulnerabilities and Exposures) to be accurate.	5.00	7.00	6.00	0.89	6
Gestion Libre de Parc Informatique (GLPI)						
Statements	Overall	**4.00**	**6.67**	**5.67**	**0.90**	**6**
IE02xTLBS01	[Incident] There is enough information in an alert to identify the particular asset impacted.	4.00	7.00	5.50	1.05	6
IE02xTLBS02	I trust the asset information to be up-to-date.	6.00	7.00	6.20	0.45	5

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE02xTLBS03	The asset information in GLPI correctly reflects the information in my airport system.	4.00	7.00	5.80	1.10	5
IE02xTLBS04	I trust the vulnerability information to be accurate.	6.00	7.00	6.50	0.58	4
IE02xTLBS05	I can easily find additional information about the asset or vulnerability in the incident.	6.00	7.00	6.25	0.50	4
IE02xTLBS06	The information about assets and vulnerabilities is easy to understand.	5.00	6.00	5.80	0.45	5
How-Question	Overall	**6.00**	**7.00**	**6.25**	**0.50**	**4**
IE02xTLBH01	How beneficial (how much information is gained) is it to access GLPI specifically?	6.00	7.00	6.25	0.50	4
Secured Communication on the BHS (ComSEC)						
Statements	Overall	**2.67**	**7.00**	**5.39**	**1.34**	**9**
IE03INOVS01	I think that deploying ComSEC would raise the airport infrastructure security compared to the current situation.	3.00	7.00	5.56	1.33	9
IE03INOVS02	The possibility to receive ComSEC alerts via Kafka. syslog. or email is compatible with the current security operations centre.	3.00	7.00	5.00	1.58	5
IE03INOVS03	The ComSEC alerts are informative enough to pinpoint cyber-attacks.	2.00	7.00	5.29	1.60	7
Unified Access Control						
Statements	Overall	**5.60**	**7.00**	**6.36**	**0.48**	**9**

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE04xIDES01	The dual authentication (Face + finger or card) is useful against fraud.	6.00	7.00	6.56	0.53	9
IE04xIDES02	The tailgating detection is useful. (tailgating = unauthorized person following an authorized person into a secured area)	6.00	7.00	6.67	0.50	9
IE04xIDES03	The detection of threats that are unrelated to the access workflow is useful.	5.00	7.00	6.22	0.67	9
IE04xIDES04	The contactless aspects of this solution (e.g. capturing a fingerprint without touching a surface) are essential for end-users.	4.00	7.00	6.00	1.00	9
IE04xIDES05	I think that the end-users will like to use this solution.	5.00	7.00	6.33	0.71	9
How-questions	Overall	**5.00**	**7.00**	**6.05**	**0.76**	**10**
IE04xIDEH01	How easy is it to integrate the Unified Access Control solutions in your eco-system?	3.00	7.00	5.00	1.41	6
IE04xIDEH02	How important it is to differentiate "group access rights" between different type of employees?	5.00	7.00	6.50	0.71	10
Anomaly Detection on Passenger Records						
Statements	Overall	**1.00**	**6.80**	**5.63**	**2.08**	**7**
IE05xIDES01	The information in alerts generated by passenger data anomaly detection is easy to understand.	1.00	7.00	5.86	2.19	7
IE05xIDES02	The information in alerts generated by passenger data anomaly detection is useful.	6.00	7.00	6.83	0.41	6
IE05xIDES03	The passenger data anomaly detection is useful for my day-to-day work.	6.00	7.00	6.50	0.58	4

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE05xIDES04	The passenger data anomaly detection is easy to integrate into my existing system.	3.00	7.00	5.33	2.08	3
IE05xIDES05	The passenger data anomaly detection improves the threat detection.	6.00	7.00	6.83	0.41	6
IE05xIDES06	I am interested in more anomaly detection functions like the use of other watch lists (SLTD. TDAWN) or a business rules engine.	5.00	7.00	6.00	0.63	6
IE05xIDES07	The baggage registration service is easy to understand.	6.00	7.00	6.33	0.58	3
IE05xIDES08	The baggage registration service is easy to use.	6.00	6.00	6.00	0.00	3
IE05xIDES09	The baggage registration service is useful in my day-to-day work.	6.00	6.00	6.00	0.00	2
IE05xIDES10	The baggage registration service is accurate enough to be used in day-to-day operations.	6.00	7.00	6.33	0.58	3
Secured ATM Services						
Statements	Overall	**5.50**	**7.00**	**6.33**	**0.55**	**10**
IE06xFQSS01	The possibility of the Incident Management to adjust the Threat Level of the ATM Service is useful.	5.00	7.00	6.10	0.74	10
IE06xFQSS02	The correlated alert is received early enough to provide sufficient time to react.	6.00	7.00	6.50	0.53	10
IE06xFQSS03	The alerts are improving my detection of attacks compared to my current system.	5.00	7.00	6.33	0.87	9
IE06xFQSS04	The alerts are improving my time to detect attacks compared to my current system.	5.00	7.00	6.44	0.73	9

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
How-questions	Overall	**5.50**	**7.00**	**6.33**	**0.56**	**9**
IE06xFQSH01	How useful is the provision of individual alerts (e.g. for Brute Force Attack. or DOS Attack)?	6.00	7.00	6.56	0.53	9
IE06xFQSH02	How much added value is generated by correlation of different alerts (e.g.. DOS + physical door intrusion)?	5.00	7.00	6.11	0.78	9
Traffic Management and Intrusion Compliance System (TraMICS)						
Statements	Overall	**5.00**	**7.00**	**6.47**	**0.69**	**10**
IE07xDLRS01	The combination of TraMICS single alerts and the TraMICS security situation indicator is useful.	5.00	7.00	6.50	0.71	10
IE07xDLRS02	*Statement removed due to modifications to the tool.*					
IE07xDLRS03	The TraMICS security situation indicator is received early enough to identify a potential coordinated attack.	4.00	7.00	6.20	1.14	10
IE07xDLRS04	The TraMICS information is useful in the context of Airport Operations/Security.	5.00	7.00	6.67	0.71	9
How-questions	Overall	**5.00**	**7.00**	**6.30**	**0.82**	**10**
IE07xDLRH01	How useful are the TraMICS single alerts?	5.00	7.00	6.40	0.70	10
IE07xDLRH02	How useful is the TraMICS security situation indicator?	4.00	7.00	6.20	1.03	10
Business Process-based Intrusion Detection System (BP-IDS)						
Statements	Overall	**4.00**	**7.00**	**5.50**	**1.13**	**8**
IE08INOVS01	I think that deploying BP-IDS would increase airport infrastructure security compared to the current situation.	4.00	7.00	5.63	1.19	8

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE08INOVS02	The possibility to receive BP-IDS alerts via Kafka. syslog. or email is compatible with the current security operations centre.	4.00	7.00	5.33	1.21	6
IE08INOVS03	The BP-IDS alerts are informative enough to pinpoint cyber-attacks.	4.00	7.00	5.86	1.07	7
Malware Analyser						
Statements	Overall	**5.00**	**7.00**	**6.25**	**0.60**	**8**
IE08xACSS01	The report of an analysed file provides easily understandable.	5.00	7.00	6.13	0.64	8
IE08xACSS02	The report of an analysed file provides useful information.	5.00	7.00	6.38	0.74	8
Application Layer Cyber-Attack Detection (ALCAD)						
	No bespoke validation questions were drafted for this IE as there is no user interaction.					
Correlation Engine						
Statements	Overall	**5.00**	**6.63**	**5.99**	**0.47**	**9**
IE09xACSS01	The alerts generated by the Correlation Engine are easily understandable.	4.00	7.00	5.78	0.83	9
IE09xACSS02	The alerts generated by the Correlation Engine give enough information about the possible threat.	5.00	7.00	6.00	0.50	9
IE09xACSS03	The cyber-physical alerts generated by the Correlation Engine are relevant.	5.00	7.00	6.00	0.50	9
IE09xACSS04	The alerts generated by the Correlation Engine are received in a timely manner.	6.00	7.00	6.33	0.50	9

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE09xACSS05	The alerts generated by the Correlation Engine have added value compared to the events coming from the other IEs.	6.00	7.00	6.22	0.44	9
IE09xACSS06	I trust the alerts generated by the Correlation Engine to be accurate.	6.00	7.00	6.22	0.44	9
IE09xACSS07	The rules are easily understandable.	4.00	6.00	5.67	0.71	9
IE09xACSS08	It is easy to see the events that trigged alerts from the Correlation Engine.	3.00	7.00	5.67	1.23	9
Investigation Tool (SMS-I)						
Statements	Overall Pre Post	**6.00** **5.00**	**7.00** **6.63**	**6.49** **5.84**	**0.32** **0.62**	**7** **7**
IE10ISEPS01	The interface is user friendly.	6.00 4.00	7.00 6.00	6.43 5.43	0.54 0.79	7 7
IE10ISEPS02	The dashboards display useful information.	6.00 5.00	7.00 7.00	6.57 5.86	0.54 0.69	7 7
IE10ISEPS03	The dashboards simplify the analysis of open incidents.	5.00 5.00	7.00 7.00	6.29 5.71	0.76 0.76	7 7
IE10ISEPS04	The dashboards bring awareness to suspicious alerts or events.	6.00 5.00	7.00 7.00	6.71 5.86	0.49 0.69	7 7
IE10ISEPS05	The statistics and probabilities derived from machine learning are helpful during the decision making process.	5.00 4.00	7.00 7.00	6.00 5.57	0.63 0.98	6 7
IE10ISEPS06	The Investigation Tool improves the efficiency and organization of the SOC.	6.00 5.00	7.00 7.00	6.43 6.14	0.54 0.90	7 7

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE10ISEPS07	I trust the graphics. metrics. and probabilities displayed.	6.00 5.00	7.00 7.00	6.71 6.14	0.49 0.90	7 7
IE10ISEPS08	The dashboards display critical information.	6.00 5.00	7.00 7.00	6.71 6.00	0.49 0.82	7 7
Business Impact Assessment (BIA)						
Statements	Overall	**2.50**	**6.75**	**5.54**	**1.50**	**7**
IE11INOVS01	The BIA simulations are useful to predict the impact of cyber-attacks.	2.00	7.00	5.43	1.90	7
IE11INOVS02	BIA allows me to understand which business processes could be impacted by a threat.	2.00	7.00	5.57	1.72	7
IE11INOVS03	It is easy to run a BIA simulation and visualize the results.	4.00	7.00	5.57	1.13	7
IE11INOVS04	The BIA allows me to understand which assets could be impacted by a threat.	2.00	7.00	5.57	1.72	7
Impact Propagation Simulation (IPS)						
Statements	Overall	**4.50**	**6.83**	**6.07**	**0.75**	**13**
IE11xFHGS01	The Impact Propagation Simulation provides useful decision support.	4.00	7.00	6.23	0.93	13
IE11xFHGS02	The Network Model is easy to understand.	3.00	7.00	5.92	1.32	13
IE11xFHGS03	The Agent-Based Model provides additional detailed insights compared to the Network Model.	4.00	7.00	6.08	0.95	13
IE11xFHGS04	I would implement the Impact Propagation Simulation to improve my airport operation.	4.00	7.00	6.00	1.00	11

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE11xFHGS05	The mitigation options are well defined.	4.00	7.00	5.92	0.76	13
IE11xFHGS06	The Impact Propagation Simulation is a better tool than the existing. if any. impact propagation support.	5.00	7.00	6.30	0.68	10
Incident Management Portal (IMP)						
Statements	Overall Pre Post	**5.76** **5.12**	**6.81** **6.94**	**6.26** **6.13**	**0.34** **0.55**	**10** **10**
IE12xACSS01	The alert received are easily understandable.	6.00 5.00	7.00 7.00	6.30 6.30	0.48 0.68	10
IE12xACSS02	The alert received have enough information about the possible threat.	5.00 5.00	7.00 7.00	6.00 5.90	0.50 0.74	9
IE12xACSS03	The interface is user friendly.	6.00 6.00	7.00 7.00	6.20 6.20	0.42 0.42	10
IE12xACSS04	It's easy to go to the source of the alert and see the events in the Correlation Engine (graylog) from the Incident Management Portal.	6.00 5.00	7.00 7.00	6.13 6.10	0.35 0.74	8
IE12xACSS05	It's easy to see the impact propagation of an alert by switching to the Impact Propagation Simulation.	6.00 5.00	7.00 7.00	6.25 6.20	0.46 0.63	8
IE12xACSS06	It's easy to see the business impact of an alert by switching to the Business Impact Assessment.	6.00 4.00	7.00 7.00	6.25 5.89	0.46 1.05	8
IE12xACSS07	The Incident management portal is useful.	6.00 6.00	7.00 7.00	6.44 6.50	0.53 0.53	9
IE12xACSS08	I would like to use the Incident Management Portal in my day-to-day work.	5.00 5.00	7.00 7.00	6.20 6.13	0.79 0.84	10

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IE12xACSS09	The Incident Management Portal has added value compared to my current situation.	6.00 5.00	7.00 7.00	6.60 6.33	0.52 0.71	10
IE12xACSS10	The Incident Management Portal increases my situation awareness compared to my current situation.	5.00 5.00	7.00 7.00	6.50 6.22	0.71 0.67	10
IE12xACSS11	The Incident Management Portal reduces response times to alerts compared to my current situation.	5.00 5.00	7.00 7.00	6.40 6.22	0.70 0.67	10
IE12xACSS12	The Incident Management Portal improves my efficiency compared to my current situation.	6.00 5.00	7.00 7.00	6.50 6.00	0.53 0.87	10
IE12xACSS13	It's intuitive to convert an alert into an incident and thereby send it to the AOC.	5.00 5.00	7.00 7.00	6.50 6.30	0.71 0.68	10
IE12xACSS14	The Incident Management Portal improves my communication with the AOC compared to my current situation.	5.00 5.00	7.00 7.00	6.40 5.80	0.84 0.79	10
IE12xACSS15	The ability to close an incident is useful.	6.00 5.00	7.00 7.00	6.60 6.40	0.52 0.70	10
IE12xACSS16	The number of alerts and incidents does not increase my workload compared to my current situation.	3.00 3.00	7.00 7.00	5.00 5.56	1.41 1.24	9
IE12xACSS17	It's easy to filter the alerts and incidents.	5.00 5.00	7.00 7.00	6.00 6.10	0.47 0.88	10
Crisis Alerting System (CAS)						
Statements	Overall Pre Post	**5.80** **5.50**	**7.00** **7.00**	**6.55** **6.24**	**0.43** **0.49**	**8** **8**

Ref		Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
	IE13xSATS01	The CAS improves the collaboration between the AOC and law enforcement agencies compared to my current situation.	6.00 4.00	7.00 7.00	6.63 6.13	0.52 0.99	8 8
	IE13xSATS02	The CAS improves the collaboration inside the AOC compared to my current situation.	6.00 4.00	7.00 7.00	6.57 5.43	0.54 1.13	7 7
	IE13xSATS03	The CAS improves the collaboration between the AOC and the SOC compared to my current situation.	3.00 4.00	7.00 7.00	5.88 5.86	1.55 1.07	8 7
	IE13xSATS04	The CAS improves the notification of passengers that are affected by a specific incident compared to my current situation.	6.00 4.00	7.00 7.00	6.33 5.83	0.52 1.17	6 6
	IE13xSATS05	The CAS is useful.	7.00 6.00	7.00 7.00	7.00 6.75	0.00 0.46	7 8
	IE13xSATS06	The way that the CAS collects and visualizes the operational information from multiple sources is useful.	6.00 6.00	7.00 7.00	6.63 6.50	0.52 0.54	8 8
	IE13xSATS07	CAS provides a user-friendly and intuitive graphical user interface.	6.00 6.00	7.00 7.00	6.88 6.50	0.35 0.54	8 8
	IE13xSATS08	CAS informs AOC operators about the current incidents (that are related to the airport) and their possible impact.	6.00 6.00	7.00 7.00	6.75 6.63	0.46 0.52	8 8
CyberRange							
	Statement	Overall	**4.00**	**7.00**	**5.90**	**1.10**	**10**
	IE14xACSS01	The replication of the airport environment is realistic enough for the simulation of the scenarios.	4.00	7.00	5.90	1.10	10
Baggage Handling System (BHS)							
	Statement	Overall	**4.00**	**7.00**	**5.88**	**0.99**	**8**

Ref	Bespoke validation question	Minimum value	Maximum value	Average	Standard deviation	No. of replies
IExxxALSS01	The simulation of the Baggage Handling System is realistic enough for the simulated scenarios.	4.00	7.00	5.88	0.99	8