D7.2 Evaluation Protocol and KPIs

Work Package	7
Task	7.1
Authors	Jason Sioutis, Fabio Podda, Liivar Luts, Fabien Pornet
Dissemination Level	PU
Status	Final
Due Date	31/05/2022
Document Date	31/05/2022
Version Number	1.1

Quality Control

	Name	Organisation	Date
Editor	Jason Sioutis	ICCS	31/05/2022
Peer review 1	Pietro De Vito	STAM	27/05/2022
Peer review 2	Francesca Giampaolo	ENG	27/05/2022
Authorised by (Technical Coordinator)	Jason Sioutis	ICCS	30/05/2022
Authorised by (Quality Manager)	Vasileios Sourlas	ICCS	31/05/2022
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	31/05/2022

Contributors

Name	Organisation	Date
Jason Sioutis	ICCS	11/05/2022
Fabio Podda	AMT	09/05/2022
Liivar Luts	Tallinn	17/05/2022
Luca Bianconi	SIGLA	07/05/2022
Francesca Giampaolo	ENG	12/05/2022
Rosella Omana	ENG	12/05/2022
Alkiviadis Giannakoulias	ED	10/05/2022
Fabien Pornet	ACS	12/05/2022

Document Revision History

Version	Date	Modification	Partner
0.1	11/04/2022	ToC	ICCS
0.2	30/04/2022	First draft	ICCS
0.3	10/05/2022	Content updates	ICCS+AMT+Tallinn
0.4	18/05/2022	Further content updates	ICCS + ACS + ENG
0.5	23/05/2022	Final draft	ICCS
0.6	27/05/2022	Internal review	STAM+ENG
1.0	31/05/2022	Final version	ICCS
1.1	30/11/2022	Revised version	ICCS

Legal Disclaimer

CitySCAPE is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No. 883321. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. 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. The CitySCAPE Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of Contents

List of Tables

List of Abbreviations and Acronyms

Abbreviation	Meaning
ACS	Airbus Cyber Security
CPaaS	Communications Platform as a Service
CSIRP	Collaborative security incident response platform
CTI	computer-telephony integration
CTIP	Collaborative threat investigation platform
DoA	Description of Action
DX.X	Deliverable X.X
FIMCA	Financial impact assessment engine
GDPR	General Data Protection Regulation
ICCS	Institute of Communication and Computer Systems
IDS	Intrusion Detection Systems
IOC	Indicators of Compromise
IPS	Intrusion Prevention Systems
KSP	Kaspersky
MISP	Malware Information Sharing Platform
OX.	Objective X
RITA	Risk analysis and impact assessment engine
SIEM	SIEM as a Correlation engine with backlog of markers

Executive Summary

This deliverable addresses the Evaluation protocol that is to be set in order to evaluate the outcomes of the CitySCAPE pilots in Tallinn and in Genova.
In section 2 we present the project objectives that are relevant to the pilot demonstrations.
Section 3 provides a thorough description of the tools and methodologies that will be used for the technical evaluation of the CPaaS platforms of both pilots and the modules of the CitySCAPE toolkit.
Section 4 addresses the user acceptance methodology as part of the evaluation process and makes reference to the training sessions that will be provided along with the user satisfaction questionnaires that will be handed out.
The final section provides the conclusions from this deliverable.

1 INTRODUCTION

1.1 Project Introduction

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

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

More specifically, the CitySCAPE software toolkit will:

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

The project duration extends from September 2020 to August 2023.

1.2 Deliverable Purpose

The purpose of this deliverable is to provide a detailed description of the evaluation methodology that will be employed for the quantitative and qualitative evaluation of the CitySCAPE solution for creating a Cyber-Secure Multimodal Transport Ecosystem. To this end, the deliverable defines a clear set of evaluation objectives aimed at clarifying the target of the evaluation methodology. Previously, D2.1, D3.1, D3.2 and D3.3 presented an initial set of KPIs and metrics, aimed to set up the scene for the evaluation framework for the CPaaS platforms and the CitySCAPE toolkit, including also aspects related to Impact Assessment and User Acceptance. This aims to pave the way toward the evaluation of the CitySCAPE solution, eventually leading to the sought-after conclusions.
D7.2 aims to establish the evaluation methodology of the project by creating a relevant questionnaire to evaluate the modules provided on the CPaaS platforms of both pilot sites and the CitySCAPE toolkit performance in those pilots. The questionnaire addressing both pilots' CPaaS platforms and the respected CitySCAPE performance per pilot will be the same. This will help us to highlight the different aspects of CPaaS platforms presented in each pilot and the corresponding different services required from the CitySCAPE toolkit. The CPaaS questionnaire will compose of general questions focusing on general characteristics of the CPaaS, technical questions focusing on the functionalities of the CPaaS modules and their interoperability and scenario related questions evaluating whether the CPaaS can provide the necessary environment to perform the pilot scenarios described in the DoA, D2.1.

The CitySCAPE toolkit questionnaire will compose of general questions related to general characteristics and capabilities of the toolkit, technical questions focusing on the functionalities of the CitySCAPE modules and their interconnections, scenario related questions evaluating whether the pilot scenarios properly showcased the capabilities of CitySCAPE toolkit (aligned with the project objectives) and KPI metrics related to D3.2 indicating if the previously proposed KPIs were met during the pilot demonstrations.
Finally, a user acceptance evaluation methodology will be defined based on the training sessions and user satisfaction feedback from CitySCAPE toolkit users and SIGLA Moving solution users.
This deliverable sets the ground for the subsequent work in WP7, which will be reported in Deliverables 7.5 Pilot Evaluation and Knowledge capitalisation. The evaluation methodology presented here will be used in D7.5 to generate a relevant report for the pilots.

2 EVALUATION OBJECTIVES

In order to define the evaluation methodology, it is important that we first list the relevant CitySCAPE objectives. This section approaches those objectives and categorizes them into technical, impact and user acceptance objectives.

2.1 Technical evaluation objectives

There are 9 objectives defined in CitySCAPE DoA part B section 1.1 out of which 5 are technical ones (objectives 1, 2, 3, 5 and 7), 2 are related to user acceptance (objectives 4 and 8) and 3 of them are not relevant to the pilots (objectives 6 and 9) so we will not be taking them into account for the pilot Evaluation protocol.
The technical objectives on which the evaluation protocol should focus are the following:

- **O1.** (High level) Enhance cybersecurity technologies in the multimodal passenger transportation ecosystem at city-level addressing users and data privacy concerns.
  Measurable objective: CitySCAPE gathers a broad set of innovations that collectively contribute to a higher cybersecurity level. The successful integration and validation of the toolkit's full functionality in real conditions across all pilot sites is the main objective.
  Validation indicator: All below objectives and final achieved TRL.

- **O2.** (High level) Introduce risk analysis tools to identify threats and their propagation mechanism focusing on transport/digital infrastructure but also relevant in other NIS Directive critical sectors and assess the impact of a potential attack.
  Measurable objective: CitySCAPE will consider 4 NIS directive areas i.e., emphasis on transport and digital infrastructure but also address power and finance (banking) sector. CitySCAPE will introduce an innovative risk analysis methodology that will identify more than 6 common threats and vulnerabilities with a focus on Malware, Web-Based Attacks, Web Application Attacks, Phishing, Denial of Service for each considered combination of areas. Subsequently, an effective Risk analysis and (tech) impact assessment engine (RITA) will estimate potential cascading effects and the impact (in technical terms) of each attack on the system assets.
  Validation indicator: Number of common threats and vulnerabilities across the number of the considered NIS directives areas.

- **O3.** (High level) Improve the proactive approach of handling cybersecurity challenges and actively contribute to the predictability of threats in (regional) multimodal transport systems.
  Measurable objective: CitySCAPE introduces innovative methodologies and tools to offer prediction insights on upcoming cyberattacks. The aim is to use at least two past datasets (sequence

of events) provided by DNSC and verify that given a partial view of them, CitySCAPE accurately estimates the rest of the sequence.
Validation indicator: Testing against past data of attacks and confirmation of prediction accuracy.

- **O5.** (High level) Further strengthen the role of CERTs/CSIRTs by providing them with direct/real-time informative notifications about observed cybersecurity incidents and facilitating the collaborative (among such authorities) investigation of incidents in line with the NIS Directive.
  Measurable objective: The CitySCAPE consortium brings together one CERT authority and indirectly two other CSIRTs (the ACS CSIRT and the Swedish official National CERT through letters of support). To strengthen the role of the authorities CitySCAPE will seek to collaborate with at least one more by providing to all (external ones) the opportunity to participate to threat investigation and get real-time notification about observed incidents in multimodal transport during the realization of the pilots/demonstrators.
  Validation indicator: Number of external CERTs and CSIRTs collaborating on threat investigation or receiving the CitySCAPE incident notifications.

- **O7**. (High level) Showcase and validate the CitySCAPE solution efficiency in large scale pilot demonstrators involving all relevant entities and digital infrastructure of transport providers, under use cases of interest.
  Measurable objective: CitySCAPE solution efficiency will be tested in the Tallinn and Genoa large-scale pilots over use cases shaped by the end-users needs. The project will seek for at least two other European transport providers based on the existing collaboration links of CitySCAPE partners to test the solution and provide feedback by attending and testing the solution during the pilots.
  Validation indicator: Number of 'external' transport operators to test the proposed solution.

Objectives 1, 2 and 3 are technical objectives related to the effectiveness of the CitySCAPE modules, thus the methodology will focus on the performance of those modules. Objectives 5 and 7 are more related to the pilot scenarios and execution, thus another part of the methodology will focus on evaluating the scenarios of the pilots and whether they showcased the CitySCAPE solution as expected.

2.2 User acceptance objectives

The user acceptance objectives will also contribute towards composing the Evaluation Protocol. In CitySCAPE those objectives are focusing on user engagement and raising public awareness for cybersecurity professionals and non-professional users. The relevant objectives are the following:

- **O4.** Enhance end-user engagement towards the definition and provision of multimodal passenger transport requirements about digital security, privacy and personal data protection.
  Measurable objective: CitySCAPE will rely on the partners' contacts as well as high-impact dissemination activities to approach at least two other multimodal transport operators in order to collect further input data such as cybersecurity security requirements. The involvement of DXT (CS-Group) in the multimodal transport system of other cities works in favour of that.
  Validation indicator: Number of transport operators beyond the consortium members to provide requirements and feedback.

- **O8.** Raise security and privacy awareness, improve the capabilities of cybersecurity professionals as well as regular multimodal transport users and raise awareness on the involved security and privacy cyber-risks at European level.
  Measurable objective: CitySCAPE aims to train more than 10 cybersecurity experts with more than 2 coming from transport operators outside the consortium. Training sessions of regular passengers will cover multiple sessions with more than 50 online trainees in total.
  Validation indicator: Number of trainees.

The aforementioned objectives will also be addressed in the Evaluation protocol through measuring the effectiveness of the training programs that will be provided (as foreseen in the DoA) and the inclusion of the above-mentioned third-party experts (O4).

3 TECHNICAL EVALUATION METHODOLOGY

3.1 Evaluation methodology overview

The technical evaluation methodology will address the effectiveness of the modules used in the CitySCAPE pilots and will focus on the CPaaS pilot platform modules where the CitySCAPE toolkit will be deployed and the CitySCAPE toolkit itself.

3.1.1 CPaaS evaluation

This section provides the evaluation methodology that will be used to assess the CPaaS from a technical point of view. As deeply described in DoA and D4.1, the CPaaS used for the CitySCAPE piloting phases are clone-based instances of the production environment. For this reason, the technical assessment should focus on the adherence of the cloned CPaaS to the production environment for the purposes of the piloting activities, avoiding biases in the CitySCAPE toolkit testing that can influence the final evaluation. To summarize, CPaaS should not introduce new variables with respect to production environment.

3.1.1.1 Questionnaire

For the technical evaluation that has to be performed on the cloned CPaaS deployed within the Task 4.1 work, a questionnaire-like structure has been chosen to simplify both the evaluation definition and its execution. The following sub-sections contain the questions that should be asked when performing the assessment of the CPaaS. The chosen evaluators will thoroughly address those questionnaires, taking into consideration the objectives described in Section §2 of the current deliverable. Their elaborate answers will be presented in a second moment in the deliverable D7.5 Pilot Evaluation and Knowledge capitalisation (M36).

3.1.1.2 General

This section contains some high-level questions that are related to the general availability of the CPaaS and its work principles. The questions listed below, have the primary goal of assessing if the platform under analysis is integrable with the CitySCAPE toolkit from a generic point of view.

- Is the CPaaS accessible by system administrators?
- Are components of the CPaaS fully manageable? Are any limits/exceptions to be considered?
- Is CPaaS internal network fully accessible for inspections/traffic analysis?
- Are the deployments in line with the privacy regulations (GDPR)? Does monitoring of the CPaaS breach any privacy constraints?

- Is the "look and feel" of the cloned applications/appliances/services identical with respect to the production environment? Are there any major differences in the fidelity to the real-world system?
- Is the integration of the CPaaS with CitySCAPE seamless allowing easy repeatability for other multi-modal transportation environments/use-cases?

3.1.1.3 Technical

This section contains some questions that are related to the technical aspects of the CPaaS and how it has been deployed. The questions listed here have the primary goal of assessing if the platform under analysis is technically integrable with the CitySCAPE toolkit and if it does not introduce any new variable with respect to the production environment.

- Is the CPaaS completely separated from the production environment? How?
- What is the maximum difference between the production environment and the cloned CPaaS in terms of performances?
- Are the CPaaS module clearly identifiable by CitySCAPE tools? (i.e. are modules deployed independently or are they on the same host machine?)
- How many servers/machines/virtual machines have been deployed in the CPaaS?
- How many modules have been deployed in the CPaaS?
- How many ancillary services/modules have been deployed? Which are their main duties?
- Are the CPaaS performance in line with the production environment? (response time, latency, availability).
- Is the IDS/IPS integrable within the deployed CPaaS? How?
- Is the SIEM integrable within the deployed CPaaS? How?
- Were any changes to the infrastructure in the CPaaS required to accommodate the CitySCAPE tools? (i.e. encryption of network traffic)
- Is the CPaaS on-premise or in a hybrid or cloud/hosted environment?
- What is the freshness of the data in the CPaaS? Are release versions managed in the CPaaS?
- What are the troubleshooting mechanisms for system recovery?

3.1.1.4 Scenario-related

This section contains some questions that links the CPaaS deployment with the pilot scenarios defined in D2.1. The questions here have the main goal of assessing if the platform under analysis is linked with the scenarios and, in general, with the objectives of the pilot demonstration campaign as defined in the DoA.

- Is the CPaaS covering the needs of the use case scenario foreseen by the project (i.e. by D2.1 Multi-Modal Transport Ecosystem Use-Cases)?
- Are all modules of the deployed CPaaS involved in the scenarios foreseen by the project?

- Is it possible to gather the service topology from the mobile application?
- Is it possible to gather the real time transit information from the mobile application and the website?
- Is it possible to purchase electronic tickets within the mobile application?
- Is it possible to register the subscription card (a.k.a. “CityPass”) inside the mobile application?
- Is it possible to replicate data standards and flows of the Tallinn transport assets as described in the DoA?
- Does the CPaaS adhere to the GDPR and personal data privacy regulations mandated by Tallinn Transportation authorities?
- Does the CPaaS contain the data of the multi-modal transport journeys?
- Can the CPaaS enable the assessment of cyber security threats to availability of transportation modes?

3.1.2 CitySCAPE toolkit evaluation

This section provides the evaluation methodology that will be used to assess the CitySCAPE toolkit modules. The development of those modules take place in WP5 but the requirements have been also presented in D3.2.

3.1.2.1 Questionnaire

In order to perform the technical evaluation of the CitySCAPE modules deployed in WP5, we will use a questionnaire-like structure. The following sub-sections contain the questions that should be asked when performing the assessment of the CitySCAPE toolkit on a per-component basis.

3.1.2.2 General

This section contains some questions that are related to the general functionalities of the CitySCAPE toolkit. The questions listed in this section will be answered by the evaluators and a short explanation will be provided for each answer in a form of a short report.

	Very Unlikely	Somewhat Unlikely	Neutral	Somewhat Likely	Very Likely
Does the CitySCAPE toolkit accurately assess the security state of the multimodal transport?					
Is the CitySCAPE toolkit capable of robustly and hierarchically supporting risk modelling of the multimodal transport ecosystem?					
Does the CitySCAPE toolkit introduce innovative risk analysis methodologies and tools?					
Does the CitySCAPE toolkit support iterative risk and impact assessments on existing multimodal transport value chain assets?					
Does CitySCAPE introduce innovative methodologies and tools to offer prediction insights into upcoming cyberattacks?					
Does the CitySCAPE toolkit address user and data privacy concerns efficiently?					
Does the CitySCAPE toolkit communicate efficiently with the CERT/CSIRT network?					

Table 1: CitySCAPE toolkit general questions

3.1.2.3 Technical

This section contains a set of questions for each one of the components of the CitySCAPE toolkit. The questions are an outcome of the Each set of questions will be answered by the evaluators and a short explanation will be provided for each answer in a form of a short report. The questionnaire for each tool was based on the definition of the CitySCAPE system requirements (D3.2 System requirements of the CityScape solution section 2.3).

CTIP questionnaire

	Yes	No
Are the APIs available to the other CitySCAPE components (MISP API available to SIEM and CSIRP, OpenCTI API available to SIEM, CSIRP and RITA)?		
Is SIEM able to request IoCs from the CTIP?		
Is CSIRP able to push observables to CTIP?		
Is RITA receiving CAPEX numbers from CTIP?		
Can IoCs / SCOs be used as inputs from SHERLOCK's ENRICH & PIVOT processes?		
Are the outputs of SHERLOCK's ENRICH & PIVOT properly stored in CTIP according to STIX2.1 Standard?		
Are all the web services required for SHERLOCK' processes available?		

Table 2: CTIP technical questionnaire

CSIRP questionnaire

	Yes	No
Can the user log-in to the CSIRP?		
Can the user interact with the CSIRP?		
Is CSIRP able to push observables to CTIP?		
Can the user add a case?		
Can the user add a customer?		
Can the user generate a report?		
Can the user add an asset?		
Can the user add a timeline?		
Can the user add a task?		
Can the user register evidence?		
Can the user add a note?		
Can the user update a case?		

Table 3: CSIRP technical questionnaire

SIEM questionnaire

	Yes	No
Can the user log-in to the SIEM?		
Can the user interact with the SIEM?		
The SIEM received logs events from CPaaS?		
Can the user see the logs from the CPaaS?		
The logs are enriched with MISP?		
The user is able to search for IoC in the backlogs?		
The SIEM can raise an alert?		
From ElasticHunter can the user perform the search of IoCs in the backlog in a timerange?		
From ElasticHunter can the user relaunch the search to use the latest IoC?		
From ElasticHunter can the user navigate back to the source of compromise in Graylog?		
From ElasticHunter can the user see the history of searches in decreasing order of launches?		

Table 4: SIEM technical questionnaire

IPS/IDS questionnaire

	Totally disagree	Somewhat disagree	Neutral	Somewhat agree	Totally agree
Is the documentation and its overall contents satisfying?					
Is the IDS/IPS engine configurable and/or customisable? Can you change detection mode or create/edit detection rules?					
Can the IDS/IPS engine identify potential threats such as DOS attacks?					
Is the IDS/IPS engine automatically updated with community-defined rules?					
Is the accuracy of the Anomaly Detection Procedure satisfying?					
Can you easily update the Anomaly Detection Procedure model with new a legit/normal traffic dataset?					
Can you export alerts' information from the GUI?					
Is the overall performance satisfying?					

Table 5: IPS/IDS technical questionnaire

RITA questionnaire

	Totally disagree	Somewhat disagree	Neutral	Somewhat agree	Totally agree
Documentation availability and overall contents were sufficient.					
The RITA engine is easy to deploy.					
The RITA engine is configurable and/or customisable.					
The RITA engine can use interfaces to third party information sources, in order to receive vulnerability and threat feeds.					
The RITA engine can consume information from external sources regarding large-scale attacks, zero-day threats, etc.					
The RITA engine introduces new threats by itself (Security and privacy by design and by default).					
The RITA engine has great accuracy of risk and impact assessments.					
The RITA engine is extendable to support new and up-coming needs.					

Table 6: RITA technical questionnaire

FIMCA questionnaire

	Totally disagree	Somewhat disagree	Neutral	Somewhat agree	Totally agree
The functionalities of the FIMCA are clear					
The FIMCA engine need to be customized.					
The FIMCA engine interfaces are simple					
The fact that the integration of the FIMCA and RITA components are based on the well-known standards is a facilitating					
The FIMCA engine can use OpenAPI standard allowing each component to easily consume the REST API endpoints of another application.					
The FIMCA engine can be improved to implement additional needs					

Table 7: FIMCA technical questionnaire

3.1.2.4 Pilot scenario-related questionnaire

	Totally disagree	Somewhat disagree	Neutral	Somewhat agree	Totally agree
The CTIP module functionalities were adequately presented during the pilot					
The CSIRP module functionalities were adequately presented during the pilot					
The SIEM module functionalities were adequately presented during the pilot					
The IPS/IDS module functionalities were adequately presented during the pilot					
The RITA module functionalities were adequately presented during the pilot					
The FIMCA module functionalities were adequately presented during the pilot					
The CitySCAPE toolkit was tested against past data sets of attacks.					
A sufficient number of stakeholders (including CERT and CSIRT authorities) were participating in the CitySCAPE pilots					

3.1.2.5 CitySCAPE toolkit KPIs

Cityscape toolkit offers a list of services that supports the CISO and the risk manager of an organization to take decisions based on risk assessment, cost and benefit analysis, games to protect the data that no expert share online from cyber-attacks, the security monitoring and detection of cyber-attacks thanks to IDS/IPS.
One critical aspect of the evaluation methodology is the monitoring of the KPIs of the CitySCAPE components. Those KPIs were presented on D3.2 (System requirements of the CitySCAPE solution) section 2.4 and can be found on ANNEX 1 of this document. The evaluators will be asked to check if the thresholds of the KPIs per component are met and fill in a relevant report.

4 USER ACCEPTANCE METHODOLOGY

CitySCAPE will be hosting a number of training sessions to better approach professional and non-professional users as part of its user acceptance methodology. Additionally, a number of user satisfaction questionnaires will be handed out to be filled by the users and the evaluators.

4.1 Training sessions

CitySCAPE will provide the following three different training sessions:

1. Training sessions for non-IT experts organized and executed by KSP.
2. Training sessions for IT experts organized by ICCS and ACS using the Airbus Cyber-Range.
3. Two dedicated CSIRTs training sessions organized by DNSC.

All the training sessions will provide their own user satisfaction questionnaires to receive feedback over user acceptance once the training scenarios are defined. However, the training sessions themselves are considered to be part of the user acceptance methodology.

4.2 User satisfaction

Additionally, in the training sessions, separate user satisfaction questionnaires will be handed to all users for each CitySCAPE component, including the SIGLA moving app.

4.2.1 CitySCAPE toolkit users questionnaire per tool

The following user satisfaction questions are open questions where the users can provide their opinion and suggestions over different aspects of the toolkit components.

CTIP

- Are the interfaces user friendly?
- Does the CTIP modules (MISP, OpenCTI, SHERLOCK) feel like part of a unique platform?
- Is SHERLOCK easy to use?
- Are SHERLOCK's ENRICH & PIVOT processes easy to understand and to apply?
- Is the STIX2.1 model well implemented?
- The CTIP reduces response times compare to my current situation?
- The CTIP improves my efficiency compared to my current situation?
- The CTIP facilitates intelligence sharing with my partners ?
- The CTIP improves the pivoting capabilities compared to my current situation?

The CTIP is a useful addition to my SOC ecosystem of tools ?

CSIRP

- Is the interface user-friendly?
- Is the setup easy to install?
- Is there a functionality you would like to change? Why?
- Is there a functionality you would like to see?
- Is the documentation useful?
- Would you use the CSIRP in your incident response engagements?
- The CSIRP facilitate information exchange between incident responders?
- The CSIRP improves my efficiency compared to my current situation?
- The CSIRP facilitates attack artefacts sharing with my partners?
- The CSIRP facilitates attack investigations compared to my current situation?
- The CSIRP is a useful addition to my SOC ecosystem of tools ?

SIEM

- The interface is user friendly?
- The alert is easily understandable?
- Is it easy to investigate and see the events that trigger the alert?
- The alert received has enough information about the possible threat?
- The Graylog tool is useful?
- The ElasticHunter tool is useful?
- The XSOAR tool is useful?
- I would like to use the SIEM in my day-to-day work?
- The SIEM reduce response times compare to my current situation?
- The SIEM improves my efficiency compared to my current situation?
- The SIEM is intuitive?
- The ElasticHunter interface is user friendly?
- Is it easy to find the IoC using ElasticHunter?
- Is it easy to check the result in ElasticHunter?
- Is it easy to navigate to the source of the IoC from ElasticHunter to Graylog?
- Is it easy to browse the history of searches?
- ElasticHunter is it a useful addition to your SOC ecosystem of tools?

IPS/IDS

Please rate your level of satisfaction regarding the following aspects of the IDS/IPS GUI for the alerts as an administrator:

- Is the interface to view alerts user friendly?
- Is the information on each alert enough to identify threats?
- Is it available when needed?
- Look and feel?
- Are you satisfied of how alerts are displayed?
- Do you prefer that alerts are displayed as tables or graphs?
- Is it easy to navigate to see more details on single alert?
- Can you filter alerts by protocol, type of threat or detection rule or by other field?
- Are the panels editable/customizable?
- It is easy to manage user accounts?
- Is the overall performance satisfying?

- Is the tool an added value for you?
- Does the interface to view alerts improves your efficiency compared to your current situation?
- Would you add or remove any features? Why?
- What would you improve?

Please rate your level of satisfaction regarding the following aspects of the IDS/IPS GUI for the alerts as a security engineer:

- Easy to use?
- Look and feel?
- Are you satisfied of how alerts are displayed?
- Do you prefer that alerts are displayed as tables or graphs?
- Is it easy to navigate to see more details on single alert?
- Can you filter alerts by protocol, type of threat or detection rule or by other field?
- Does the interface to view alerts improves your efficiency compared to my current situation?
- Overall performance and quality of the information displayed?
- Is the tool an added value for you?
- Would you add or remove any features? Why?
- What would you improve?

RITA

Please rate your level of satisfaction regarding the following aspects of the RITA engine as an administrator:

- Ease of managing user accounts?
- Ease of taking backups?
- Overall performance?

Please rate your level of satisfaction regarding the following aspects of the RITA engine as a security engineer:

- Easy to use?
- Look and feel?
- Overall performance and quality of results?

FIMCA

- How complex do you think it is to answer general questions about your organisation (e.g. company size, number of people, average hourly staff costs, etc.)?
- How complex do you consider the phase of implementing countermeasures in FIMCA for your organisation to be?
- How do you evaluate the reference countermeasures reported in FIMCA: do you think CIS Control provides a satisfactory picture in terms of cyber security for your organisation?
- How do you evaluate the estimates of cost and efficiency scores of counter-measures: how reliable do you consider them to be?
- How do you assess the information in the results of the cost-benefit analysis as a whole?

- How useful do you consider ROSI as an economic indicator to assess the effects of cybersecurity choices?
- Would you recommend other indicators? If yes, which ones?
- What other information would you like to investigate among the elements to be investigated in a Cost-Benefit Analysis?
- Would you find it useful to implement FIMCA at a strategic level in your organisation? If the answer is no, please explain why and indicate the gaps found.
- Overall, how do you rate your experience with FIMCA?
- How do you rate your experience with the platform's GUI?
  At the level of the GUI, have you identified any critical or unclear aspects that you would suggest should be changed? If so, which ones?

4.2.2 SIGLA moving users

User acceptance wants to explain perceptual and emotional aspects resulting in a person to finally accept a mobile app (or any other digital service or technological products). Hence, user acceptance depends on the willingness of a person to use a technology considering their perception, expectation and intention.

Analysing user acceptance is a challenging task and the fundamental approach to implement it implies asking questions to users during a solution design and implementation. SIGLAMoving makes no exception, being a mobile based solution with a strong user related aspect. Here after, a list of questions providing a framework for user acceptance analysis data collection.

Questions

Question	Description
What do you like most about the SIGLAMoving app?	To find out what users like more in general about app (colours, branding, font, interface, clean, straightforward, etc).
What do you like the least about the SIGLAMoving app?	To find out what users dislike more about app so to consider eventual revising or improve it.
Which feature would you likely use the most?	To find out what features are important to users.
How often would you use it?	To find out if the app is effective enough for users to use it often.
Are there any features that you think you need but are missing in SIGLAMoving app? Describe.	To find out what missing features, the users may need or like to have.
How is the navigation of SIGLAMoving app?	To find out if navigation of the app is smooth and easy to understand.
What is your goal when you want to use SIGLAMoving app?	To find out what users want to achieve when running an app.

Question	Description
With the existing features, does SIGLAMoving app help you to achieve your goals? How?	To find out if features currently available help users with achieving goals.
Describe a situation in which SIGLAMoving app is the most useful to you.	To find out if the scenario under experimentation is in line with app aims.
On a scale of 1 to 5, rate your experience using SIGLAMoving app.	To measure how users generally feel when using app.
On a scale of 1 to 5, rate the interface of SIGLAMoving app.	To measure what perception of app's look and feel.
What do you think SIGLAMoving app should improve on?	To find out from users' perspective how improving app and what they expect the future product to be.

Table 8: Questionnaire

CONCLUSIONS

This document provides the methodology for the evaluation activities of the CitySCAPE pilots taking into account the project objectives and the diverse needs and capabilities of each asset involved (either on the CPaaS platform or on the CitySCAPE toolkit). Along with the KPI quantitative evaluation indicators other qualitative indicators have been considered to better assess the functionalities of the CitySCAPE toolkit in the respected questionnaires. Finally, special focus has been given on the user acceptance methodology as part of the evaluation protocol including the training sessions and the user satisfaction questionnaires.

ANNEX 1: CitySCAPE toolkit KPIs

KPI. id	KPI-s identifications

R7.1	**CitySCAPE**
R7.1.0	CitySCAPE platform
R7.1.1.0	*KPI metrics:* CitySCAPE - Components have to be interfaced with each other - Deployment state *Comments: (=100%)*

R7.1.1	**CitySCAPE - Collaborative threat investigation platform (CTIP)**
R7.1.1.2	KPIs
R7.1.1.2.1	*KPI metrics:* Number of external components compatible with Sherlock *Success Threshold: >2* Number of actionable IOC inside CTIP *Success Threshold: >500* Number of API request *Success Threshold: >0* Number of IOC triggering detection… *Success Threshold: >0*

R7.1.2	**CitySCAPE - Collaborative security incident response platform (CSIRP)**
R7.1.2.2	KPIs
R7.1.2.2.1	*KPI metrics:* number of user account *Success Threshold: >2* number of incident cases handled *Success Threshold: >2* Number of API requests *Success Threshold: >0*

R7.1.3	**CitySCAPE - Security Information and Event Management (SIEM)**
R7.1.3.2	KPIs

R7.1.3.2.1	*KPI metrics:* number of components inside log collection scope *Success Threshold: >2* number of alerts triggered *Success Threshold: >0* number of incident triggered *Success Threshold: >0* data volume ingested *Success Threshold: >0*

R7.1.4	**CitySCAPE - Intrusion Detection System/Intrusion Prevention System engines (IDS/IPS)**
R7.1.4.2	KPIs
R7.1.4.2.1	Minimum packet processing rate *Comments:* time to process a packet (<0,5 secs)
R7.1.4.2.2	Number of threats type detected *Comments: (>3)*
R7.1.4.2.3	Number of machines in the network *Comments: minimum number of machines in the restricted network to be monitored (>2)*
R7.1.4.2.4	Accuracy of the anomaly detection procedure *Comments:(>90%)*
R7.1.4.2.5	Pilot/user satisfaction *Comments: Percentage of the combination/sum of satisfaction for "Easy to use", "Look and feel", "Availability" and "Overall performance" characteristics (>50% or >2 out of 4 (scale: 0 to 4))*

R7.1.5	**CitySCAPE - Risk analysis and Impact Assessment (RITA) engine**
R7.1.5.1	General
R7.1.5.1.1	*General functionality* Does the component meet the requirements set (R1.5, R2.5, R3.5)?
R7.1.5.2	Risk Assessment KPIs

R7.1.5.2.1	*Number of risks identified*. Risk identification detects upstream and downstream dependencies across all business areas of an organisation. Additionally, this metric will identify areas that would benefit from centralised controls, which would eliminate the extra work and investment of maintaining separate controls, thereby increasing organisational efficiency. To gain a holistic view of organisational risk management performance, organisations would need to compare the number of risks identified to the number of risks that occurred, and finally compare it to the number of risks mitigated. *NOTE:* Operators of the RITA engine should compare the list of risks identified with the risks that have already been identified through their own risk management process. *Scale:* 0: no risks identified, 1-5 (small and insignificant – lots and significant)
R7.1.5.2.2	Number of risks not identified. Identify events that occur that should have been flagged as a risk but weren't. Look at the number of events on the event log that could have been foreseen but bypassed the risk stage. *NOTE:* Operators of the RITA engine should compare the list of risks identified with the risks that have already been identified through their own risk management process. *Scale:* 0: no risks not identified, 1-5 (small and insignificant – lots and significant)
R7.1.5.2.3	*Number of risks that occurred (i.e. became events).* Quantify the number of risks that materialised into incidents in order to better update the risk management strategy. This metric can offer better insights into whether or not the risk management/analysis process is effective. If for example lots of monitored risks turn into events, this means that the risk team have successfully spotted that these risks might cause problems. If lots of risks are monitored but none turn into events, this could be that the team are tracking the wrong things. Essentially, the ultimate goal is to minimise the number of risks as much as possible, since appropriate countermeasures where adopted. *Scale:* 0: no risks occurred, 1-5 (small and insignificant – lots and significant)
R7.1.5.2.4	*Number of risks that occurred more than once*.

	If a risk occurs multiple times, across the same organisation or several business processes, it can be an indication that teams aren't learning from past experience. Essentially, the goal is to minimise the number of risks that occurred more than once to 0. *Scale:* 0: no risks not occurred multiple times, 1-5 (small and insignificant – lots and significant)
R7.1.5.2.5	*Percentage of risks monitored.* Monitoring 100% of all identified risks is important, as risk teams can leverage security ratings to help them prioritise higher-impact risks for remediation efforts. Through risk assessments and linking risks to activities, organisations can start prioritising the activities that are most in need of monitoring. Regular risk assessments can also empower organisations to detect increased cyber threat levels, while empowering risk teams to take immediate action on specific cyber risks that are more likely than others to materialise. *NOTE:* Operators of the RITA engine should identify which business processes are being monitored as a result of the risk assessment. Any value is acceptable as it is organisational specific.
R7.1.5.2.6	*Percentage of risks mitigated.* Risk mitigation is another crucial step in the risk management process. Organisations have to develop a robust strategy to eliminate or reduce identified risks. Risk teams can leverage risk assessments to help them prioritise and allocate resources where needed, allowing them to reduce inefficiencies that come from wasted efforts on low-impact risks. All risk assessments should be based on standardised criteria, so that organisations can determine a uniform risk appetite/tolerance, or cut level, throughout the organisation based on resulting assessment indexes. Essentially, the ultimate goal is to reduce or eliminate 100% of the prioritised risks.
R7.1.5.2.7	*Percentage of process areas involved in risk assessments.* Risk management is inherently cross-functional and cannot be performed in silos. Considering that overall risk, is the sum of its parts, an incident or risk event in one business area might affect other areas.

	NOTE: Operators of the RITA engine should identify which business processes are included in risk assessments. Any value is acceptable as it is organisational specific.
R7.1.5.2.8	*Costs incurred due to risks.* Ideally, risk management strategies should not only help with risk mitigation, but they should also assist with finding cost-effective solutions. Compare the current risk status/profile to a past timeline, a drop in the expenses incurred due to the risk might be noticed. This metric therefore can be indicative of an effective risk management process. *Scale:* 1-5 (insignificant cost reduction – significant costs reduction)

R7.1.7	**CitySCAPE - Financial impact and cost-benefit assessment engine (FIMCA)**
R7.1.7.1	Financial impact engine KPIs
R7.1.7.1.1	*Number of assets investigated* FIMCA analyses the financial impact of each organisation estimating the impact on each asset present. The analysis is carried out based on the RITA dataset. Each asset is also associated to a service that generates the organisation revenues. *Reference metrics*: amount of objects (= assets) analysed in FIMCA related to the total amount of objects (= assets) considered in CitySCAPE.
R7.1.7.1.2	*Number of countermeasures investigated* FIMCA analyses the financial impact of each organisation estimating the impact on the operativity of each service. The analysis is carried out based on the RITA dataset. Each service owns a set of assets that are functional to guarantee the correct operativity of the service. *Reference metrics*: amount of countermeasures analysed in FIMCA.
R7.1.7.1.3	*Number of configurations created* The user can create several configurations of his own

	organisation. Each configuration is characterised by different sets of countermeasures. The configurations will be then compared in the cost-benefit analysis to assess the economic indexes. *Reference metrics*: amount of security configurations of the same organization created in FIMCA.
R7.1.7.1.4	Financial impact estimated on each asset The financial impact of the assets is estimated on the basis of the integrity of the asset (referred to CIA architecture exploited by RITA) and the recovery time (including the costs of spare components or replacement). *Reference metrics*: amount of objects (= assets) for which the financial impact has been computed in FIMCA related to the total amount of objects (= assets) considered in CitySCAPE.
R7.1.7.1.5	*Financial impact estimated on each service* The financial impact of the services is estimated on the basis of the availability (referred to CIA architecture exploited by RITA) of its asset with the highest risk. The financial impact estimates the costs due to the out of service and recovery. *Reference metrics*: amount of objects (= services) for which the financial impact has been computed in FIMCA related to the total amount of objects (= services) considered in CitySCAPE.

R7.1.8	**CitySCAPE - Cost-benefit analysis module**
R7.1.8.1	Cost-benefit analysis KPIs
R7.1.8.1.1	*Number of configurations compared* The cost-benefit analysis compares couples of configurations to provide feedbacks about the improvement in terms of investment and economic losses due to the application of new countermeasures. *Reference metrics*: the amount of configuration that are compared in the cost-benefit analysis.
R7.1.8.1.2	*Financial impact reduction* The objective of the financial is to reduce the financial impact on the organisation, supporting the user on the selection of the most appropriate security measures. *Reference metrics*: The impact reduction based on ROSI indicator.

R7.1.9	CitySCAPE - CyberSafety Management Games (CSMG)
R7.1.9.2	Training process
R7.1.9.2.1	*KPI metrics:* Number of trainees Training sessions of regular passengers will cover multiple sessions with more than 50 online trainees in total. *Comments: KPI included in Objective O8* *(>50 participants)*
R7.1.9.2.2	*KPI metrics:* Number of trained employees Training sessions of multimodal transport companies' employees of the administrative and operational areas will cover multiple sessions with more than 100 trainees in total. *Comments: (>100 participants)*

R7.1.10	CitySCAPE - Cyber-range (Training) platform
Notes	Not applicable

R7.1.11	CitySCAPE - Kaspersky Mobile Security Software Development Kit
R7.1.11.1	KMS-SDK security features integration
R7.1.11.1.1	*KPI metrics:* Number of mobile app integrating security features. KMS-SDK security features integrated in at least 3 mobile apps dedicated to multimodal transport stakeholders (i.e., Genova and Tallinn LTPs involved in CitySCAPE) and for at least 2 different categories of end-users (i.e., passengers and LTPs staff). *Comments:* (>3 integrations to mobile apps and >2 integrations within the end-users)
R7.1.11.1.2	*KPI metrics:* Number of mobile devices assessed - KMS-SDK risk assessment features enabled in at least 30 Android-based mobile devices and at least 15 iOS-based mobile devices. *Comments:* (>30 integrations to Android-based mobile devices and >15 integrations to iOS-based mobile devices)
R7.1.11.1.3	*KPI metrics:* Number of mobile devices protected - KMS-SDK protection features enabled in at least 30 Android-based mobile devices.

	Comments: (>30 integrations to Android-based mobile devices)
R7.1.11.1.4	*KPI metrics:* Number of mobile devices with web and network connection secured. - KMS-SDK securing connection features enabled in at least 30 Android-based mobile devices and at least 15 iOS-based mobile devices. *Comments:* (>30 integrations to Android-based mobile devices and >15 integrations to iOS-based mobile devices)
R7.1.11.1.5	*KPI metrics:* Number of mobile devices with data secured. - KMS-SDK securing data features enabled in at least 30 Android-based mobile devices and at least 15 iOS-based mobile devices. *Comments: (*>15 integrations to iOS-based mobile devices)
R7.1.11.1.5	*KPI metrics: Modularity and replaceability of cyber-security module* - KMS-SDK can be modularly integrated and easily replaceable to avoid any eventual vendor lock-in
R7.1.11.1.6	*KPI metrics: Full-control of App owner over cyber-security features* - The five KMS-SDK group of features (device assessment, device protection, network connection securing, data securing, app self-protection) can be turned-on/-off easily by LTPs to fully manage the mobile app deployment and eventual compliance with LTPs regulations
R7.1.11.1.5	*KPI metrics:* Number of self-protected mobile app. - KMS-SDK self-defense features integrated in at least one Android-based mobile app. - *Comments:* (>10 integrations to Android-based mobile devices)

R7.1.12	**CitySCAPE - Threat Data feeds**
R7.1.12.2	API integration process
R7.1.2.2.1	*KPI metrics:* Feeds integrated in a Threat Intelligence Platform - KSP Threat Data Feeds integrated in at least one Threat Intelligence Platform for multimodal transport stakeholders. - *Comments:* (>1 integrations to platform)