PRECINCT

Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyber-Physical Threats

D.6.3 PRECINCT Capacity Building Programme

Document Summary Information

Grant Agreement No	101021668	**Acronym**	PRECINCT
Full Title	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-Physical Threats		
Project URL	https://www.precinct.info		
Start Date	01.10.21	**Duration**	24 months
Deliverable	D6.3	**Work Package**	WP6
Contractual due date	30.09.2023	**Actual submission date**	19.09.2023
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	UCD		
Responsible Author	Marisa Escalante (TECNALIA); Páraic Carroll (UCD)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101021668

Disclaimer

Copyright

Contributors

Name	Name (organisation)
Marisa Escalante	TECNALIA
Nicola Durante	ENGINEERING
John Limaxis	INLECOM
Shirley Delannoy	VIAS
Daniel McCrum	UCD
Páraic Carroll	UCD

Quality Control

Date	Role	Name (organisation)
04/08/2023	SAB Reviewer	Jenny Rainbird (ICP)
29/08/2023	Peer Reviewer	Carmela Canonico (UITP)
29/08/2023	Quality Control Reviewers	Mark Miller/Victoria Menezes Miller (CPT)
31/08/2023	Peer Reviewer	Boris Tomas (DLR)
14/09/2023	Ethics Review	Vagelis Papakonstantinou, Vrije Universiteit Brussel (VUB), Law, Science, Technology & Society Studies (LSTS)
18/09/2023	Final QA Review	Mark Miller/Victoria Menezes Miller (CPT)
19/09/2023	Final PM Review	Jenny Rainbird (ICP)

Revision history

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.0	19/06/2023	0	Initial Deliverable Structure	Marisa Escalante (TECNALIA)
V0.1	15/07/2023	70%	Section M12 and M24 Training	Marisa Escalante (TECNALIA)
V0.2	19/07/2023	90%	Training LLs section	Nicola Durante (ENG) John Limaxis (INLECOM) Shirley Delannoy (VIAS)
V0.3	27/07/2023	95%	General sections	Marisa Escalante (TECNALIA)
V0.4	28/07/2023	100%	Version ready for SAB review	Páraic Carroll (UCD) Daniel McCrum (UCD) Marisa Escalante (TECNALIA)
V1.0	05/09/2023	100%	Version ready for submission	Páraic Carroll (UCD) Daniel McCrum (UCD) Marisa Escalante (TECNALIA)

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
BDIS	Big Data Infrastructure Services
CEP	Complex Events Processing
CES	Cascading Effects Simulation
CESE	Cascading Effects Simulation Engine
CI	Critical Infrastructure
CIIG	Critical Infrastructure Interdependency Graph
DB	Data base
DT	Digital Twins
GA	Grant Agreement
GUI	Graphical User Interface
KG	Knowledge Graph
LL	Living Lab
RCA	Root Cause Analysis
RMF	Resilience Methodological Framework
RSC	Resilience and supervisory control
SG	Serious Games

1 Executive Summary

The purpose of this deliverable is to report the activities carried out to ensure that the platform and supporting tooling developed within PRECINCT is widely adopted and used by first responders, emergency personnel and CI stakeholders across the EU.

During the PRECINCT project a capacity building programme has been developed and delivered to relevant stakeholders in two open training sessions, the first of which was organized in November 2022 (M14) and the second one in May 2023 (M20). In addition to these two sessions, other activities to facilitate the adoption of the PRECINCT ecosystem have been organized together with all the partners involved in the four LLs. The PRECINCT Capacity building programme that has been prepared also supports Training for Transferability.

This deliverable reports the approach followed to build the PRECINCT capacity building programme, the contents of each of the sessions and the results of the evaluation were carried out with the objective of collecting feedback from the participants in the training to define a pathway to improve the tools composing the PRECINCT ecosystem.

The mentioned capacity building programme consists of different training blocks that cover the main technologies and tools provided in PRECINCT. The rationale for these different training blocks is due to there being differences among the technologies and tools regarding the maturity and audience of each tool. Not all of the technologies and tools are mature enough at the same time during the project, and as for the audience, not all the tools and technologies are for people with the same knowledge or role.

2 Introduction

The objectives of this deliverable are to present the PRECINCT Capacity Building Programme. The main objective of the PRECINCT Capacity Building Programme is to ensure a wide adoption of the PRECINCT cyber-physical security management platform and supporting tooling by first responders, emergency responders and CI stakeholders across the EU.

To achieve these objectives, two training sessions were held, one in M12 and the other in M24. The audience was CI stakeholders, emergency responders, first responders and decision makers. In the first training session in M12, three training blocks were presented:

- **Cascading effects and interdependency graphs**: The objective was to inform the audience around the process of creating the interdependency graph and subsequent cascading effects to threats/attacks/hazards.
- **Resilience Methodological Framework**: The objective was to inform the audience as to how resilience was calculated based on the threats/attacks/hazards presented in the interdependency graphs. The concept of spending budget on mitigation/response actions to improve the resilience of the interdependent CIs was discussed and an example presented.
- **Serious games & Serious game storyboard**: The preliminary Serious Game interface and the storyboard concept for the entire game were presented. The concept of Serious Game attacker, defender, Game Director and their potential actions was discussed. The gameplay actions and how they are linked to the resilience methodological framework, cascading effects & interdependency graphs was presented so that the audience could understand what the gameplay actions related to.

The second training session in M24 was presented in three different parts of training blocks:

- **Cyber Attack detection and analysis**: The objective of this training was to explain how PRECINCT supports the detection of attacks and how it processes this information to support the decisions of potential recovery actions or mitigation actions.
- **Simulation and respons**e: The objective was to show the different tools that support CI in understanding how a potential cyber-physical threat can be derived in different cascading effects. The main tools trained in this flow were: Digital Twins (DT) and Resilience Supervisory Control.
- **Technical support**: This part was focused on presenting those tools that supports the flows defined. During this part the tools presented were PRECINCT Blueprints Directory, Big Data Infrastructure Services (BDIS) and Knowledge graph.

Finally, the details of the training events that took place in each of the four LLs is presented. The aim of this is to demonstrate how all of the PRECINCT Ecosystem tools can be implemented into specific LLs.

2.1 Mapping PRECINCT Outputs

Table 2-1: Adherence to PRECINCT's GA Deliverable & Tasks Descriptions

PRECINCT GA Component Title	PRECINCT GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D.6.3 PRECINCT Capacity Building Programme	*PRECINCT Capacity Building Programme report on capacity building activities and training events.*	*Section 4, section 5 and section 6*	*These section provide the detailed description of the training events carried out during PRECINT project.*
TASKS			
Task 6.4 PRECINCT Capacity Building Programme	*Two training events will be scheduled during the project (M12, M24) with the end goal of education, enablement and training to incentivise discussion and dialogue in a direction that can influence accelerated adoption of PRECINCT's concepts, innovation, blueprints and open tooling*	*Section 4 and Section 5*	These sections describe the training contents and the evaluation of the two sessions done: M12 (section 4) and M24 (section 5)

2.2 Deliverable Overview and Report Structure

This deliverable is associated with Task 6.4 of the PRECINCT project which focuses on building capacity about the PRECINCT's concepts, innovation, blueprints and open tooling.

The main content of the deliverable is structured as follows:

- Chapter 1: contains an executive summary of the deliverable
- Chapter 2: defines introductory content that includes the objectives and how the evidence of the deliverable shows the progress with respect to the Grant Agreement (GA)
- Chapter 3: describes the general approach followed for the Capacity building programme
- Chapter 4: describes the contents and evaluation for the M12 training
- Chapter 5: describes the contents and evaluation for the M24 training
- Chapter 6: describes how the capacity building programme was customised for each of the LLs.
- Chapter 7: describes the conclusions of the deliverable

3 PRECINCT Capacity Building Programme

The main objective of the PRECINCT Capacity Building Programme is to ensure a wide adoption of the PRECINCT cyber-physical security management platform and supporting tooling by first responders, emergency responders and CI stakeholders across the EU.

The PRECINCT Capacity training programme has two main objectives:

- to present PRECINCT's concepts, innovation, and tooling of the project and
- to get feedback from the stakeholders that attend the meeting.

This capacity building programme consists of different training blocks, that cover the main technologies and tooling provided in PRECINCT. The rationale behind creating these different training blocks is that there are differences among the technologies and tools regarding the maturity of the tool and the audience using each tool. Not all the technologies and tools are mature enough at the same time during the project, and in the audience, not all the tools and technologies are for people with the same knowledge or role.

According to the GA, two training sessions had to be held alongside the PRECINCT general assembly events to reach all the relevant CI stakeholder community.

The first training session was organized during the 2nd PRECINCT general assembly in Brussels in November 2022, the second one was organized together with the PRECINT conference held also in Brussels in May 2023.

In the first training session, three training blocks were presented:

- Cascading effects and interdependency graphs
- Resilience Methodological Framework and integration with graphs
- Serious games & Serious game storyboard

These three blocks were prepared because they are the more mature ones due to the timeline of the project. More detail of this session is provided in the following sections.

The second training session was structured into three different parts with the corresponding training blocks.

- Flow "Cyber Attack detection and analysis". The objective of this flow was to explain how PRECINCT supports the detection of attacks and how information is processed to support the decisions on potential recovery actions or mitigation actions. The main tools involved in this flow were: Security and privacy tool, Root Cause Analysis (RCA), Complex Events Processing (CEP) and Situational awareness UI.
- Flow "Simulation and response." The objective was to show the different tools that support CI in the understanding of how a potential cyber-physical threat can be derivate in different cascading effects. The main tools trained in this flow were: Digital Twins (DT) and Resilience and supervisory control.
- Technical support. This part was focused on presenting those tools that support the flows defined. During this part the tools presented were PRECINCT Blueprints Directory, Big Data Infrastructure Services (BDIS) and Knowledge graph.

The training blocks were designed to focus on highlighting three main aspects: i) understand why to use the presented tool, ii) the main advantages of using it and iii) finally, to show how to use it. The training was composed by a mix of presentations, demos, and practice with some of the tools.

Both sessions were organized in a hybrid format and approximately 120 participants attended.

One benefit of organizing these training blocks is that this material has been reused to train the LLs participants and also to facilitate the transferability of the knowledge and PRECINCT approach.

4 Training M12

As mentioned in the previous section the training was held together with the second PRECINCT stakeholders' workshop. In the following section, the details of the contents delivered, and the feedback received, are provided.

4.1 Contents

The objectives of this training session were:

- Familiarise participants with the technology (Cascading effects and interdependency graphs; Resilience Methodological Framework; Serious games)
- Present an LL Scenario: City impacted by a flood hazard
- Allow trainees to suggest enhancements to the Scenario
- Show trainees the impact of their strategy
- Show trainees which strategies work and which ones do not work
- Obtain feedback on the PRECINCT Results presented
- Provide a lecture on material produced for future training for transferability

In order to fulfil these objectives, the agenda presented in Table 4-1 was prepared:

Table 4-1: M12 Training Session Agenda

Title	Content and Justification	Trainers
Introduction	Plan for the session and presentation of example LL. City, services, hazards etc.	Marisa Escalante (TECNALIA)
Cascading effects and interdependency graphs	Familiarise audience with the technology, input and output.	Sandra König (AIT)
Resilience Methodological Framework and integration with graphs	Familiarise audience with the technology, input, output and how the calculation is developed in the graphs.	Lorcan Connolly (RDS)
Presentation of serious games & Serious game storyboard	Familiarise audience with the technology, input, output and motivation. Demonstrate an application to a wide audience for interactive input.	Meisam Gordan (UCD)
Questions and discussion	Get feedback on approaches and ensure that any issues are recorded and addressed.	
Interactive defence of the (dummy) precinct	Allow users to try to put in place enhancements to the precinct. Use Mentimeter or similar to obtain feedback on how the audience might defend the precinct from the hazards in question.	Sandra König (AIT) & Lorcan Connolly (RDS)
Demonstration of the audience's suggestions	Based on average input from the audience, put the suggested mitigation / enhancement measures in place and calculate new resilience index. Demonstrate where this strategy does well and where it does not.	Sandra König (AIT) & Lorcan Connolly (RDS
Demonstration of optimized maintenance strategy	Based on a predefined (optimised) strategy, demonstrate this to the audience, showing why it is an effective strategy.	Sandra König (AIT) & Lorcan Connolly (RDS
Discussion on learnings and future plans for PRECINCT tools.	Feedback session	Marisa Escalante (TECNALIA)

The following section explains at a high level the most relevant contents of the training. The section of the training was recorded and can be found in the following link: Video (approx 3 hours and 16 minutes)

4.1.1 Cascading effects and interdependency graphs

The objective of this part of the training is to demonstrate how to model the interdependencies among different critical infrastructures [1].

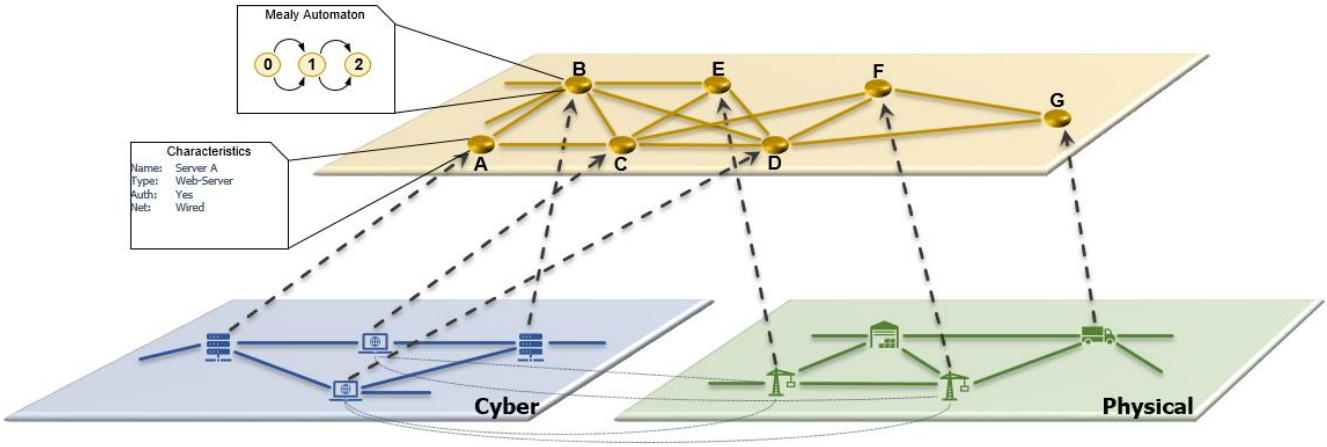

Figure 4-1: CI Interdependency Graph

This training covered the following tools: Critical Infrastructure Interdependency Graph (CIIG) (Figure 4-2) model and the Cascading Effects Simulation (CES) that builds on the CIIG. The modelling approaches and process of creation of the CIIG and CES were discussed by the relevant technical project partners.

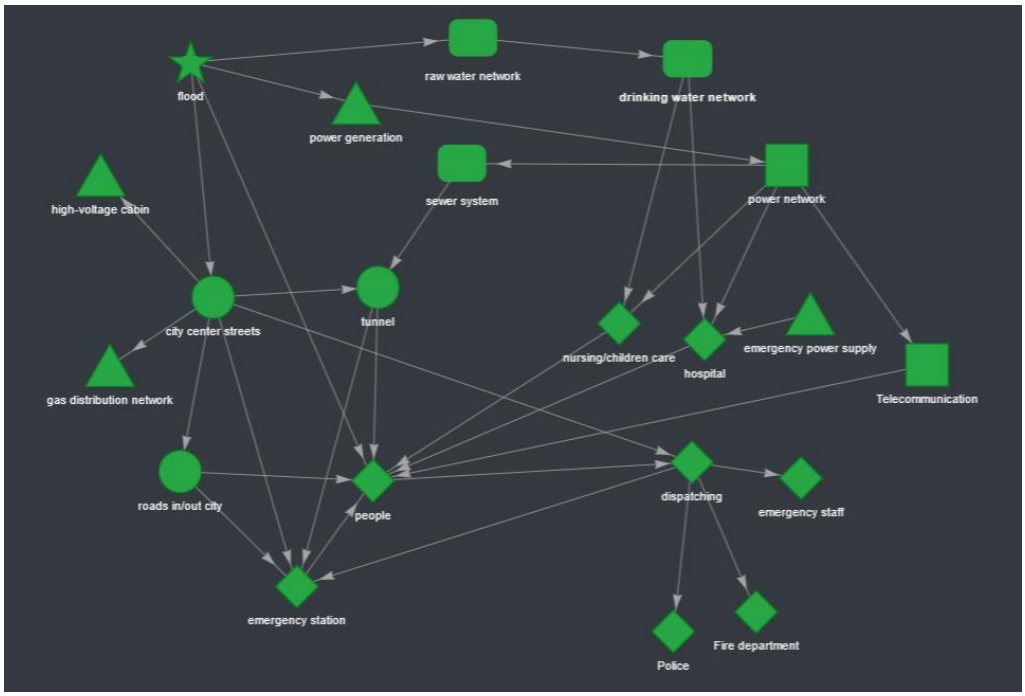

Figure 4-2: Example of Interdependency Graph

4.1.2 Resilience Methodological Framework

The objective of the Resilience Methodological Framework (RMF) is to facilitate quantification of resilience and thereby identification of measures that enhance resilience (1) during normal operations, (2) for threats with short-term impacts, and (3) for threats with longer-term impacts [2].

This part of the training covers the explanation of what is understood by Resilience. A brief presentation of previous resilience frameworks and the process to be followed with the RMF to quantify the resilience, and also how to optimize the resilience and the investment, is provided.

Figure 4.3 shows the different steps of the RMF explained in the training. Figure 4-2 shows the interdependency graph associated with a hypothetical CI system/network. Table 4-2 shows an example to the audience of the methodology used to calculate resilience in the hypothetical example shown in Table 4-3. The example demonstrated the resilience output and cost benefit associated with each of the relevant resilience indicators for each of the CIs within all the interdependent Cis, is presented in Table 4.4.

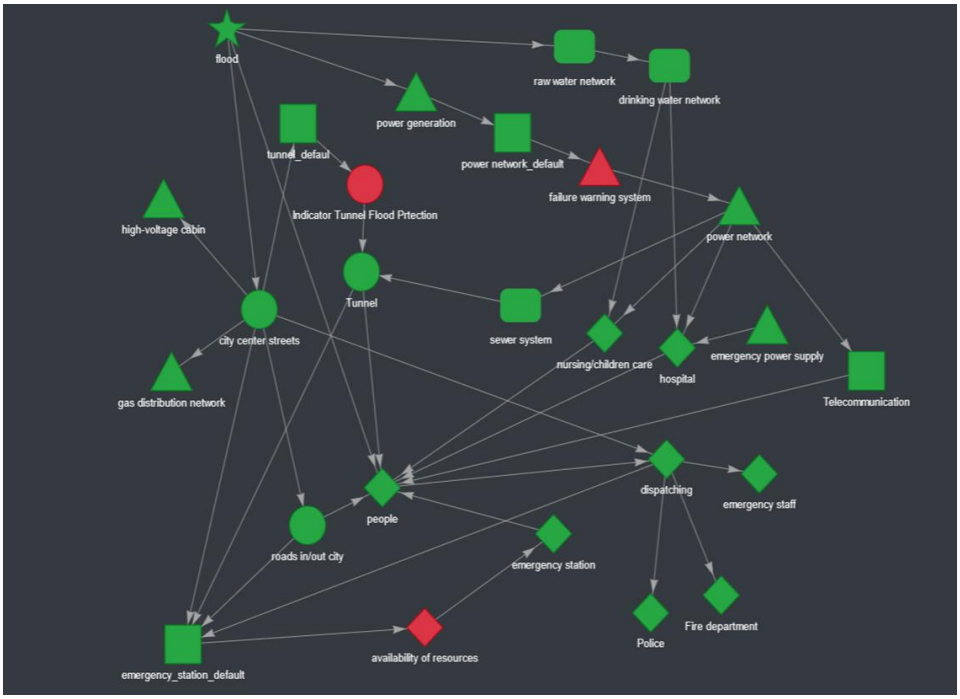

Figure 4-3: Step1: Define Infrastructure System

Table 4-2: Step 2: Quantify Service

User Type	Users per day	Average uses per lifetime	User value	Total service provided
Nursing / childcare	25,000	5,000	€100,000.00	€500,000.00
Hospital	20,000	70	€100,000.00	€28,571,428.57
Telecomunications	0	500,000	€100,000.00	€0.00
Kennedy Tunnel	100,000	2,500	€100,000.00	€4,000,000.00
Roads in/out city	300,000	5,000	€100,000.00	€6,000,000.00
			Sum	**€39,071,428.57**

Table 4-3: Step 3 Quantify Resilience

Indicator	Possible values	Meaning	Cost to achieve indicator state from state 5
Condition of Tunnel flood protection measures	5	No Flood mititgation and poor sealing of tunnel	N/A
	4	No flood mitigation but tunnel sealing in good condition	€100,000
	3	Tunnel sealed and drainage available in poor condition	€500,000
	2	Tunnel sealed and drainage available in good condition	€1,500,000
	1	High level of flood mitigation, drainage effectively removing flood damage	€3,000,000
Presence of Electricity failure Warning Systems	3	No warning system	N/A
	2	one warning system	€100,000
	1	Multiple warning systems sure to identify threat in advance	€1,000,000
Availability of emergency resources (Number of emergency staff)	4	20 voluntary emergency staff	N/A
	3	10 trained emergency staff & 20 voluntary emergency staff	€500,000
	2	40 trained emergency staff	€1,800,000
	1	100 trained emergency staff	€4,050,000

Table 4-4: Step 4 Set targets

Indicator	Legal req.	Possible values	Increment cost (€)	Increment Benefit (€)	B/C ratio	Net Benefit (€)
Condition of flood protection measures	-	1	0	0	-	0
		2	10,000	50,000	5.00	40,000
		3	30,000	50,000	1.67	60,000
		4	60,000	25,000	0.42	25,000
		5	100,000	10,000	0.10	-65,000
Condition of Tunnel	3	1	0	0	-	0
		2	50,000	100,000	2.00	50,000
		3	100,000	80,000	0.80	30,000
		4	250,000	25,000	0.10	-195,000
		5	500,000	0	0.00	-695,000
Presence of Tunnel Alert / Warning Systems	-	1	0	0	-	0
		2	25,000	150,000	6.00	125,000
		3	100,000	125,000	1.25	150,000
Accessibility of Infrastructure	3	1	0	0	-	0
		2	40,000	100,000	2.50	60,000
		3	100,000	250,000	2.50	210,000
		4	1,000,000	500,000	0.50	-290,000
Presence of a monitoring strategy	-	1	0	0	-	0
		2	10,000	25,000	2.50	15,000
		3	100,000	85,000	0.85	0
Practising of emergency plan	-	1	0	0	-	0
		2	15,000	65,000	4.33	50,000
		3	30,000	45,000	1.50	65,000
		4	60,000	35,000	0.58	40,000
		5	120,000	15,000	0.13	-65,000

4.1.3 Serious Games

During this section, an explanation of the definitions, characteristics and applications of the Serious games was presented.

Serious games in PRECINCT are used to train the CI operators in the identification of potential unseen cascading effects and to show them the cascading effects and impact on different CIs.

The main advantaged of the Serious games are:

- Simulating unseen events for better preparedness,
- Involvement of different roles within the game (Game Director, Attacker, Defender),
- Experiential learning with challenging tasks (learning goals),
- Obtaining immediate feedback,
- Active learning and support critical thinking (empowerment),
- Immersion and repeated play (reusable),
- Cost-effective (not costly compared to what it can bring).

The training explains how the Serious Game could be used depending on the role of the "player" and an example of the gameplay concept was presented to the audience. Figures 4-4 to 4-6 are screenshots of different steps within storyboard of the Serious Game. In the gameplay of the proposed Serious Game, firstly, a registered user logs in by entering their username, email, and password, then selecting a character, either the Game Director, an Attacker or Defender.

Once a user is logged in, the game will present the qualified director with a director's dashboard to select the type of physical or cyber-attack, the location, and the budget for the attacker and the defender for each CI (see Figure 4-4).

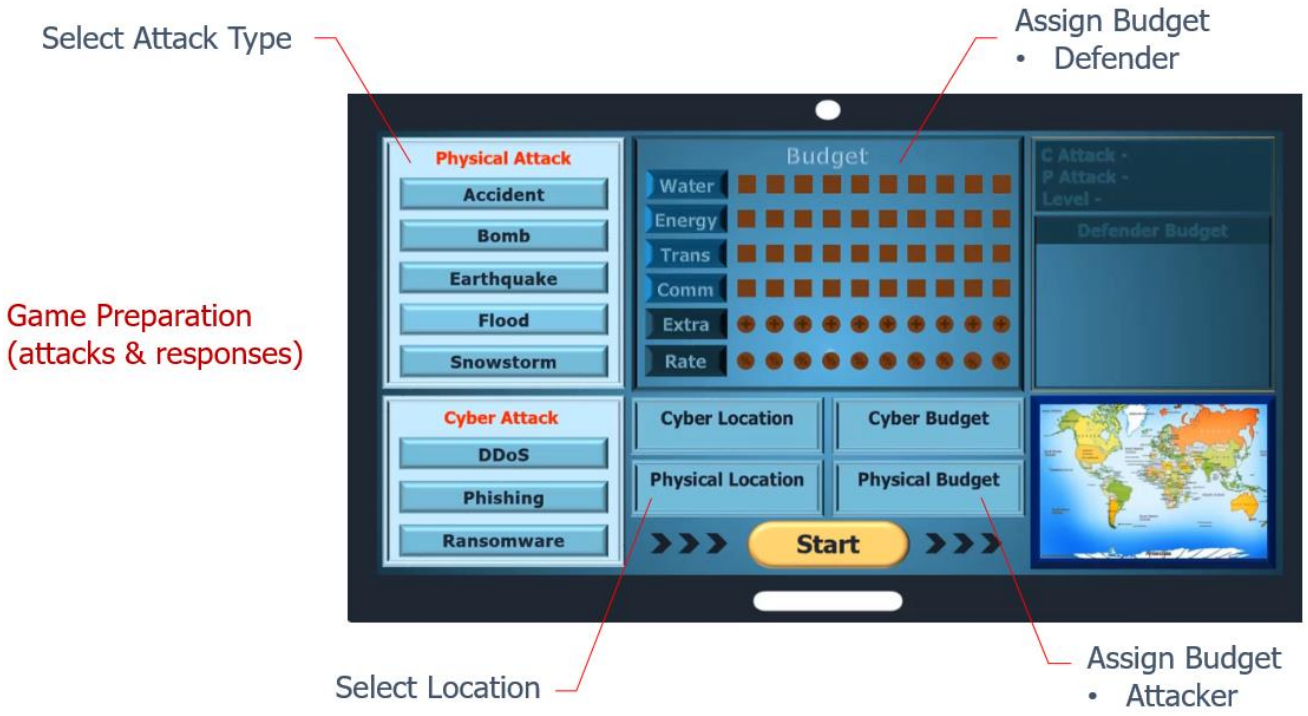

Figure 4-4: Director Dashboard

The attacker's dashboard enables the attacker to select tools for the initial attack, use upgrade tools for changing the severity of the hazard or threat, and utilise noise to generate small attacks aiming to confuse the player (see Figure 4-5).

Figure 4-5: Attacker Dashboard

The defender will be presented with the game's initial budget balance, the player's ranking, the attack type and the level set by the director. Next, the defender must enter his or her job role and the number of years of experience in this position (see Figure 4-6). The game director will be a trusted member of staff from the CI operator or else emergency response coordination team.

Critical Infrastructure Emergency Operator

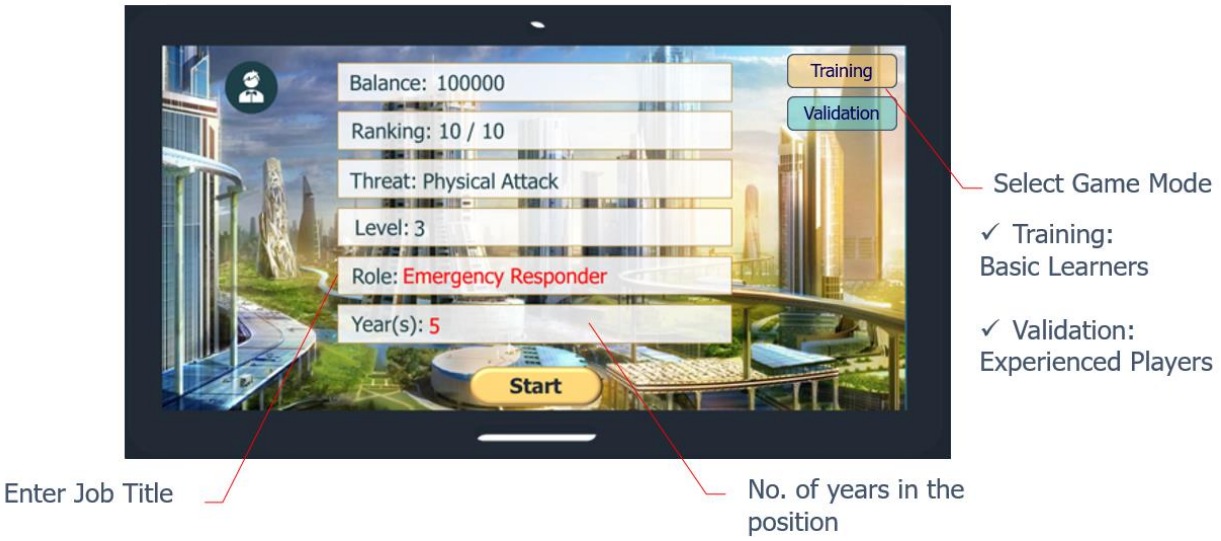

Figure 4-6: Defender Dashboard

Next, the defender is presented with the opening attack scenario. The game provides a set of analysis tools to help the defender understand the impact of the attack/threat, through geospatial visualization, and the CI's resilience rating, for example. The game uses the interaction of the attacker and the defender to simulate an attack's cascading effect. After the defender implements a solution to counteract the attacker's first attack, the attacker can intensify the attack by increasing the severity of the attack event. Consequently, the target infrastructure is damaged due to the additional attack. The size of the affected area, the resilience rating for each CI, the links of affected CIs, and the detailed cascading effect between different CIs can also be displayed using the proposed Serious Game.

4.1.4 Training for transferability

Following the training event in M12, lecture material was produced to aid the training for transferability. The technical content described in Section 4.1.1, Section 4.1.2 and Section 4.1.3 was converted to lecture material.

4.2 Evaluation

After the delivery of the training, an evaluation form was presented to the participants to obtain their feedback about the training. The questionnaire was composed of several questions organised in 4 sections:

- General evaluation: To obtain the general impression about the training.
- Contents and process: To get feedback about the provided contents and the process followed to deliver it. (Rated from 1-5, Five is the highest level of agreement.)
- Organisational aspects: To get feedback on the format, the timing and so on. (Rated from 1-5, Five is the highest level of agreement.)
- General feedback: Free text option to indicate those aspects that Participants liked and those aspects that should be improved.

Figure 4-7– 4-10 show the responses from participants related to general evaluation. The best rates (> 80% of the participants evaluated as excellent) are related to the structure and the usefulness of the information provided and an aspect for improvement was the usefulness of the material of the training. The overall rating for the training was evaluated as excellent by 78% of the participants.

Overall quality rate

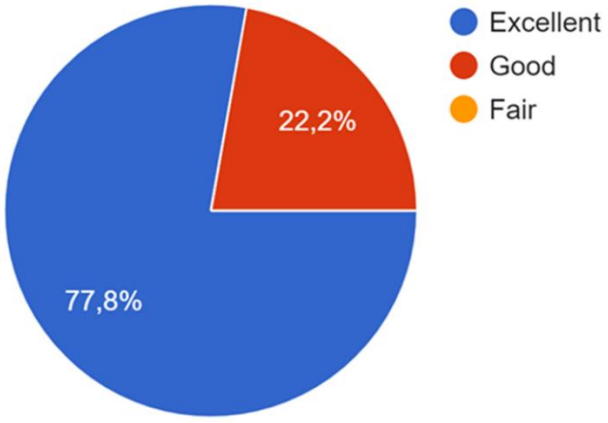

Figure 4-7: M12 Overall quality rate

Structure of the training session

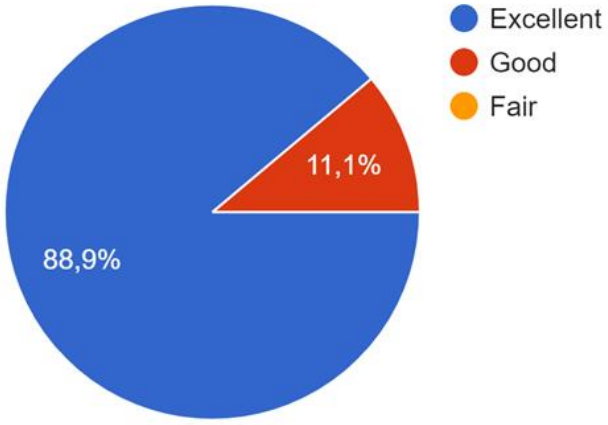

Figure 4-8: M12 Structure of the training session

Usefulness of the information received in the training

Usefulness of the training material

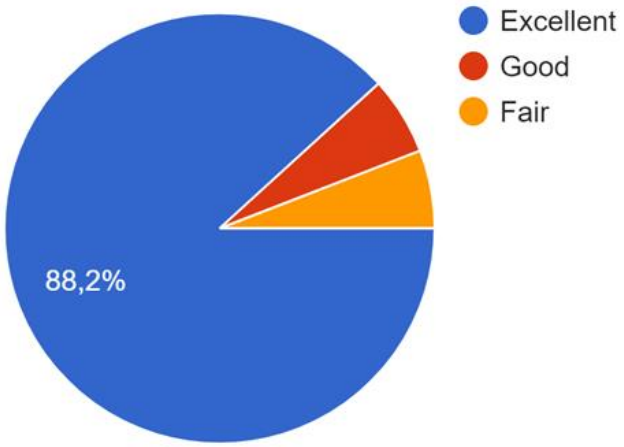

Figure 4-9: M12 Usefulness of the information received in the training

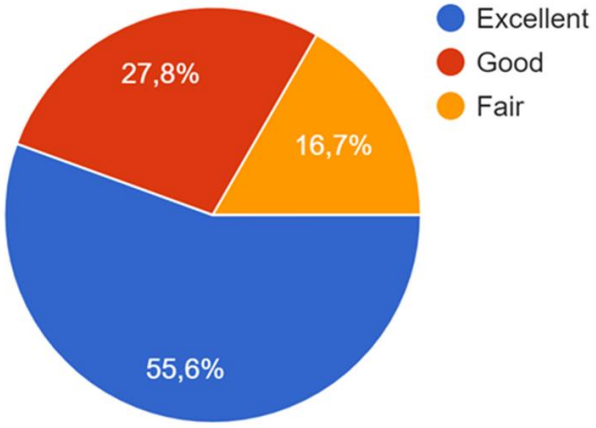

Figure 4-10: M12 Usefulness of the training material

Most of the participants recognised that the training covered the defined objectives and that it covered their expectations, although some of them remarked that the training was not very useful for their work. The contents and the techniques used in the training session were effective to understand the tools explained. (See Figures 4-11 to 4-15).

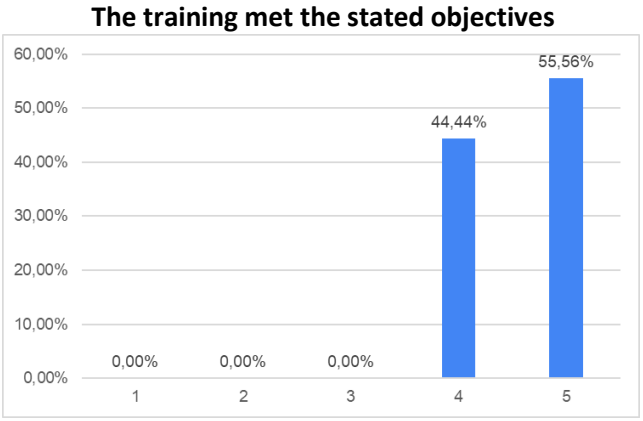

Figure 4-11: M12 The training met the stated objectives

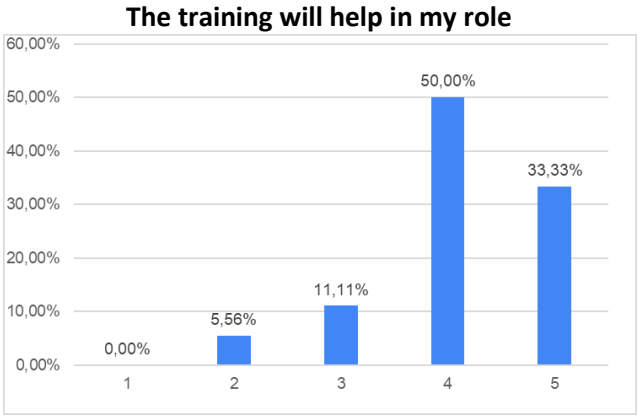

Figure 4-12: M12 The training will help in my role

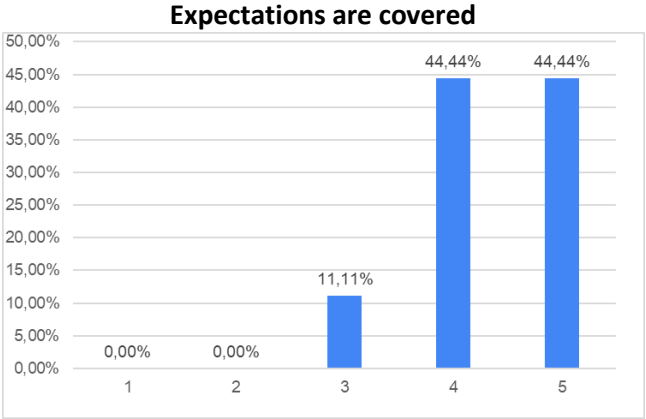

Figure 4-13: M12 The training covered what I expected it

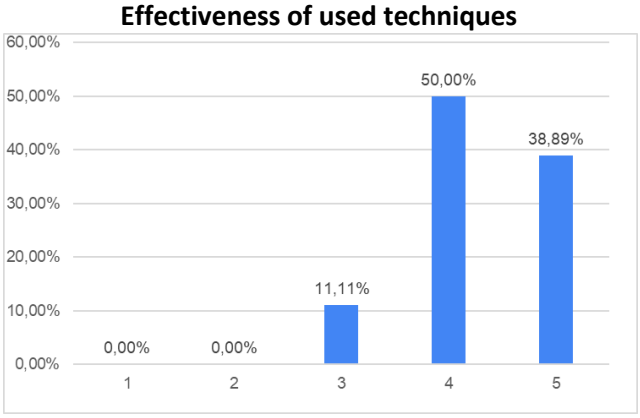

Figure 4-14: M12 Effectiveness of used techniques

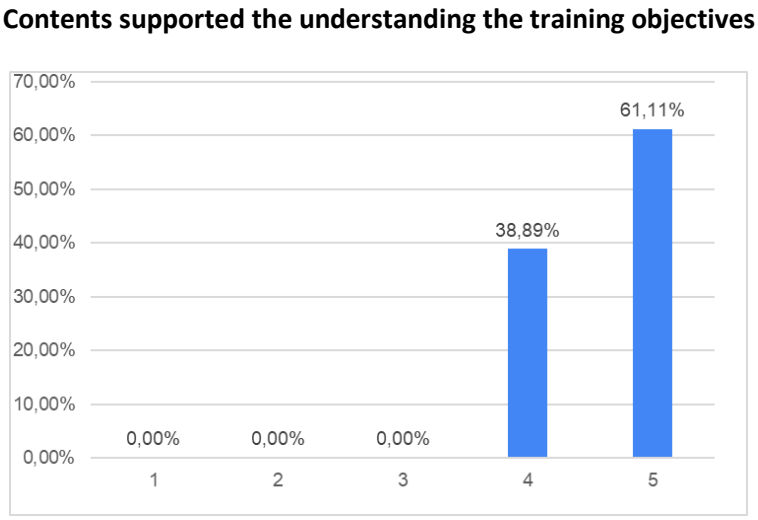

Figure 4-15: M12 Contents support the understanding the training objectives

Finally, the Figures 4-16 to 4-18 show the evaluation about the aspects regarding the organization of the training. The training was a hybrid event during the afternoon of the second stakeholders' workshop. Most of the participants evaluated the hybrid format as an appropriate approach but some of them commented that following the training was more difficult in a hybrid format. According to the answers, more time was needed, and the methods adopted to involve the participants in the training was appreciated.

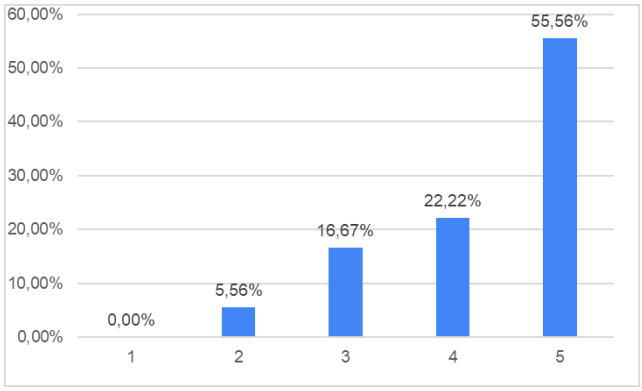

Figure 4-16: M12 The hybrid format is appropriate

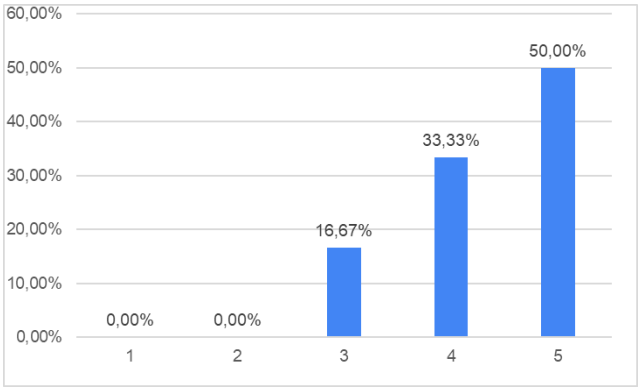

Figure 4-17: M12 The training will help in my role

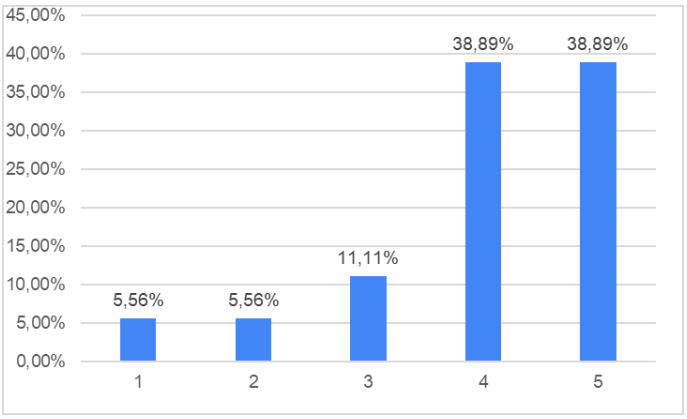

Figure 4-18: M12 The time allocated to training was sufficient

5 Training M24

It was decided that the M24 training session would be organised together with the PRECINCT general assembly event for two main reasons: i) the CI stakeholder community was already attending this event i.e. a target audience would be present, and ii) the PRECINCT tooling was mature enough in M24 to be fully presented and subsequently obtain valuable feedback from the CI stakeholders.

In the following section, the details of the contents delivered, and the feedback received, are provided.

5.1 Contents

The main objectives of this session of training were mainly the same as those in the M12 session.

- To familiarize the audience with the PRECINCT's concepts, innovation, blueprints and tooling;
- To obtain feedback on the PRECINCT Results presented.

As the focus in M12 had been the cascading effect, interdependency graph, resilience methodological framework and Serious Game, the focus in the M24 training switched to other aspects of PRECINCT. An approach to prepare training sessions in 'blocks' meant that each 'block' could be reused in other future trainings about PRECINCT. The tools presented were grouped in three different parts according to the objective of each tool.

1. **Cyber-attack detection and analysis**. In this training block, the following tools were presented: Security and privacy tool, Root Cause Analysis (RCA), Complex Events Processing (CEP) and Situational awareness UI.
2. **Simulation and response**, where the tools presented were Digital Twins (DT) and Resilience and supervisory control (RSC)
3. **Technical support**. In this block, the supporting tool to facilitate the understanding and deployment of PRECICNT Ecosystem were presented: PRECINCT Blueprints Directory, Big Data Infrastructure Services (BDIS) and Knowledge graph.

The agenda followed during this M24 session is presented in Table 5-1.

Table 5-1: M24 Training Session Agenda

Title	Trainers
Introduction	Marisa Escalante (TNCL)
FLOW 1: Cyber Attack detection and analysis	
Collection of information (Network traffic & Events): Agents and Broker	Marisa Escalante (TNCL)
Anomaly Detection and Root Cause Analysis	Vinh Hoa La (MON)
Complex events processing	Nicola Durante (ENG)
Situational Awareness UI	Nicola Durante (ENG)
FLOW 2: Simulation and response	
Digital Twins: Core elements	Mircea Iacob (IMEC)
Resilience and supervisory control	Jose Carlos Carrasco (BSC)
e-Learning Module	Benoit Baurens (Akkodis)
Tools to support the flows	
PRECINCT Blueprints Directory	Djibrilla Amadou Kountche (Akkodis)
BDIS: Big Data Infrastructure Services	Nicola Durante (ENG)
Knowledge graph	Stephane Kundig (KNT)

5.1.1 Cyberattack detection and analysis

The objective of the process flow described in this section is to present the activities and tools required to detect an attack and to analyse it. There are three main activities followed in PRECINCT (Figure 5-1) to complete this first flow of the PRECINCT Ecosystem.

- **Collect information from the CI**: The objective is to capture, preprocess and send real information from the CIs for further analysis.
- **Anomaly Detection and Root-cause Analysis**: During this activity, the network traffic and trace is analyzed, the anomaly detection is done based on rules and machine learning, and a root cause analysis is performed.
- **Processing of the events**: This activity covers the ccorrelation of simple events, the identification of high-level events and provision of insights on an occurring event through the interface.

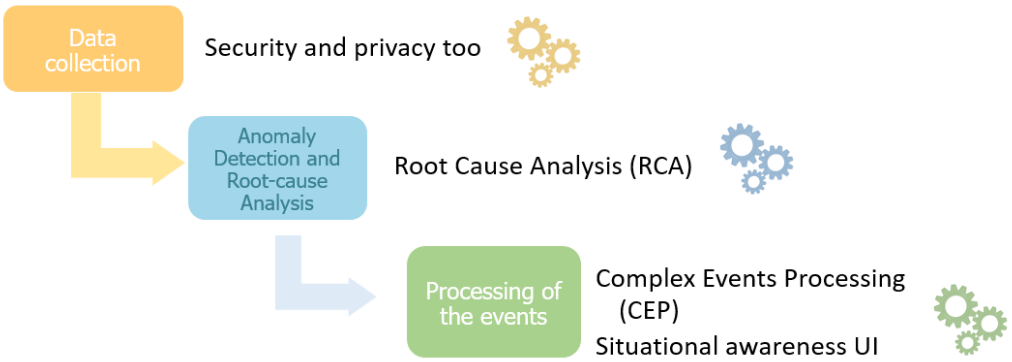

Figure 5-1: Cyber Attack and detection flow: Activities and tools

For each tool presented in the process flow in Figure 5-2, the objectives, details of the implementation, the main outputs, examples, and demos were presented during the M24 training. Following the presentation, a quiz was prepared to evaluate if the participants understood the flow and tools. The next figures show examples of some screenshots for the training of each tool.

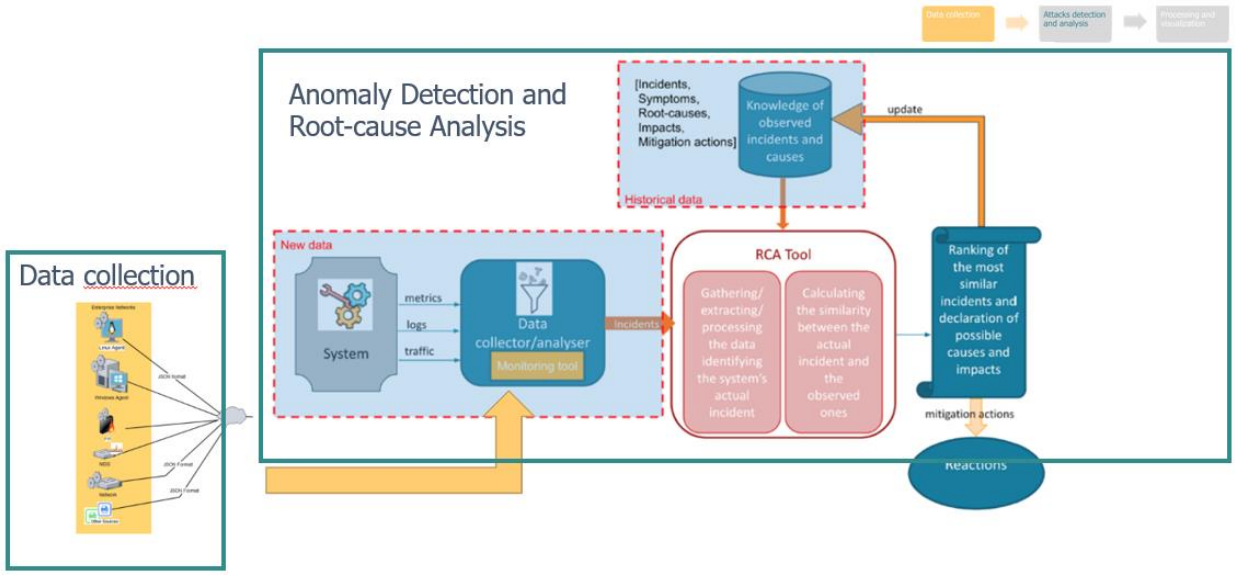

Figure 5-2: Security monitoring tool and RCA relationship

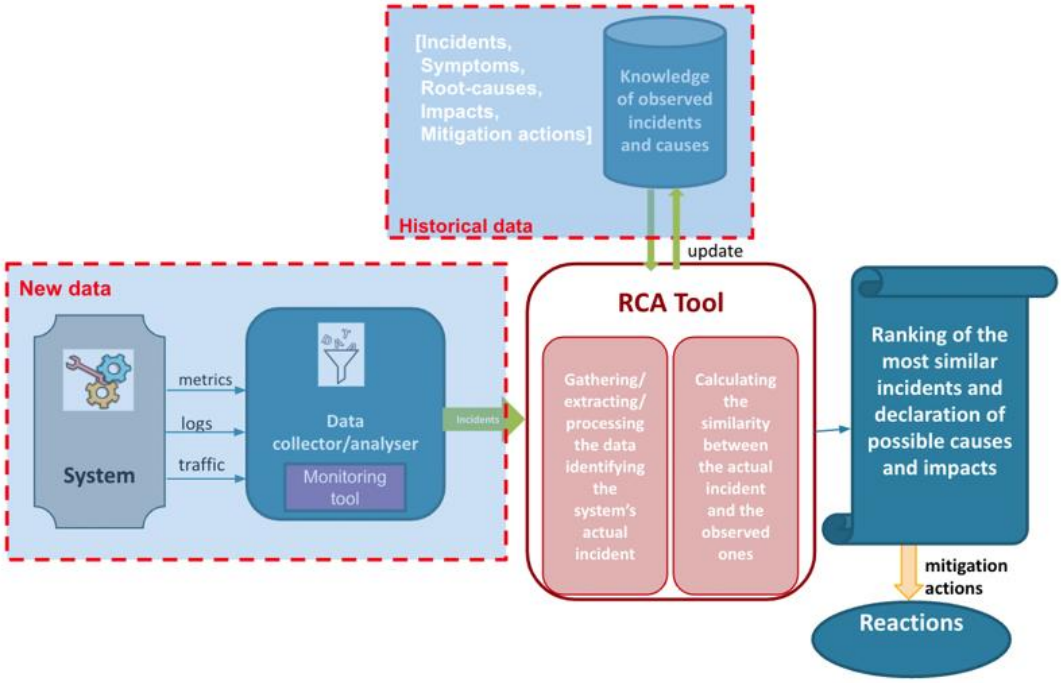

Figure 5-3: RCA Main components and flow

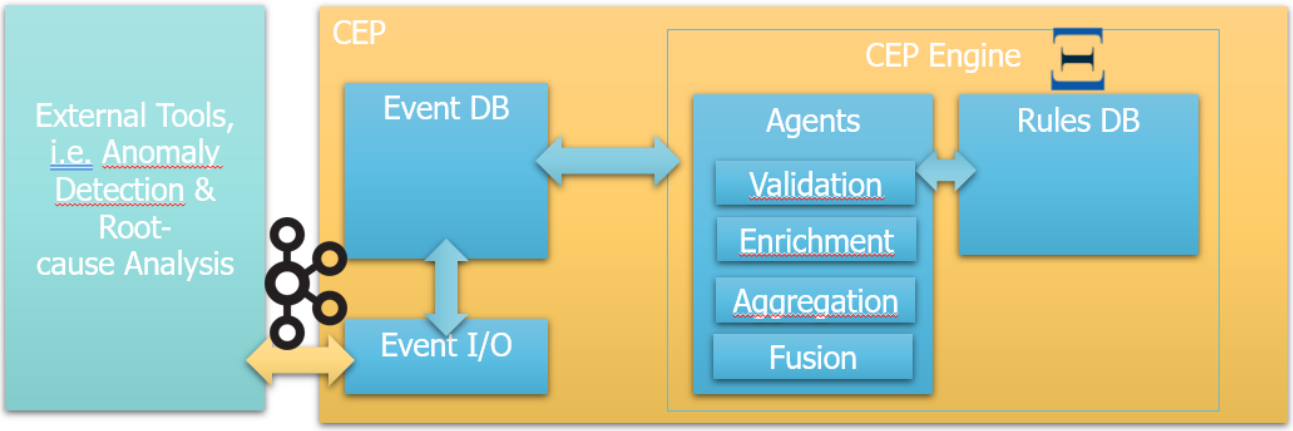

Figure 5-4: Implementation of the CEP

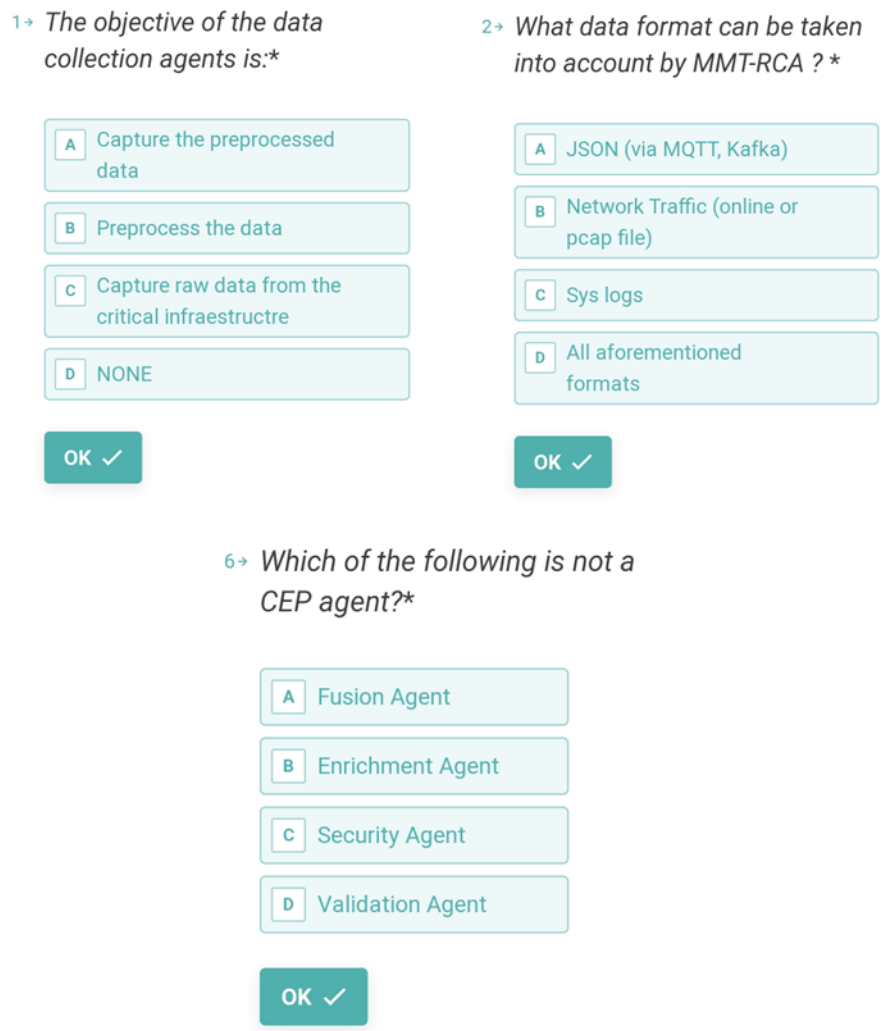

Figure 5-5: Examples of the questions of the quiz.

5.1.2 Simulation and response

In the second part of this training session, the focus was to explain the specific tools that support the simulation and the potential responses that could be given in case of CI cascading effects. As part of the process, this training block was composed of two main tools:

- **Digital Twin (DT)**: This part of the training covered several aspects to highlight the importance of the DTs inside the PRECINCT Ecosystem:
  - DT small background
  - DT architecture (Figure 5-6) and the PRECINT DT architecture in each LL
  - Detailed explanation of the functional flow.
  - DT Core components (Figure 5-7Figure 5-7)
- **Resilience supervisory control**: During this presentation, the purpose of this tool was set up so as to suggest a sequence of response actions to improve the operational state of the CIs network. The functional description and the integration within the DT Graphical User Interface (Figure 5-8) were shown. Also, a graphical demo on how this tool could be used was presented.

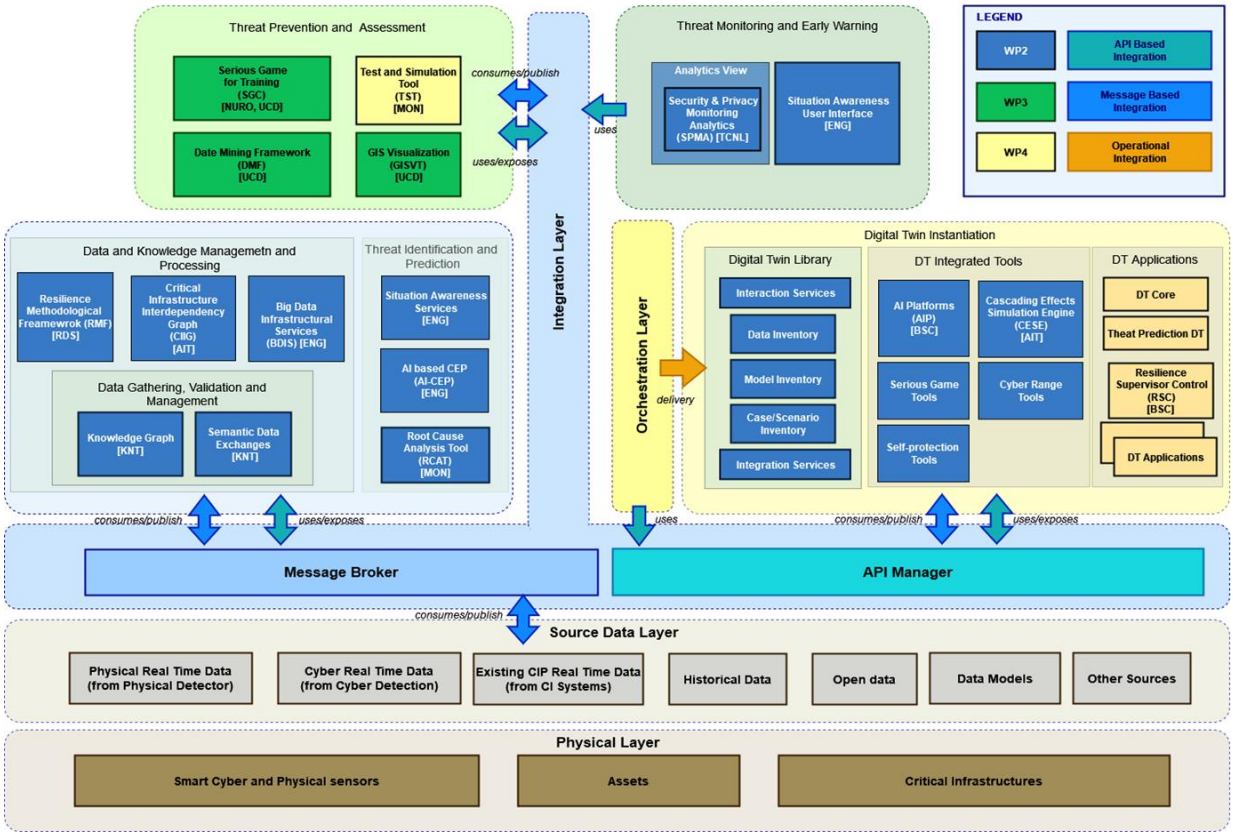

Figure 5-6: PRECINCT DT Architecture

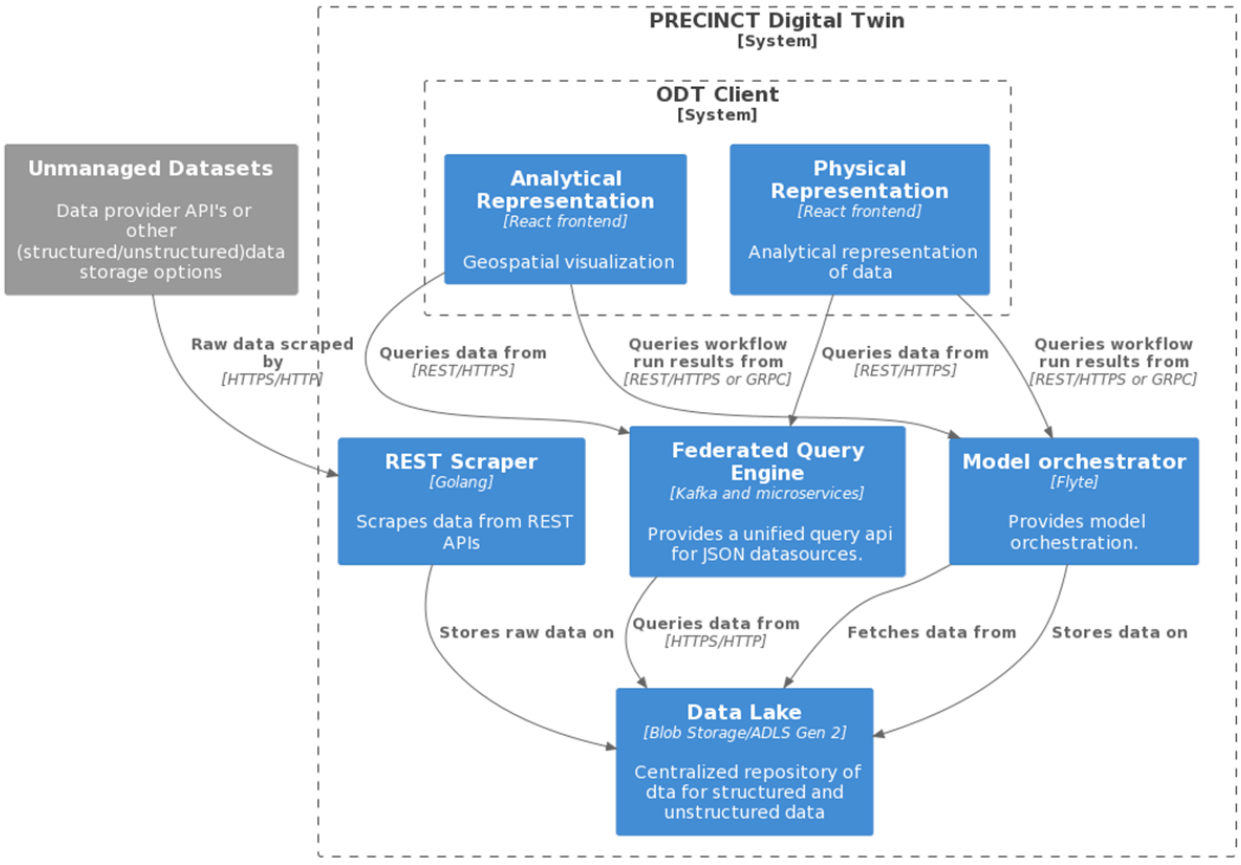

Figure 5-7: DT Core components

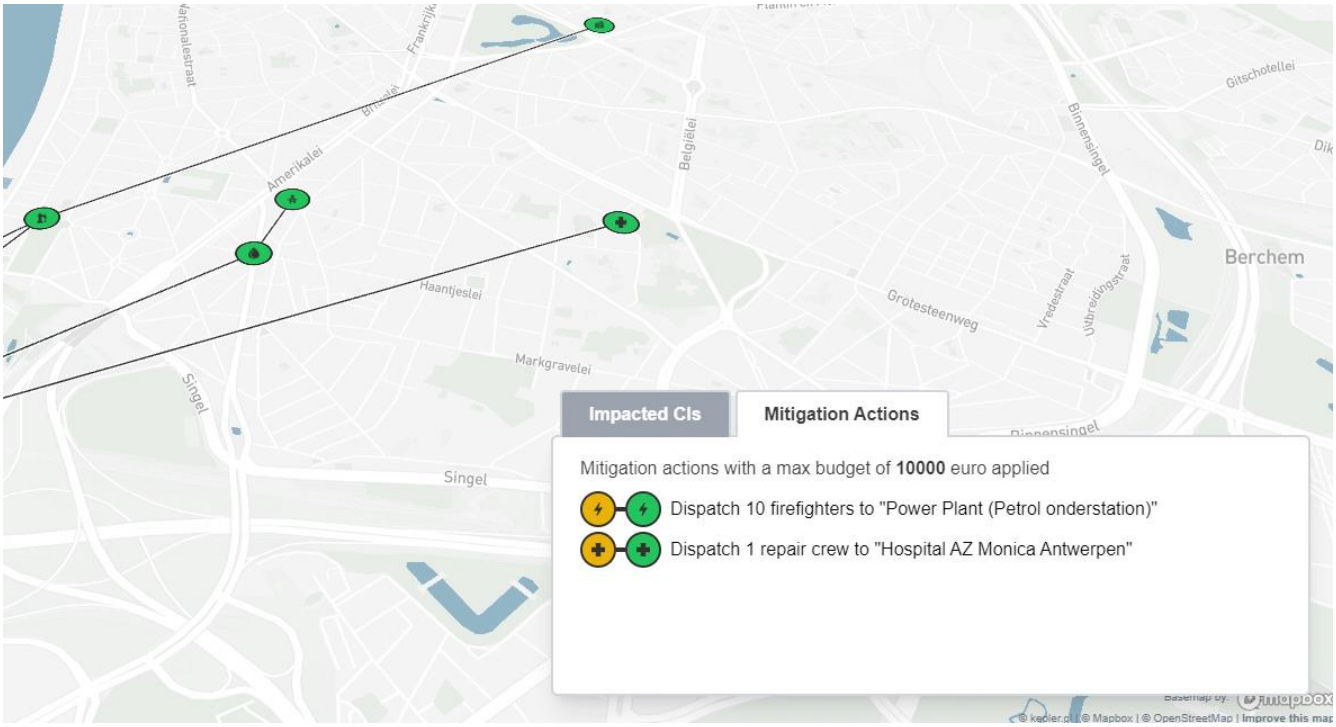

Figure 5-8: Screenshot of RSC integration in the DT GUI

After the M12 training was developed, an additional eLearning module was developed to enable users to understand their roles, the information flow in the Serious Game, the data usage in the Serious Game and how to play the Serious Game. The purpose of the eLearning module was to enable new users to understand what the Serious Game is for and how it works. They could view the eLearning module within the Serious Game itself (Figure 5-9and the purpose was to view the video prior to starting the Serious Game. Some feedback questions, based on the content of the eLearning module, probed users' understanding and the objectives of the Serious Game.

Figure 5-9: Screenshot of the introduction of the SG eLearning eLearning module

5.1.3 Technical support for adoption of PRECINCT Ecosystem

The objective of this section is to provide a description of the tools to support the adoption of the PRECINCT ecosystem. Three tools were presented in this part of the training:

- **Knowledge Graph (KG)**. The objectives of this tool are to instantiate CI assets and their interdependencies in a KG structure, to allow for data exchanges around the KG, encapsulating schema-based validation (SHACL) and to enable threshold-based event detection based on predefined rules. During the training, the detailed implementation and the main outputs were presented (Figure 5-10). A live demo of the operation of this tool was shown during this presentation.

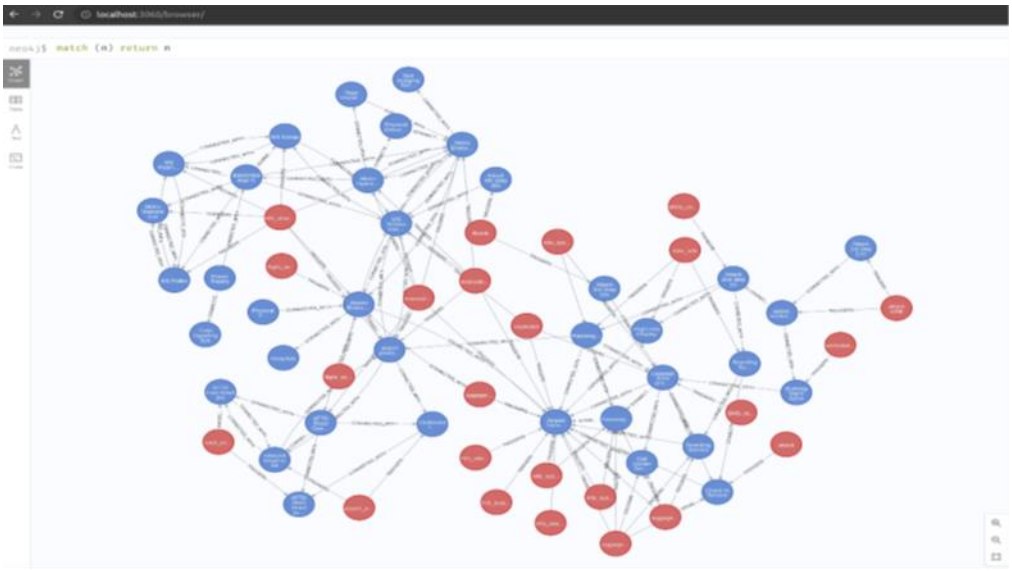

Figure 5-10. Example of KG visualization [3]

- **PRECINCT Blueprints and Blueprints Directory**: The concept behind the Blueprints is to provide a way to systematically re-use results of past CIP projects. An approach based on Blueprints, which was based on: reference architectures, human and machine-readable blueprint description languages used for deployment and orchestration, is defined to support the re-use of previous results. The presentation provided a technological and functional mapping (Figure 5-11) and how PRECINCT tooling fits within this mapping approach. Also some examples of the deployment of the blueprint were shown (Figure 5-12).

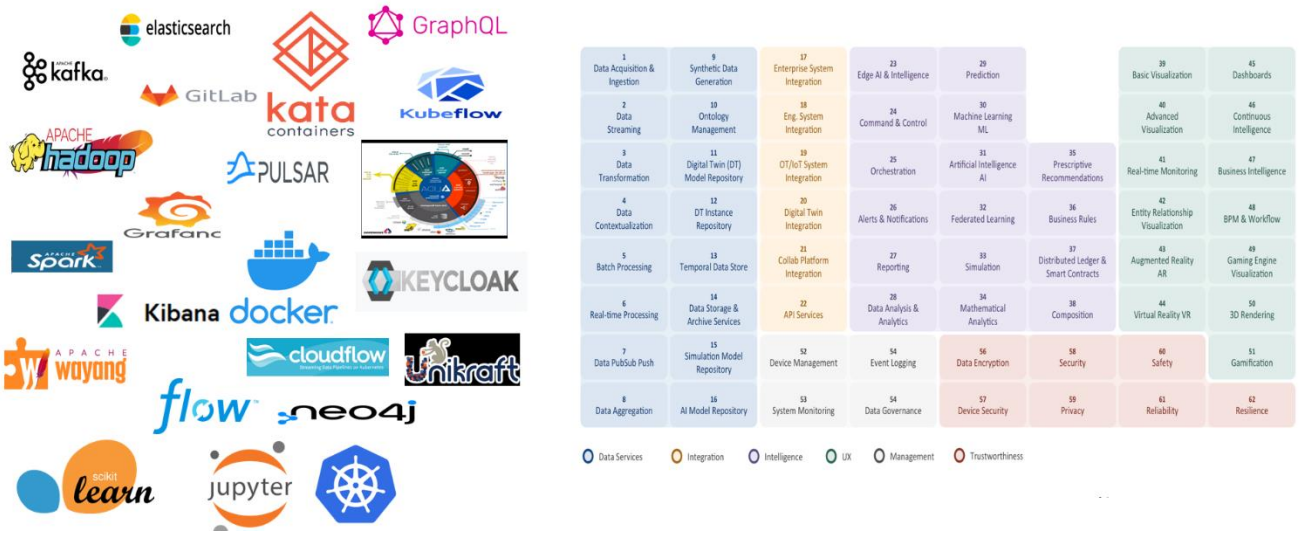

Figure 5-11: Technological and functional mapping

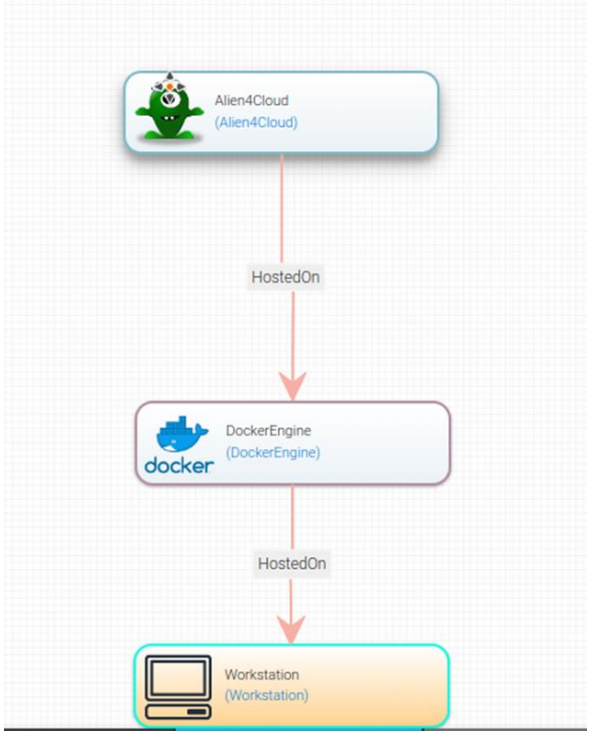

Figure 5-12: Example of deployment of the Blueprints

- **Big Data Infrastructure Services (BDIS)**: As in the other tools, this presentation showed the objectives, implementation and the main outputs. BDIS is a platform based on a microservice-based big data and ML platform, that facilitates users in the creation of big data workflows to process and visualize data. During the presentation, the steps of the implementation were described (Figure 5-13), and finally an example of how BDIS is used in LL4.

1. Can collect relevant data, events, and anomalies through the PRECINCT message broker
2. The data collected is normalized and filtered, The results are stored in a database
3. The resulting data is passed to the BDIS platform where the custom modules performing data pre-processing and data analytics
4. The results from the BDIS platform are then forwarded and elaborated by Elasticsearch
5. Using Kibana, dashboards are created that can be imported into the Unified PRECINCT Situational Awareness User Interface.

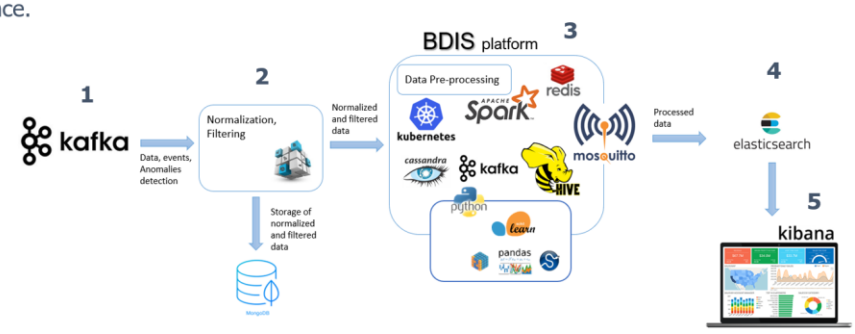

Figure 5-13: BDIS – Implementation

5.2 Evaluation

The evaluation of the M24 training session was done using the same questions and sections as those described for M12 (refer to Section 4.2.).

Figure 5-14 - Figure 5-17 show the responses related to general evaluation. Most of the participants considered as excellent or good the usefulness of the provided content and the training material, as well as considered that the structure of the training is good enough. However, some of the participants commented that some parts of the presentation are quire technical and other ones wanted to have the opportunity to interact directly with the tools during the training.

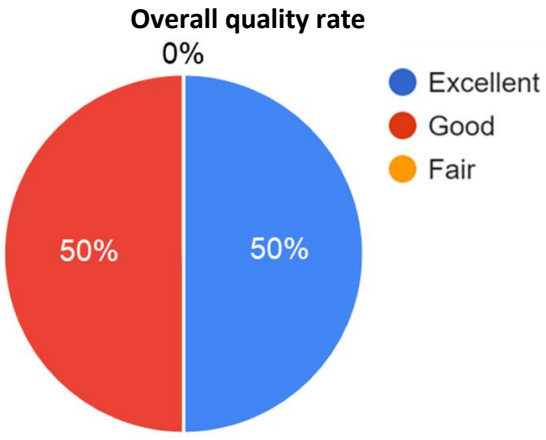

Figure 5-14: M24 Overall quality rate

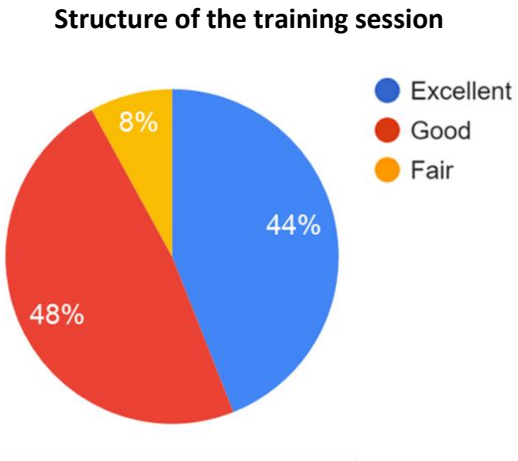

Figure 5-15: M24 Structure of the training session

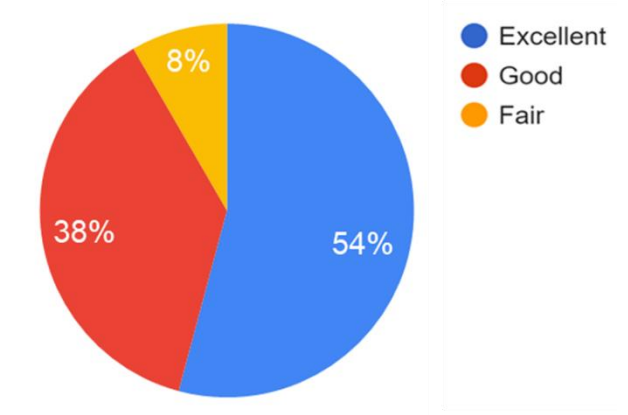

Figure 5-16: M24 Usefulness of the information received in the training

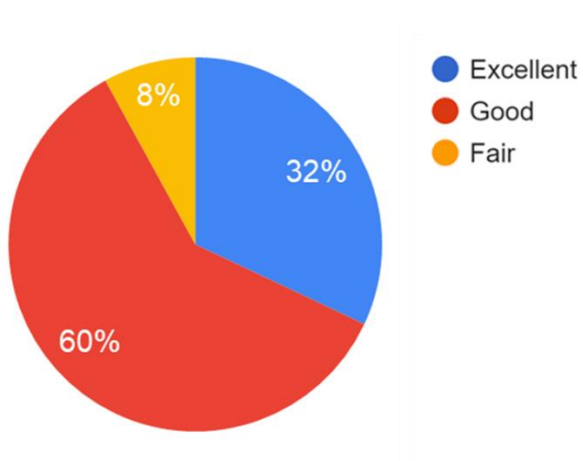

Figure 5-17: M24 Usefulness of the training material

In Figures 5-18 to 5-22 the legends mean "5" is the highest level of agreement and "1" is the lowest level of agreement. Most of the participants agreed ("5" or "4" rating) on all of the statements in this section. The participants recognised that the training covered the defined objectives and that it covered their expectations. The participants also considered that the contents and the techniques used to explain them were effective to understand the tools explained, although some of the participants mentioned that it could be useful—for a better understanding of the tool—to have the opportunity to practice with them. Some participants commented that it was a bit repetitive and that it was important to indicate that the training is focused for people with at least some technical background.

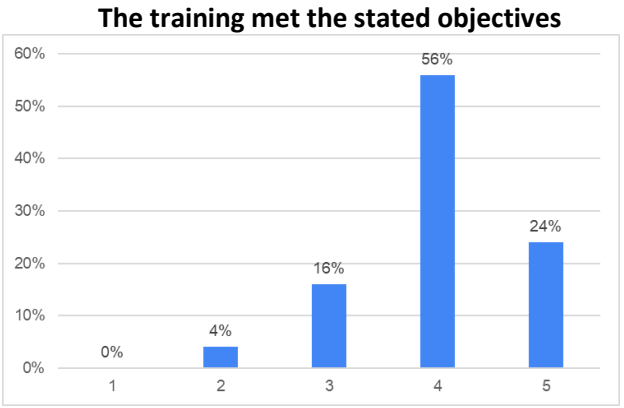

Figure 5-18: M24 The training met the stated objectives

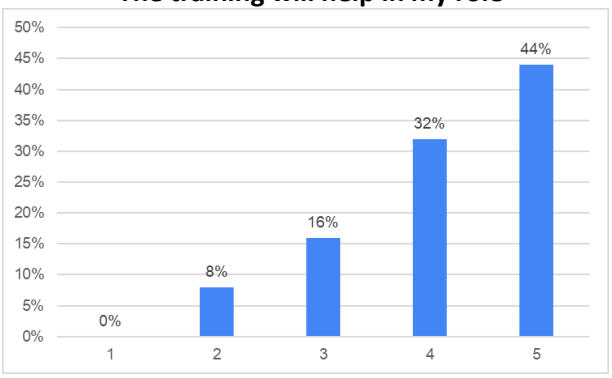

Figure 5-19: M24 The training will help in my role

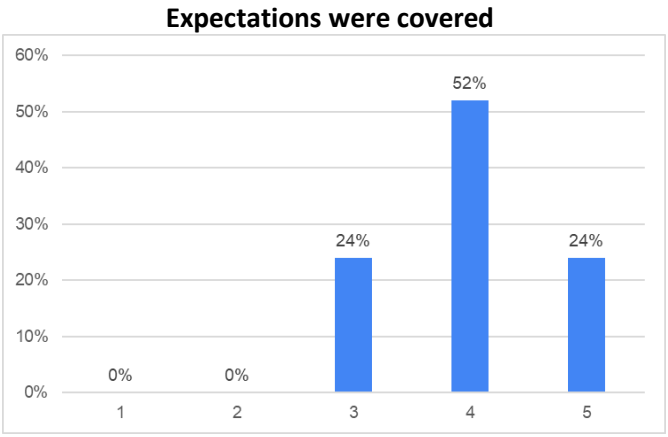

Figure 5-20: M24 The training covered what I expected it

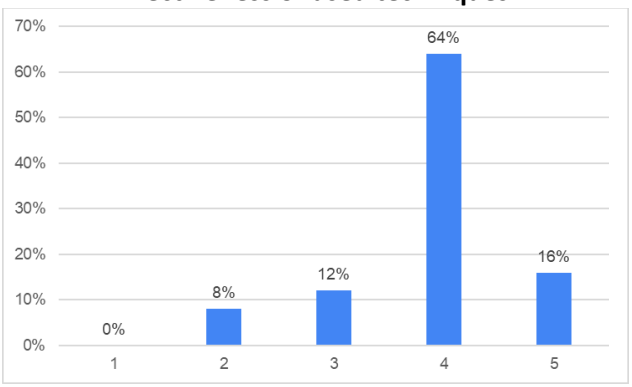

Figure 5-21: M24 Effectiveness of used techniques

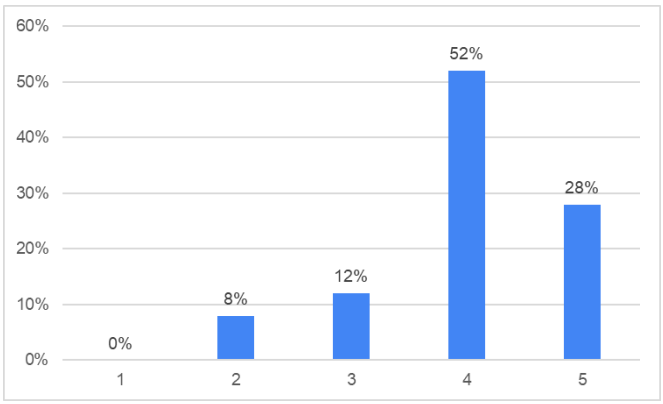

Figure 5-22: M24 Contents supported the understanding the training objectives

Finally, the responses in Figure 5-23 to 5-25elated to the aspects regarding the organization of the training. It was observed that the results are very similar to the ones obtained in the M12 training session. Most of the participants evaluated the hybrid format as an appropriate approach but some of them commented that following the training was more difficult in a hybrid format. According to the answers, more time was needed, and the method used to involve the participants in the training was appreciated.

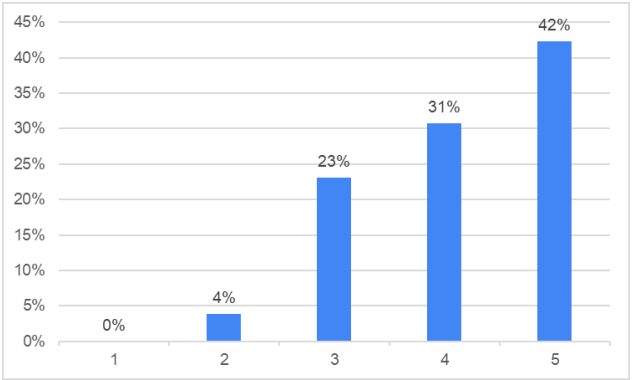

Figure 5-23: M24 The hybrid format is appropriate

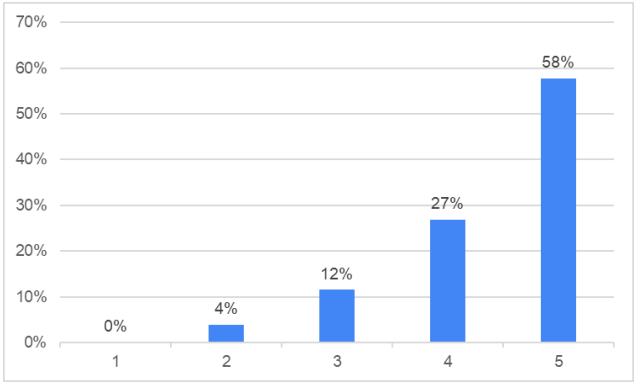

Figure 5-24: M24 The training will help in my role

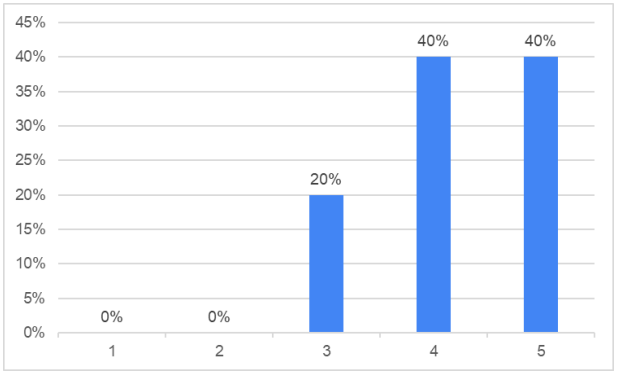

Figure 5-25: M24 The time allocated to training was sufficient

6 Training for the LLs

This section details the information provided to the LLs participants and stakeholders. The material used for this training was the different training blocks prepared for the training in M12 and M24. Some of this training was customised to each of the LL characteristics.

6.1 Contents and structure of the training

This section presents how the different training blocks presented in sections 4 and 5 were customized and presented to the LLs to facilitate understanding the implications of the PRECINT tooling in each separate LL.

6.1.1 Cyber-physical detection and alerting

The content presented in the cyber-physical detection and alerting block (

Figure 6-1) allowed users to better understand how the detection works and why the Security Monitoring Tool (TCNL), Root Cause Analysis and Test and Simulation (MON) and the Complex Event Processing (ENG) are used in the PRECINCT project.

By comprehending the inner workings of these components, participants gained insight into the key functionalities of the PRECINCT project approach to cyber-physical security. By leveraging the knowledge gained from the cyber-physical detection and alerting block, users were better equipped to enhance the security and privacy of their network infrastructure.

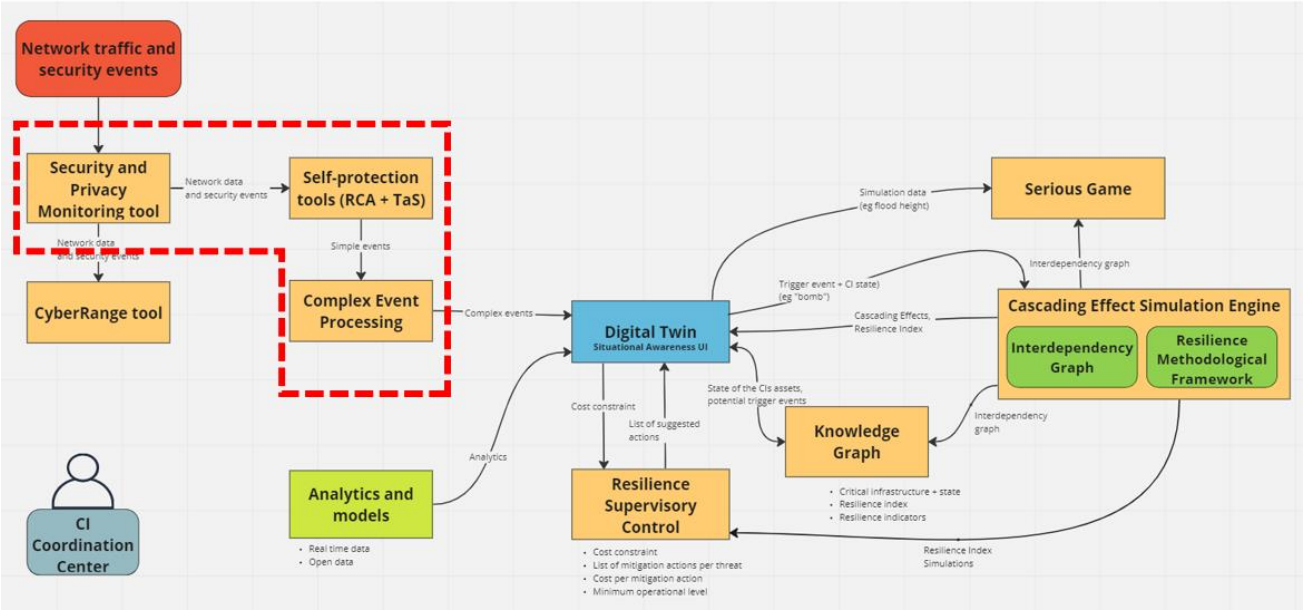

Figure 6-1: Cyber-physical detection and alerting block

6.1.2 Monitoring through a Digital Twin

This section introduced participants to the concept of utilizing a Digital Twin for effective monitoring. This block comprised several key components (Figure 6-2): the Knowledge Graph (KNT), E2E Encryption Message Exchange (ENG), Situational Awareness UI (ENG) the DT components (IMEC), and the flood model (KUL).

The Knowledge Graph (KNT) component served as a repository for storing and organizing data related to the DT. It provided a structured representation of the physical system being monitored, capturing its various attributes, relationships, and behaviours. By leveraging the Knowledge Graph, participants could gain a holistic understanding of the system's functioning and its corresponding DT.

The E2E Encryption Message Exchange (ENG) component focused on ensuring secure communication and data exchange between the physical system and its Digital Twin. It employed end-to-end encryption techniques to protect the confidentiality and integrity of the information shared. This secure message exchange facilitated real-time monitoring, enabling participants to receive accurate and reliable data from the digital twin, ensuring the integrity and authenticity of the information.

The Unified PRECINCT Situational Awareness UI (ENG) component provided a user-friendly interface that presented the monitored data and relevant insights derived from the DT (Figure 6-2). This interface enabled participants to visualize and analyse the system's current state, detect anomalies, and make informed decisions based on real-time information. By leveraging the Situational Awareness UI, participants could monitor the system's performance, identify potential issues, and respond promptly to critical events.

The DT components (IMEC) provided a description of the urban DT and it's functionality, the components integrated into the LL2 DT and the possible actions that could be undertaken in the DT (flow of actions). One of the examples presented identified the flow initiated in the DT when there is a flood alert in Antwerp city (see Figure 6-3). the example also presented the real time flow in the DT and the actions to gather the CP-Ops that can be done based on the flood model predictions provided in the DT. KUL introduced the Antwerp city's pluvial-flood model and rainfall nowcasting developed and deployed in the DT tool.

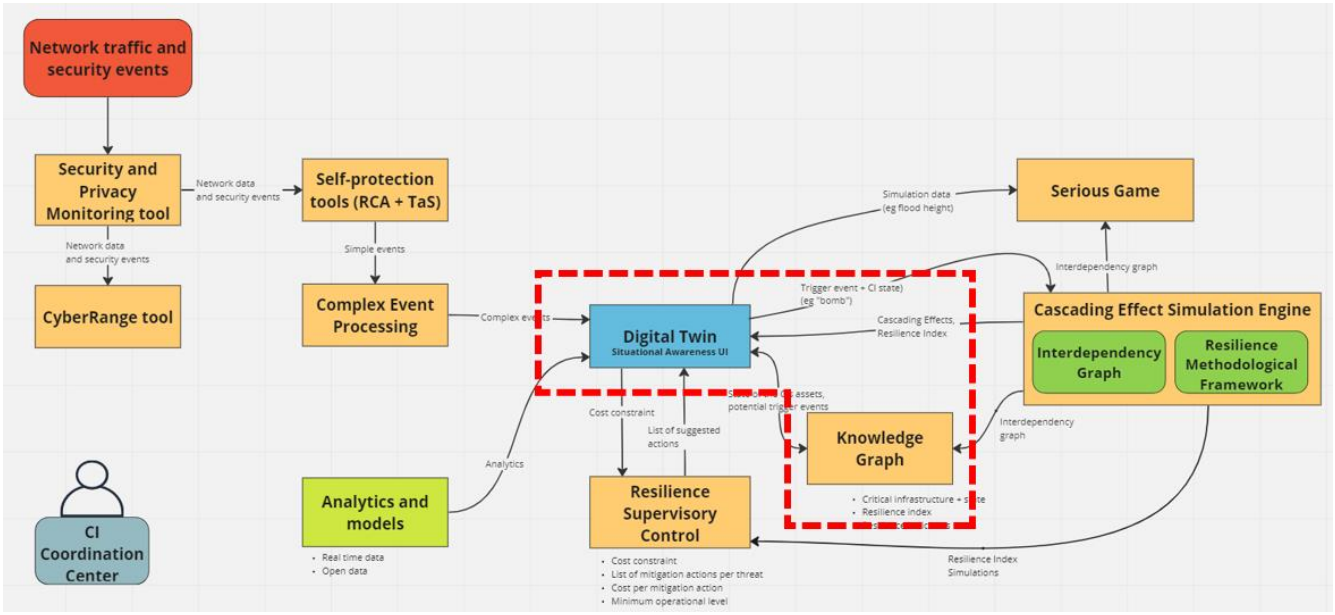

Figure 6-2: Monitoring through a Digital Twin block

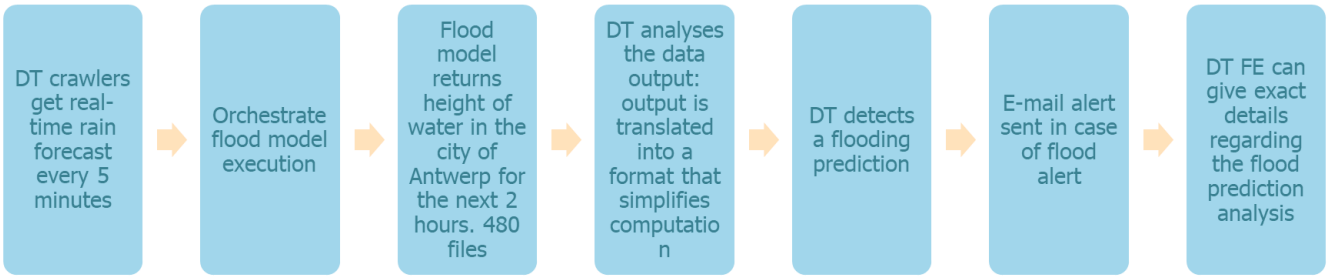

Figure 6-3: LL2 Flood model in DT - Behind the scene (IMEC)

6.1.3 Mitigation and response

The Mitigation and Response block introduces the Resilience Supervisory Control (BSC) (Figure 6-4). This component analyzes an interconnected infrastructure network and suggests mitigation actions based on a predefined budget allocation. Using advanced algorithms and risk assessment techniques, the Resilience Supervisory Control prioritizes mitigation options that provide the most significant risk reduction within the allocated budget. By following the Resilience Supervisory Control recommendations, decision-makers can proactively enhance the network's resilience, minimize vulnerabilities, and ensure the continuity of essential services, thereby optimizing system reliability and performance.

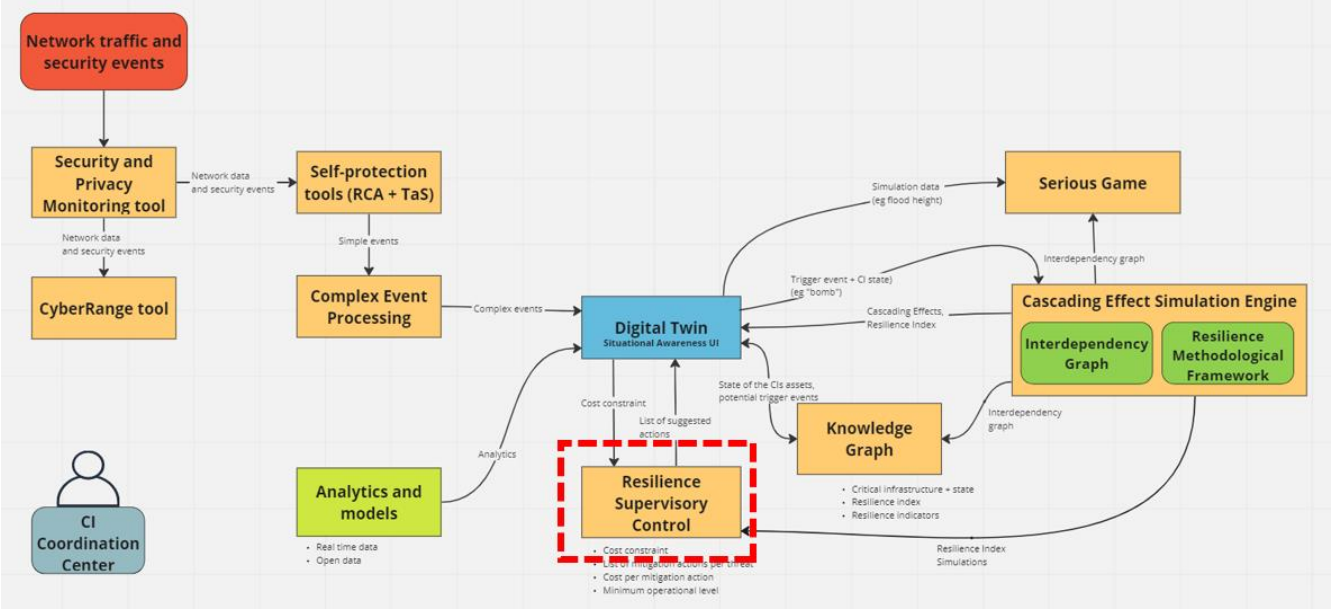

Figure 6-4: Mitigation and response block

6.1.4 Simulation and Serious Games

The Simulation and Serious Games block (Figure 6-5) encompasses three components: the Cascading Effects Simulation Engine (CESE) (by AIT), the Resilience Methodological Framework (RDS), and Serious Games (NURO & UCD).

The CESE component enables the simulation of cascading effects on the network of CIs. The CESE models and assesses the potential consequences of disruptions within the network, allowing for the evaluation of different scenarios and their impact on overall system performance. This simulation capability helps stakeholders

understand the vulnerabilities and interdependencies of CIs, facilitating proactive measures to enhance resilience and minimize cascading effects.

The Resilience Methodological Framework (RDS) component focuses on resilience index calculations. It provides a structured approach for quantifying the resilience levels of the network and assessing its ability to withstand and recover from disruptions. By utilizing this framework, stakeholders can measure and compare the resilience of different infrastructures, identify areas for improvement, and implement targeted strategies to enhance overall resilience.

Serious Games (UCD, NURO) offers an interactive and immersive learning experience. The Serious Game provides a gamified environment where participants can engage in simulated scenarios related to CI resilience. These games enable users to explore and understand the complexities of managing and responding to various disruptions, fostering skill development and decision-making capabilities in a risk-free and engaging manner.

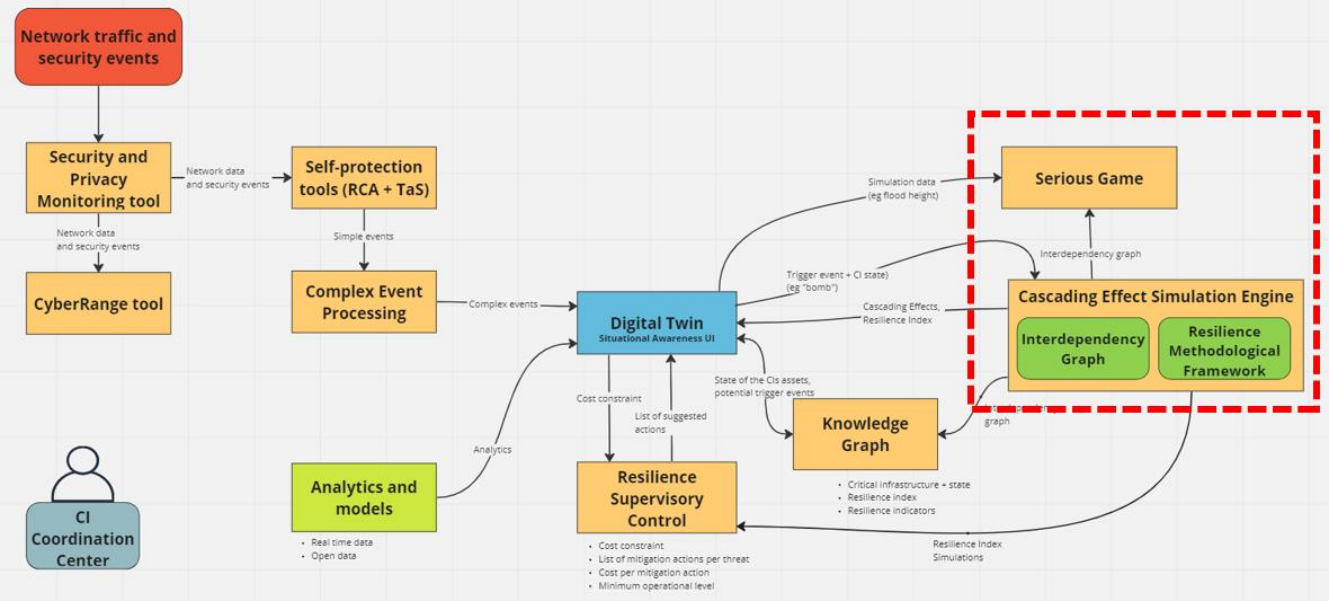

Figure 6-5: Simulation and Serious Games block

6.2 Living Labs Training Session

The following sections present the details of each of the training sessions carried out in each LL. LL1 – Ljubljana
The training session of LL1 took place on 29th May 2023 and was held online. The purpose of the training session was to present the PRECINCT solution to the LL1 end users, to give context on the components forming the PRECINCT solution and explain benefits of the components and why they are used in PRECINCT.

The training was hosted by ICS and ENG, the following technical partners attended:

- AIT
- BSC
- ICP
- KEMEA
- KNT
- RDS
- UCD

The audience was formed by the following LL1 partners:

- Elektro Ljubljana (Electric network)
- Institute of Traffic and Transport Ljubljana
- LPP (public transport)
- MOL (Municipality of Ljubljana)
- Slovenske železnice (Slovenian railways)
- Telekom Slovenije (Slovenia communications provider)

The training was divided into the following blocks:

- Cyber-physical detection and alerting (Details in section 6.1.1):
  - Security Monitoring Tool (TCNL)
  - Root Cause Analysis and Test and Simulation (MON)
  - Complex Event Processing (ENG)
- Monitoring through a Digital Twin (Details in section 6.1.2):
  - Knowledge Graph (KNT)
  - E2E Encryption Message Exchange (ENG)
  - Unified PRECINCT Situational Awareness UI (ENG)
- Mitigation and response (Details in section 6.1.3):
  - Resilience Supervisory Control (BSC)
- Simulation and Serious Games (Details in section 6.1.4):
  - Cascading Effects Simulation Engine (AIT)
  - Resilience Methodological Framework (RDS)
  - Serious Games (UCD, NURO)

6.2.1 LL2 - Antwerp

The training session of LL2 took place on 1st June 2023 and was held on site, in the Operational Command Post (CP-Ops) meeting room. The purpose of the training session was to present the PRECINCT solution to the LL2 end users, to give context on the components forming the PRECINCT solution and to explain benefits of the components and why they are used in PRECINCT.

The training was hosted by VIAS and IMEC, with the following LL2 partners:

- KUL (flood modelling)
- PZA (police)
- WTL (water utility)

In addition to the LL2 partners, the audience was made up of the following representatives from the CP-Ops disciplines and Crisis management team of the City of Antwerp. The latter stakeholders were not consortium partners but were invited as key stakeholders/end-users of PRECINCT ecosystem platform:

- Fire department
- Medical emergency services
- Communication Emergency department
- Civil Protection
- CP-Ops director
- Resilience Manager of Antwerp city
- Disaster Manager of Antwerp city
- Coordinator of Emergency and Incident Management of Antwerp city

The following consortium partners attended the session online:

- UCD

- NURO
- AIT
- BSC
- ENG
- ICP

The training was divided in the following blocks (refer to Figure 6-6):

- PRECINCT project in a nutshell (VIAS and PZA)
  - LL2 ambitions
  - LL2 components deployed (SG and DT)
- Simulation and Serious Games (Details in section 6.1.4):
  - Cascading Effects Simulation Engine (AIT)
  - Resilience Methodological Framework (RDS)
  - Serious Games (UCD, NURO)
- Monitoring through a Digital Twin (Details in section 6.1.2):
  - Digital Twin core components (IMEC):
  - Flood model (KUL)
  - Knowledge Graph (KNT):
- Mitigation and response (Details in section 6.1.3):
  - Resilience Supervisory Control (BSC)

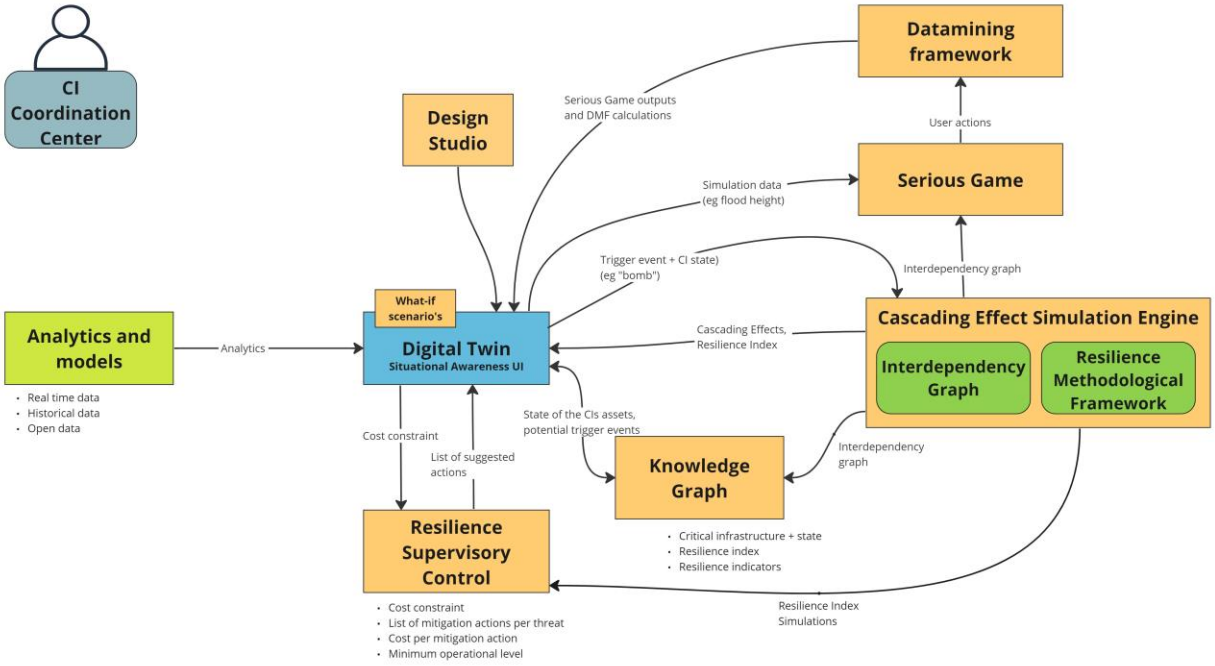

Figure 6-6: LL2 architecture

6.2.2 LL3 - Athens

PRECINCT LL3 consists of three CIs providing transportation services in the broader area of Athens and more specific those areas are:

- Athens International Airport (AIA) the largest and busiest international airport in Greece, serving the city of Athens region.
- Atiiked Diadromes S.A. responsible for the operation and maintenance of the Attiki Odos Motorway. The motorway mainly links the airport to the city center, as well as other public transport modes.
- AMETPO is the owner of infrastructure and critical assets such us tunnels,stations,depots etc. oof the Athens Metro network.

As described, LL3 consists of three different organizations and as part of the PRECINCT LL3 demonstrations, stakeholders from each organization were invited to be present and/or participate in them. For example, some roles/colleagues invited included Civil and Transport Engineers, Data Analysts, Crisis Planning Supervisors, members from the Traffic Management & Maintenance Department and the airport's Network Operation Center (i.e. System and Information Security engineers) and others. Therefore, since such a heterogenous set of LL3 CIs stakeholders would be present during PRECINCT demonstration day, it was decided that prior to the actual demonstration of PRECINCT platform capabilities or the usage project's solutions from LL3 end-users, a series of training session should take place to ensure that all the project's stakeholders/end-users were up to date about project's developments, the logic and how to use platform tools/components.

To this end, two training sessions took place prior to the demonstration of the actual tools. The format of the trainings/training material included presentations, pre-recorded videos, or manuals helping PRECINCT end users to get more familiar with PREICNCT tools and framework. In more detail, the first demonstration and respective training session took place on 12th June 2023, online. The purpose of the training session was to present to LL3 end-users the PRECINCT LL3 Digital Twin solution components and explain benefits of each component, how they can detect threats and why they are used in PRECINCT. The training and demonstrations were coordinated by Inlecom and Konnecta.

The first session of training was divided into the following blocks:

Objective: Usage of Digital Twin Solution for Operational Improvement

Introduction to Digital Twin Concept and LL3 DT Architecture (KNT). (Details in section 6.1.2)

Cyber detection (Details in section 6.1.1)

- Security Monitoring tool (SPM) (TNCL)
- Root Cause Analysis (MMT-RCA) (MON)
- Test and Simulation (MMT-TaS) (MON)

Preparedness and Alerting (Details in sections 6.1.1, 6.1.2 and 6.1.4)

- Complex Event Processing (ENG)
- Cascading Effects Simulation Engine (AIT)
- Knowledge Graph (KNT)
- Resilience Index Framework (RDS)

Response and Coordination

- Resilience Supervisory Control (BSC) (Details in section 6.1.3)
- PRECINCT Blueprints (AKKA) (Details in section 5.1.3)
- Coordination Centre (KEMEA)

The second demonstration and respective training session took place online on 11th July 2023. Prior to that day, an educational video was shared among the LL3 CIs members.

Objective: Serious Game for Resilience Improvement

- PRECINCT Serious Game E-learning module (AKKA - Prerecorded video) (Details in section 5.1.2)
- LL3 Interdependency Graph and Resilience (AIT-RDS) (Details in section 6.1.4)
- Serious Game Application – User Interface and Game Roles (NURO) (Details in sections 6.1.4)
- Data Mining Framework (UCD-Pre-recorded video)

6.2.3 LL4 – Bologna

The training session of LL4 took place on 16th June 2023 and was held online. The purpose of the training session was to present the PRECINCT solution to the LL4 end users, give context on the components forming the PRECINCT solution and explain benefits of the components and why they are used in PRECINCT.

The training was hosted by ITL and ENG and the following technical partners attended:

- AIT
- AKKA
- BSC
- ICP
- MON
- NURO
- RDS
- TCNL
- UCD

The audience was formed by the following LL4 partners:

- AdB (Bologna Guglielmo Marconi Airport)
- Comune di Bologna ()
- FSTechnology (ICT Company of the Ferrovie dello Stato Italiane Group)
- LEPIDA (ICT Services)
- SRM (Public Transport Authority in Bologna)
- TPER

Following the same structure used for LL1, the LL4 training was divided into the following blocks:

- Cyber-physical detection and alerting (Details in section 6.1.1):
    - Root Cause Analysis and Test and Simulation (MON)
    - Complex Event Processing (ENG)
- Monitoring through a Digital Twin (Details in section 6.1.2):
    - Knowledge Graph (KNT)
    - E2E Encryption Message Exchange (ENG)
    - Unified PRECINCT Situational Awareness UI (ENG)
- Mitigation and response (Details in section 6.1.3):
    - Resilience Supervisory Control (BSC)
- Simulation and Serious Games (Details in section 6.1.4):
    - Cascading Effects Simulation Engine (AIT)
    - Resilience Methodological Framework (RDS)
    - Serious Games (UCD, NURO)

7 Conclusions

The Capacity Building programme created during the PRECINCT project has been prepared for being delivered as a whole or customized training according to the requirements, background, and/or role of the participants.

Six different training blocks were created:

- Cascading effects and interdependency graphs
- Resilience Methodological Framework
- Serious Games
- Cyber Attack detection and analysis
- Simulation and response
- Technical Support

This material was used to deliver two general PRECINCT training session (M12 and M24) to an audience of CI stakeholders and four training sessions customized to each LL and with the attendance of all the involved stakeholders.

According to the feedback provided, the quality and usefulness of the training was very well rated. But some remarks pointed to the issue that some technical background was required by the audience of the training in order to reap the expected benefits.

As the objective of this task is to obtain a great impact, this training material will be accessible through the webpage of the PRECINCT Webpage (https://www.precinct.info/en/)

8 References

[1] PRECINCT consortium, “D1.2 Critical Infrastructure Interdependencies and Cascading Effects Interdependency Graphs,” 2022.

[2] PRECINCT Consortium, “D1.3 Resilience Methodological Framework,” 2022.

[3] PRECINCT Consortium, “D2.1 Semantic CIs Connectivity and Dynamic Integration Infrastructure,” 2023.