CitySCAPE Presentation

Alkiviadis Giannakoulias, Paraskevi Plagaki
European Dynamics SA

CitySCAPE Overview, Architecture and Risk Assessment Approach

Project at a Glance

- **Call identifier**: H2020-SU-DS-2019
- **Topic**: SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors
- **EC Funding:** 6 293 011,25 €
- **Duration**: 36 months
- **Consortium**: 15 partners
- **Coordinator:** Institute of Communication and Computer Systems (ICSS), Greece – Dr. Angelos Amditis (a.amditis@iccs.gr)
- **Learn more**: www. cityscape-project.eu
- **Join us**: @EUCityscape CitySCAPE Project

Cybersecurity and multimodal transport: The Challenges

- Realization of truly interconnected transport systems
- Need for globally cyber-secure systems
- The mosaic of ICT services integrated over interconnected infrastructures makes it increasingly vulnerable to cyber-attacks
- Personal hand-held devices of users increase the system's attack surface
- Transport services relate to other NIS Directive areas that scale-up relevant cybersecurity and security-assurance challenges.
- Authorities' collaboration is needed

CitySCAPE Objectives

- **Enhance** cybersecurity technologies in the multimodal passenger transportation ecosystem at city-level addressing users and data privacy concerns

- **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

- **Improve** the proactive approach of handling cybersecurity challenges and actively contribute to the predictability of threats in (regional) multimodal transport systems

- **Enhance** end-user engagement towards the definition and provision of multimodal passenger transport requirements about digital security, privacy and personal data protection

CitySCAPE Objectives

- Further **strengthen** the role of CERTs/CSIRTs by providing them with direct/real-time informative notifications about observed cybersecurity incidents and facilitate the collaborative investigation of incidents in line with the NIS Directive
- Significantly **contribute** to multimodal transport standards and gain experimental evidence on the feasibility of security labelling in city-level multimodal transport
- **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
- **Analyze** and **outreach** the multimodal transport security market to maximize the CitySCAPE footprint and exploitation.

CitySCAPE Solution

CitySCAPE introduces innovative risk analysis techniques and orchestrates a number of software solutions to realize an interoperable toolkit that seamlessly integrates to any multimodal transport system.

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.

CitySCAPE Solution

Impact

CitySCAPE

- ✓will offer the **concrete technical basis** for a unique opportunity of an efficient collaborative threat investigation among a broad set of CERTs/CSIRTs by introducing **a platform capable of sharing information coming from different sources** and therefore achieve the maximization of the CSIRT network added value
- ✓will allow **an accurate identification of so-far under-explored/hidden privacy risks** serving the in-depth application of privacy-by-default principle and GDPR regulation in all city-level transportation stakeholders
- ✓will **introduce and validate an agile concept of a standalone interoperable solution** to manage current cybersecurity/privacy risks across complex interconnected infrastructures
- ✓will **estimate the attack impact on both technology and financial terms** that will drive a cost-benefit analysis on potential further investments to cybersecurity and privacy countermeasures
- ✓will provide a scheme for **cybersecurity labelling** for City-level multimodal travel

Impact

CitySCAPE

- ✓will address related security issues of mobile devices, **increasing passengers' safety** in city-level transport
- ✓will **identify and track the potential path of a cyber-attack** across the whole multimodal transport chain showcasing how an attack may unexpectedly affect modules that are not directly connected to its entry point
- ✓will immediately **strengthen the CERTs/CSIRTs link to the transportation stakeholders**
- ✓will **promote best practices in cybersecurity management solutions** to the multimodal transport community and through **training of security experts** will seek to communicate their value and thus, increase their acceptance
- ✓will **fill the gap in security labelling** showcasing the solid basis of a mature EU market and rendering the compliance to standards a clear path for commercial growth

Platform Components

CitySCAPE Components

Name	Functionality	Provided By	Inputs	Outputs
Collaborative threat investigation platform (CTIP)	Discover new Advanced Persistent Threats	ACS	Kaspersky threat data feeds Information from CERTs/CSIRTs Information from databases Information from CTI teams (Cyber Threat Intelligence) IoC from CSIRP	Information about the activity of APTs IoC and IoA
Collaborative security incident response platform (CSIRP)	Perform collaborative analyses on incident responses	ACS	Alerts/incidents from SIEM Logs from SIEM IoC and threat report from CTIP Information from multiple CERTs/CSIRTs and security management teams	Incident reports

CitySCAPE Components

Name	Functionality	Provided By	Inputs	Outputs
SIEM	A correlation engine monitoring the CPaaS platform.	ACS	Event logs from CPaaS Event logs from IPS/IDS IoC and IoA from CTIP	Alerts/incidents Notifications of alert/incident towards CPaaS
IDS/IPS engines	Detect anomalies and traces of attacks/incidents. It pushes events from the network level up to the SIEM for correlation and (risk-based) response. It also provides basic blocking capabilities.	ENG	Network traffic from the CPaaS platform	Events to SIEM Blocking rules for network control systems

CitySCAPE Components

Nam	Functionality	Provided By	Inputs	Outputs
Risk analysis and Impact Assessment (RITA) engine = Risk Modelling and Analysis Tool (**RMT**) + Dynamic Risk Assessment (**DRAS**)	**RMT**: Assets identification and Asset Based Risk Analysis, Dynamic knowledge base. Operator through a well-defined UI identifies assets, creates the system model and configures the assets that will be used by the RMT algorithm. **DRAS**: overall risk and impact of the system based on individual asset risk scores, the significance and respective importance ("weight") of each asset and risk to the whole system	UPRC ED	**RMT**: - Assets database, - Risk models, - Knowledge base of vulnerabilities and risks - Threats, attacks and vulnerabilities reported by external entities **DRAS**: - Individual assets risk scores produced by RMT, - weight of each asset and risk/impact provided by the user through a well-defined methodology and a UI	**RMT**: risk analysis models, organizational and attack flows, cascading effects and individual assets risk scores and impact types **DRAS**: Overall system risk, overall system impact

CitySCAPE Components

Name	Functionality	Provided By	Inputs	Outputs
Financial impact and cost-benefit assessment engine (FIMCA)	Uses the Monte Carlo simulation Performs the Cost-Benefit-Analysis (CBA) from a pre-defined set of security countermeasures.	ENG	• Company revenues • Asset values expressed in percentages based on company revenues • Countermeasures already applied for assets protection	• Suggestions about possible countermeasure to adopt (to do: list of countermeasures and costs associated) • ROSI

CitySCAPE Components

Name	Functionality	Provided By	Inputs	Outputs
Cost-benefit analysis module	Uses STAM Risk assessment tool It will be integrated into FIMCA and aims to economically evaluate the impacts of an undesirable event. It will analyze the possible security measures that can be applied to reduce the risk and will provide an estimate of the economic investment required for their integration. Finally, a balance will be made that will compare whether the benefits justify the investment or not.	STAM	• Economic value of the asset • Countermeasures already applied for assets protection (if possible with an indication on the effectiveness) • List of possible countermeasures • Risk associated to the assets	• List and suggestions about new possible countermeasures • ROSI

CitySCAPE Components

Name	Functionality	Provided By	Inputs	Outputs
CyberSafety Management Games (CSMG)	Gamified educational training designed for the multimodal transport domain	Kaspersky	Content Definition with Use-case partners	A new map for training multimodal transport domain stakeholders, included passengers.
Cyber-range (Training) platform	Simulated environment to ensure a realistic hands-on experience for the trainees. Supports the training sessions. Hosts the CitySCAPE solution	ACS	- Virtual machines and virtual containers (CTIP, CSIRP, SIEM, RITA, FIMCA) - Realistic simulated environment brought directly by end-users systems	2 workzones (one per pilot case) with the integrated solutions (alpha and final versions) Training workzone with attack scenarios

CitySCAPE Components

Name	Functionality	Provided By	Inputs	Outputs
Kaspersky Mobile Security Software Development Kit	Library for building online security solutions for mobile devices that run the Android and iOS operating systems. Used for mitigating cyber-security threats	Kaspersky	Integration with a mobile app for public transport stakeholders.	Alerts about threats and vulnerabilities of the mobile app and the mobile device hosting the app.
Threat Data feeds	Lists of continuously updated threats by heterogeneous and highly reliable sources (Kaspersky Security Network)	Kaspersky	Feeds from Kaspersky Security Network	Feeds to SIEM

Risk Assessment

Risk analysis and impact assessment engine (RITA)

- The CitySCAPE Risk analysis and impact assessment engine (RITA) aims to provide a **collaborative risk assessment** of the multimodal transport chain.

- In the context of CitySCAPE, the RITA engine will be a **risk assessment suite** supported by a **well-defined methodology** for evaluating the cybersecurity risk in the multimodal transport ecosystem. In this context, RITA is promoting a **holistic security management and risk assessment framework**.

- RITA will conduct a risk analysis process of multimodal transport ecosystem, by **assets**, **vulnerabilities** and **threats** and by calculating the **threat probability** and by identifying the **impact** of possible attacks. However, since each of the aforementioned factors can change through time, RITA is capable of performing risk assessments either on demand or on a periodic basis.

Risk analysis and impact assessment engine (RITA)

- RITA is designed to assess the security state of the multimodal transport interconnected digital infrastructures (Communication Platform as a Service – CpaaS) based on a **Risk Assessment methodology**. RITA functions include:
  a) an automated framework for **assets identification**,
  b) the iterative **risk analysis and vulnerability assessments** on existing multimodal transport value chain assets,
  c) the **estimation of threats cascading mechanisms**, with the extraction of risk scores leading to the timely identification and warning on vulnerabilities and attack entry points,
  d) the **prediction** of forthcoming incidents using information from events, actions and abnormalities (internal or external to the system)

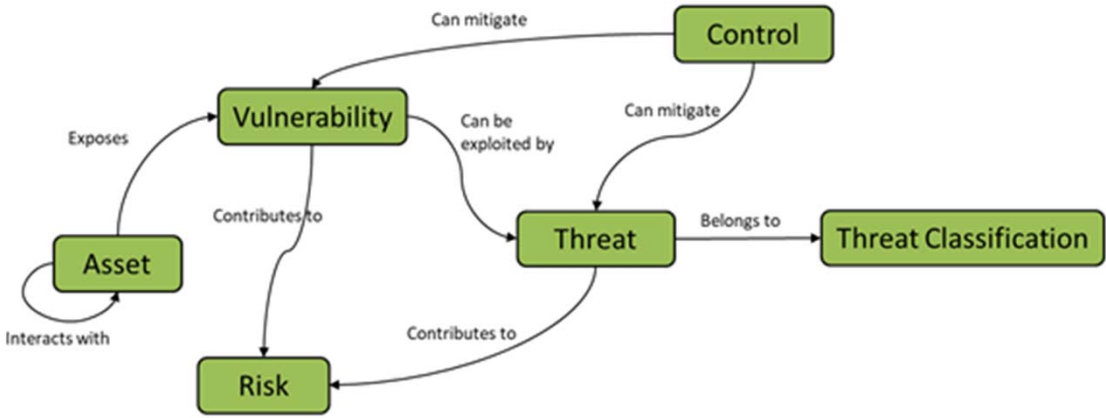
Risk analysis and impact assessment engine (RITA)

- RITA works in collaboration with other components and more specifically:
  a) the collaborative threat investigation platform (CTIP) that provides input on newly discovered Advance Persistent Threats (APTs), including interconnected threats and propagated vulnerabilities
  b) the collaborative security incident response platform (CSIRP) that provides Indicators of Compromise (IoC) and incident reports and
  c) the Financial impact and cost-benefit assessment engine (FIMCA) that provides suggestions about possible countermeasure to adopt

Methodology

Risk Assessment

- Common model that will be used during the lifecycle of the entire project and adopts concepts from the domain of Risk Assessment.
- Development of the DRAS which will be used to perform risk assessment tailored to the needs of Intelligent Public Transport (IPT) ecosystems and will take into consideration the requirements imposed by the distributed architecture of CitySCAPE and the mosaic of the adopted technologies.
- The Risk Assessment methodology will consider well-established standards, such **ISO/IEC 27001** and **ISO/IEC 27002** for Information Systems, **IEC 62443** for Industrial Cybersecurity standards and the **NIST Cybersecurity Framework**.



Vulnerabilities Management

- The practice of identifying, classifying, prioritizing, remediating and mitigating software vulnerabilities. We consider this as an integral part of computer and network security
- Vulnerabilities can be:
  - ✓ typically discovered with a **vulnerability scanner**;
  - ✓ identified by **consulting** public sources (such as NVD or CVE);
  - ✓ found using **fuzz testing** (an automated software testing technique that involves providing invalid, unexpected or random data);
  - ✓ found with antivirus software capable of **heuristic analysis**.
- In order to fix vulnerabilities, the installation of a patch may be involved, as well as a change in the network security policy, reconfiguration of software or educating users about social engineering.

Vulnerabilities Management

1. **Assets Inventory**

   One of the first steps to undertake in a vulnerability management program. Point out all assets that require protection levels. IPT systems often have large amounts of unknown assets in their environment, and these assets may compromise their safety in the long run.

2. **Information Management**

   In CitySCAPE, this is automated by keeping an updated Assets Inventory and a specific Vulnerability Repository. These databases are kept up to date by regular assessment processes.

3. **Risk Assessment**

   Essential to understand the various threats to IT systems, determine the level of risks faced by these systems, provide a quantitative and/or qualitative perception of the risk in order to ease and support the decisions of the security analysts in remediating the risk level.

Vulnerabilities Management

4. **Vulnerability Assessment**

   Key element of the vulnerability management framework, and can be considered as the primary step in improving IT security. Offers many advantages that make it possible to focus IT resources more effectively: once all the assets have been identified, all the vulnerabilities that threaten the security of those assets can be detected, providing recommendations to reduce risks.

5. **Reporting and Remediation**

   Clear and easy-to-understand report with prioritized remediation tasks. **Executive management** participation should be enforced.

6. **Response Planning**

   To apply an effective response planning process, it is essential to have an accurate and up-to-date assets list.

Vulnerabilities Management

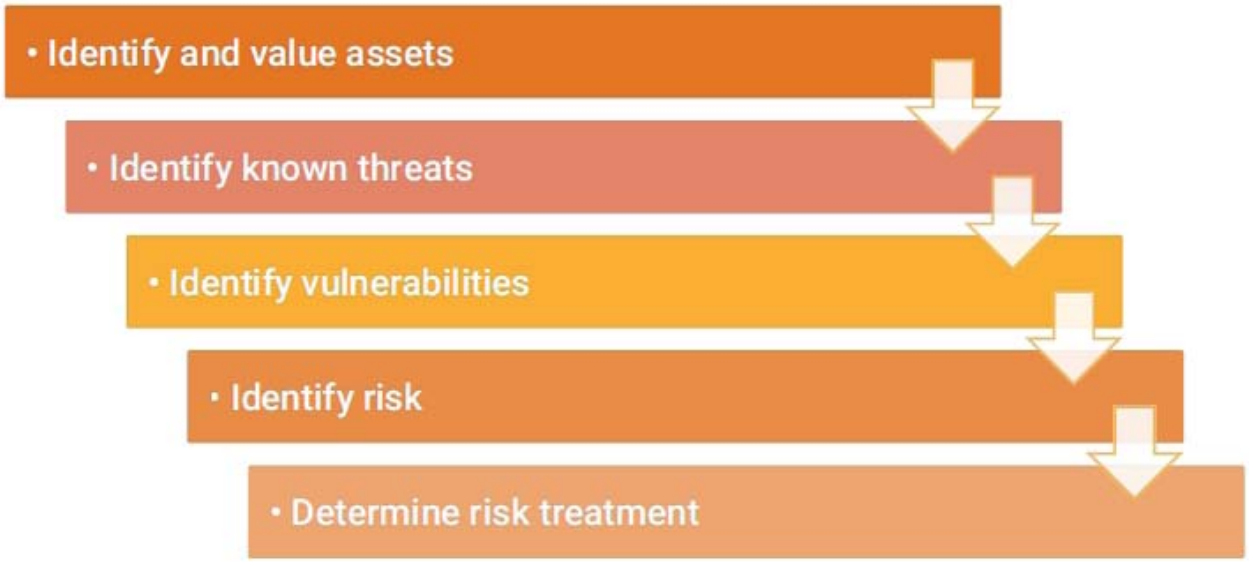
- ✓Repeat these steps on a regular basis.
- ✓To be effective it should be a continuous process (a cycle) designed to manage vulnerabilities consistently.
- ✓Vulnerability assessments should be repeated at regular intervals.

Existing Methodologies

- Several risk assessment methodologies have been proposed. The following are among the most popular ones:
  - ✓ **CRAMM** (Yazar, 2002),
  - ✓ **OCTAVE** (Caralli, Stevens, Young, & Wilson, 2007),
  - ✓ **NIST SP800-30** (Blank & Gallagher, 2012),
  - ✓ **MAGERIT** (Crespo, Amutio-Gómez, Candau, & Mañas, 2006)

Risk Assessment Methodology

- According to Information Systems Audit and Control Association (ISACA) the most common steps, include:



Approach

o Based on the above risk assessment will be based on:

- ✓ **Asset Management** that includes: Asset Identification, Valuation and Categorization;
- ✓ **Threat Modelling** that includes: Vulnerability and Threat Identification and Assessment.
- ✓ **Risk Assessment and Management** that includes: Qualitative Assessment and Quantitative Measurement of individual risk. Qualitative risk assessment methods estimate risks descriptively by using human linguistic terms, such as “low”, “medium”, and “high”. Quantitative risk measurement is based on formulas and mathematical expressions to produce numeric estimates for risks.
- ✓ **Impact Analysis** that measures the effect that can be expected as a result of the successful exploitation of a vulnerability that resides in an asset.

Assets Management

Asset Identification

- DRAS will allow the **declaration of any, customer-driven, arbitrary number of asset properties** (e.g. multiple IP addresses, MAC addresses, tag numbers, product identifiers, manufacturer settings etc.).
  - ✓ **embedded asset management system**
- **CitySCAPE user** (CPaaS security officer) is **responsible to maintain a dynamic and up-to-date asset inventory**.
- **Two types of assets** that make up the information are identified: **Tangible** and **Intangible**.
- **Three categories of tangible type assets**: **application software, operating systems** and **physical assets** (i.e. hardware equipment, buildings, staff; assessed with locations where appropriate). **Asset modelling is one of the most critical issues** since too fine granularity here may unnecessarily extend the review process, while a too coarse one may miss important assets causing misleading results.

Assets Management

Asset Valuation

Valuation of assets considers **confidentiality**, **integrity**, and **availability** dimensions (CIA triad).

1. **Qualitative valuation** which is based on the expertise of the person making the assessment. It is inherently subjective and tends to use ordinal rankings such as “low”, “medium”, and “high”. Its subjectivity is inherently localized, since what may be categorized as high in one context can be considered low or medium in another;
2. **Quantitative valuation** takes the opposite approach, assigning values based on objective monetary calculations such as net present value, replacement cost or book value. As such it eliminates the subjective localization
3. **Semi-quantitative valuation** reflects a compromise approach. It fundamentally involves qualitative assessment, often by associating subjective categories with numeric values.

Risk Assessment and Management

- To **quantitative** assess **risk** of a multimodal transport organization's specific IT assets, the potential risk value and the probability that the hazardous event will occur, are required as shown in the following formula:

*Risk Impact = Potential Risk * Probability of Occurrence*

- **Potential Risk** could be any type of risk that is conceivable for a business or any risk associated with an action that is possible in certain circumstances. Risk potential should be estimated without a detailed consideration of the individual risk, and is the product of total asset value, severity of vulnerability and severity of threat, as shown in following formula:

*Potential Risk = Total Asset Value * Severity of Vulnerability * Severity of Threat*

Risk Impact

- **Probability of Occurrence**, is an estimate of how often a hazardous event occurs. The likelihood can be expressed in terms of the frequency of occurrence. A review of historic events assists with this determination.

Value	Explanation	Example
1	Never happened	Not happened in last 3 years
2	Rare	Once in year
3	Periodic	Once in a quarter
4	Regular	Once in a fortnight
5	Frequent	Once in a week

Asset Identification, Valuation and Categorization

- **Asset Valuation,** is the worth of the organization's information system assets based on its CIA security, using the following formula:

Total Asset Value = Asset Value * Weight of Asset

- Assumptions for asset valuation include:
  - ✓ The value of an asset depends on the sensitivity of data inside the container and their potential impact on CIA.
  - ✓ The value of levels for CIA could be based on a simple rating of: 3 (high), 2 (medium) and 1 (low) or on a more elaborate one as the CRAMM.
  - ✓ The value of the information asset is determined by the sum of the three (C + I + A) attributes.

Asset Identification, Valuation and Categorization

	CIA Matrix									
	Confidentiality	Low (1)			Medium (2)			High (3)		
	Integrity	L	M	H	L	M	H	L	M	H
Availability	Low (1)	3	4	5	4	5	6	5	6	7
	Medium (2)	4	5	6	5	6	7	6	7	8
	High (3)	5	6	7	6	7	8	7	8	9

Asset Identification, Valuation and Categorization

Potential Impact			
Security Objective	Low (1)	Medium (2)	High (3)
Confidentiality The unauthorized disclosure of data or information could be expected to have a:	Limited adverse effect on organizational operations, organizational assets, or individuals	Serious adverse effect on organizational operations, organizational assets, or individuals	Severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Integrity The unauthorized modification or destruction of data or information could be expected to have a:	Limited adverse effect on organizational operations, organizational assets, or individuals	Serious adverse effect on organizational operations, organizational assets, or individuals	Severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Availability The disruption of access to or use of information or an information system could be expected to have a:	Limited adverse effect on organizational operations, organizational assets, or individuals	Serious adverse effect on organizational operations, organizational assets, or individuals	severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Asset Identification, Valuation and Categorization

Potential Impact			
Security Objective	Low (1)	Medium (2)	High (3)
Accountability Not being able to ensure that the actions of an entity may be traced uniquely to that entity could be expected to have a:	Limited adverse effect on organizational operations, organizational assets, or individuals	Serious adverse effect on organizational operations, organizational assets, or individuals	severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Non-repudiation Not being able to protect against an individual falsely denying having performed a particular action could be expected to have a:	Limited adverse effect on organizational operations, organizational assets, or individuals	Serious adverse effect on organizational operations, organizational assets, or individuals	severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Authenticity Not being able to be prove that data or information is genuine and can verified and trusted could be expected to have a:	Limited adverse effect on organizational operations, organizational assets, or individuals	Serious adverse effect on organizational operations, organizational assets, or individuals	severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

DRAS - Asset Identification, Valuation and Categorization

- Weight of Asset, is determined by the sensitivity value of data in the container, since similar containers are not equally important to the organization, and the value of a container is determined by the data it holds, processes or transfers.

- The suggested “weight” or “weighting” helps to measure each asset’s value based on the data it holds/processes compared to other assets.

Weight	Rate	Description
Low	1	The value of data in the container is low/non-existent based on business objectives, as compared to another similar container’s data value
Medium	2	The value of data in the container is medium based on business objectives, as compared to another similar container’s data value
High	3	The value of data in the container is ight based on business objectives, as compared to another similar container’s data value

	Total Asset Value							
	Asset Value	3	4	5	6	7	8	9
Weight	1	3	4	5	6	7	8	9
	2	6	8	10	12	14	16	18
	3	9	12	15	18	21	24	27

Vulnerability and Threat Assessment

- When a vulnerability is exploited by a threat, it increases the likelihood of attack and leads to risk.

- The **severity of the threat and the vulnerability** is graded as very low (1), low (2), medium (3), high (4) and very high (5)

- To measure the overall value of the **severity of a vulnerability**, the combination of the value of **susceptibility** and **exposure** rating must first be decided.

- To measure the overall value of the **severity of a threat**, the combination of the value of **capability** and **impact** rating must first be decided.

DRAS - Vulnerability Rating Factors

Term	Explanation
Susceptibility	Simply measures the effort required to successfully exploit a given weakness. For example, fire is a threat. Poor fire prevention standards, poorly managed flammable liquids and poor circuit insulation are some of the weaknesses (vulnerabilities) or factors that help the fire threat to happen and cause damage.
Exposure	Is the potential exposure to loss, resulting from the occurrence of one or more threat events. It may be disseminated across other system components.

Susceptibility	Rating	Exposure
Minor Susceptibility: Vulnerability requires significant resources to exploit with little potential for loss.	1	**Minor Exposure**: Effects of the vulnerability are tightly contained and do not increase the probability of additional vulnerabilities being exploited.
Moderate Susceptibility: Vulnerability requires significant resources to exploit with significant potential for loss. Or, vulnerability requires little resources to exploit, moderate potential for loss.	2	**Moderate Exposure**: Vulnerability can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited.
High Susceptibility: Vulnerability requires few resources to exploit with significant potential for loss.	3	**High Exposure**: Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited.

Vulnerability Rating			
	Exposure Rating		
Susceptibility Rating	1	2	3
1	1	2	3
2	2	3	4
3	3	4	5

DRAS - Threat Rating Factors

Term	Explanation
Capability	Measures a threat agent's ability (including the level of effort required) to successfully attack an asset by exploiting its vulnerabilities, e.g., the threat agent's technical ability, knowledge and available material to exploit the vulnerability.
Impact	A forceful consequence or a strong effect of the launch of a threat on the business.

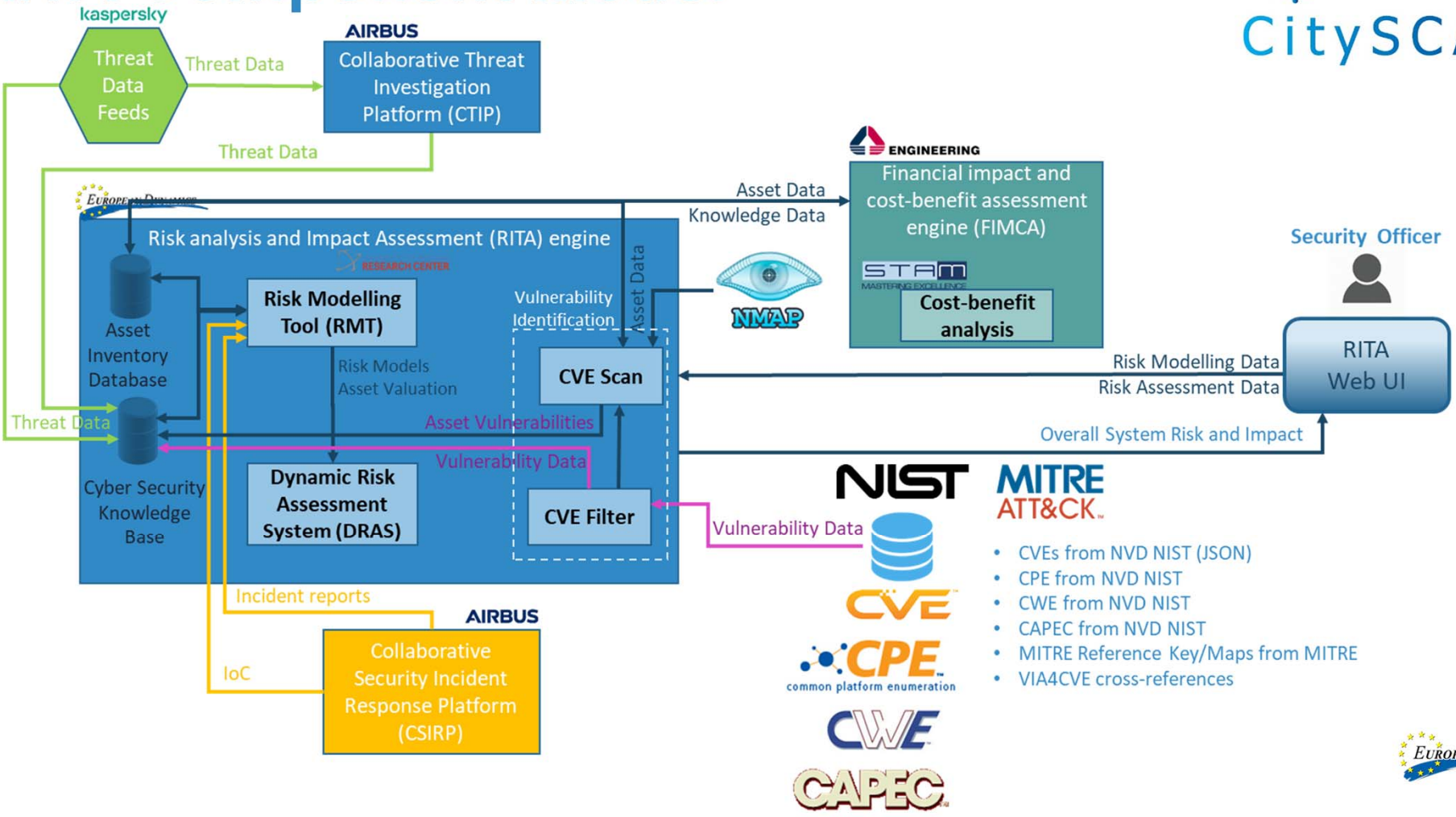
CAPABILITY	Rating	IMPACT
Little or no capacity such as knowledge, resource or technical skill to launch a threat on a given information asset of the organisation	1	Exercise of the threat may result in loss of some/few assets or resources; may have little effect on the organisation's business continuity, immaterial financial loss, low legal impact and low impact on business process.
Moderate capacity indicates the knowledge and skills to mount an attack, but some resources are lacking. Or, knowledge is lacking, but sufficient resources to mount an attack on a given information asset of the organisation does exist.	2	Exercise of the threat may result in loss of some assets or resources; may have a moderate effect on the organisation's business continuity, some material financial loss, perceptible legal impact and average business process impact.
High capacity indicates professional knowledge, skills and resources to mount an attack on a given information asset of the organisation.	3	Exercise of the vulnerability may result in the costly loss of major assets or resources; may significantly violate, harm, or impede on organisation's mission, reputation, or interest; or may result in serious injury or catastrophic impact.

Vulnerability and Threat Assessment

- The **severity of the threat and the vulnerability** is graded as very low (1), low (2), medium (3), high (4) and very high (5)

Rating	Grade	Description
1	Very low (VL)	Minor exposure, minor susceptibility
2	Low (L)	Minor exposure, moderate susceptibility; or moderate exposure, minor susceptibility
3	Medium (M)	High exposure, minor susceptibility; or minor exposure, high susceptibility; or moderate exposure, moderate susceptibility
4	High (H)	High exposure, moderate susceptibility; or moderate exposure, high susceptibility
5	Very High (VH)	High exposure, high susceptibility

RITA Component Model



Assets Inventory Database

- Need for sharing information about different assets which belong to the architecture.
- Information is loaded into the database (in CPE format) using a secure REST-API, which allows other components, and developers to make queries, create, update and delete entries about transport assets. The AIDB is a key component of the CitySCAPE architecture. It is used by several components, including:
  - ✓ **DRAS**, which needs to look up the AIDB to identify what asset groups belong to the scope of interest and thus individually calculate each asset group the risk value.
  - ✓ **RMT**, which needs information about available assets in order to define the system architecture, by grouping assets in asset groups, and assign the security and privacy objectives. This enables the creation of the transport topology and the risk model that is used by the DRAS component.
  - ✓ **FIMCA**, which needs information about asset values expressed in percentages based on company revenues, as well as the economic value of the asset (to support the cost-benefit analysis module)

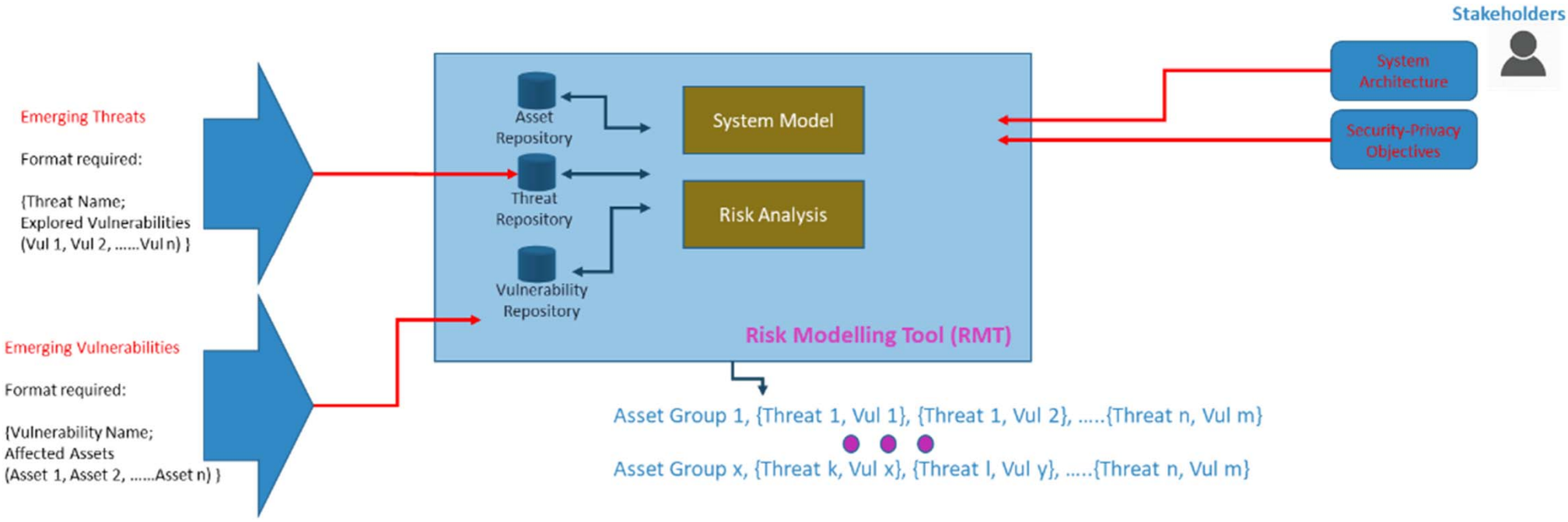
Cyber Security Knowledge Base

- Comprises of multiple repositories, (the Threat Repository, the Vulnerability Repository and the Countermeasure Repository) allowing security systems to access knowledge about past threats and incidents, including vulnerabilities, threats/attacks, implemented and available countermeasures and the relationship of the above.
- The **Threat Repository** will be populated by the Collaborative Threat Investigation Platform (CTIP), with threats (CTI) which are applicable to the CPaaS multimodal transport ecosystem.

Cyber Security Knowledge Base

- The **Vulnerability Repository** will be populated by the **CVE Filter** component of the **Vulnerability Identification**
  - ✓ Avoid doing direct and public lookups into the public CVE databases
  - ✓ Local lookups can be faster
- The **Countermeasure Repository** will be populated by the Risk Modelling Tool (RMT) and the Financial Impact and Cost-benefit Assessment engine (FIMCA)

Risk Modelling Tool



Risk Modelling Tool – Internal Processing

- **Valuate** (quantify) the importance, for the stakeholders of the system, for each asset group
  - ✓ Related to the security objectives that have been set, since it will be performed **SEPARATELY** for each security property (confidentiality, integrity, availably) that may be affected by an incident.

Asset Group 1; Confidentiality; Value
Asset Group 1; Integrity; Value
Asset Group 1; Availability; Value
Asset Group 2; Confidentiality; Value
Asset Group 2; Integrity; Value
Asset Group 2; Availability; Value
.....
Asset Group n; Confidentiality; Value
Asset Group n; Integrity; Value
Asset Group n; Availability; Value

Asset Group 1; Confidentiality; Threat x – Vulnerability y, Risk Value 1(Tx Vy)
Asset Group 1; Confidentiality; Threat z – Vulnerability w, Risk Value 2(Tz Vw)
.....
Continues with the calculation of the risk for all asset groups, per security requirement and all possible combinations of Threat – Vulnerability that can cause an incident that will harm the specific security requirement for the specific asset group.
.....

Dynamic Risk Assessment Tool

- DRAS is responsible for calculating the overall risk score, based on:
  - ✓ Asset valuation against the defined security and privacy objectives, as produced by the RMT component;
  - ✓ Asset individual risk value, calculated per security requirement and all possible combinations of Threat Likelihood – Vulnerability Level that can cause an incident that will affect the specific security requirement for the specific asset, as produced by the RMT component;

Any questions?

Thank you!

Alkiviadis Giannakoulias

Alkiviadis.Giannakoulias@eurodyn.com

Paraskevi Plagaki

paraskevi.plagaki@eurodyn.com

This project has received funding from the EU's Research and Innovation programme Horizon 2020 under grant agreement No 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.