IANUS TECHNOLOGIES LTD.

01
V002-13-03-2026

# SERVE

THE PROJECT NPD-CAPBLD/0225/0001 WAS FUNDED BY THE RESEARCH AND INNOVATION FOUNDATION, UNDER THE «ENTERPRISES CAPACITY BUILDING IN NEW PRODUCT DEVELOPMENT» PROGRAMME AND THROUGH THE RECOVERY AND RESILIENCE FACILITY OF THE NEXTGENERATIONEU INSTRUMENT.

Funded by the European Union
NextGenerationEU
Republic of Cyprus
RESEARCH & INNOVATION FOUNDATION

IANUS TECHNOLOGIES

## SOFTWARE HANDBOOK

# TABLE OF CONTENTS

# 01 INTRODUCTION

**SECTIONS:**

**1.1 PURPOSE OF THIS MANUAL**

**1.2 INTENDED AUDIENCE**

**1.3 SCOPE OF THE PLATFORM**

## 1.1 Purpose of this Manual

This manual provides practical guidance for using the SERVE platform to perform cyber-physical risk and vulnerability assessments. It introduces the platform's structure, explains its main components, and outlines the workflows required to configure assets, model threats, and analyze risk scenarios.

The document is intended to support users in understanding how the platform operates and how its different modules interact within the assessment process. It serves as a reference during system use and provides a structured overview of the key functionalities available within SERVE.

## 1.2 Intended Audience

This manual is designed for professionals involved in security analysis, infrastructure protection, and operational risk assessment. It is intended for users who interact with the SERVE platform as part of planning, evaluating, or monitoring cyber-physical security environments.

Typical users include:

- Security analysts and risk assessment specialists
- Critical infrastructure protection personnel
- Operational planners and decision support teams
- System administrators responsible for platform configuration

The manual assumes that users have a basic understanding of security risk concepts and operational environments.

## 1.3 Scope of the Platform

SERVE is designed to support the analysis and evaluation of risks affecting critical infrastructure and strategic assets. The platform integrates cyber and physical security perspectives to provide a comprehensive assessment environment.

Within the scope of this manual, the platform is presented in terms of its operational workflows, including asset definition, threat and risk modeling, simulation of scenarios, and analysis of generated results.

The document focuses on the functional use of the platform and does not cover internal system development or implementation details.

# 02 GENERAL OVERVIEW


**SECTIONS:**



## 2.1 What is SERVE

SERVE is a cyber-physical vulnerability assessment platform designed to support the identification and evaluation of risks affecting critical infrastructure and strategic assets. The platform combines cyber security analysis with physical security considerations in order to provide a unified environment for assessing complex threat scenarios.

Through the integration of multiple analytical components, SERVE enables users to model assets, define threat conditions, and evaluate potential impacts on operational systems. The platform assists analysts in understanding how vulnerabilities, threats, and infrastructure dependencies interact within a broader security context.

## 2.2 Key Capabilities

SERVE provides a set of analytical and operational tools that support structured risk assessment and decision support. These capabilities allow users to model infrastructure components, simulate threat scenarios, and interpret resulting risk levels.

Key capabilities include:

- Integrated cyber and physical security risk analysis
- Asset-based vulnerability assessment
- Scenario-driven threat modeling
- Analytical dashboards and visualization tools
- Structured reporting and export of assessment results

Together, these capabilities allow analysts to conduct systematic evaluations of security conditions across complex operational environments.

# 02 GENERAL OVERVIEW


**SECTIONS:**

**2.3 SYSTEM ARCHITECTURE OVERVIEW**

**2.4 TYPICAL USE CASES**

## 2.3 System Architecture Overview

The SERVE platform is organized into a set of functional modules that support different stages of the assessment process. These modules operate within a unified interface that allows users to move between asset definition, threat modeling, and analysis.

At a high level, the platform architecture includes:

- Asset management components, used to define and organize infrastructure elements
- Threat and risk modeling modules, used to configure vulnerability and threat parameters
- Analysis and reporting tools, used to visualize and communicate assessment results

This modular structure allows the platform to support flexible workflows depending on the type of analysis being conducted.

## 2.4 Typical Use Cases

SERVE can be applied in a variety of operational contexts where the protection and resilience of infrastructure systems are critical. The platform supports both planning and analytical activities by enabling users to evaluate vulnerabilities and potential threat impacts.

Typical application areas include:

- Assessment of critical infrastructure security
- Operational risk analysis for complex facilities
- Evaluation of cyber-physical threat scenarios
- Support for security planning and preparedness exercises

These use cases highlight the platform's role as a decision-support tool for organizations responsible for managing security risks in complex environments.

# 03
# GETTING STARTED

**SECTIONS:**



## 3.1 System Requirements

Before accessing the SERVE platform, users should ensure that their system environment meets the necessary technical requirements for proper operation. The platform is designed to operate within standard modern computing environments and is accessed through a web-based interface.

Minimum system requirements include:

- A modern web browser supporting current web standards
- Stable network connectivity to the platform server
- Appropriate user credentials and access permissions
- Sufficient display resolution to support the platform interface and visualization components

Ensuring that these requirements are met allows the platform interface, analysis tools, and visualization modules to function correctly.

## 3.2 Accessing the Platform

Access to the SERVE platform is performed through the system's designated web interface. Users must connect to the platform using the provided system address and authenticate with their assigned credentials.

Procedure

1. Open a supported web browser.
2. Navigate to the SERVE platform address.
3. Enter the assigned user credentials.
4. Submit the login request to access the platform environment.

Once authenticated, users are directed to the main platform workspace.

# 03
# GETTING STARTED

**SECTIONS:**

**3.3 USER AUTHENTICATION**

**3.4 INTERFACE OVERVIEW**

---

## 3.3 User Authentication

The authentication process ensures that access to the platform is restricted to authorized personnel. User roles and permissions determine the level of functionality available within the system.

Procedure

1. Enter the username and password provided by the system administrator.
2. Verify the login credentials.
3. Confirm successful access to the platform dashboard.

Depending on the assigned role, users may have access to specific modules such as asset configuration, risk modeling, or reporting.

## 3.4 Interface Overview

After successful authentication, users are presented with the main platform interface. The interface provides access to the different functional modules of the SERVE platform and supports navigation between assessment activities.

The interface includes the following elements:

- Navigation panel for accessing platform modules
- Workspace area where assessments and configurations are performed
- Visualization components used to display analysis results
- Control tools for creating, editing, and managing data entries

Understanding the basic layout of the interface helps users efficiently navigate the platform and locate the tools required for their assessment tasks.

# 04
# CORE PLATFORM WORKFLOW

SECTIONS:
4.1 THE ASSESSMENT PROCESS

## 4.1 THE ASSESSMENT PROCESS

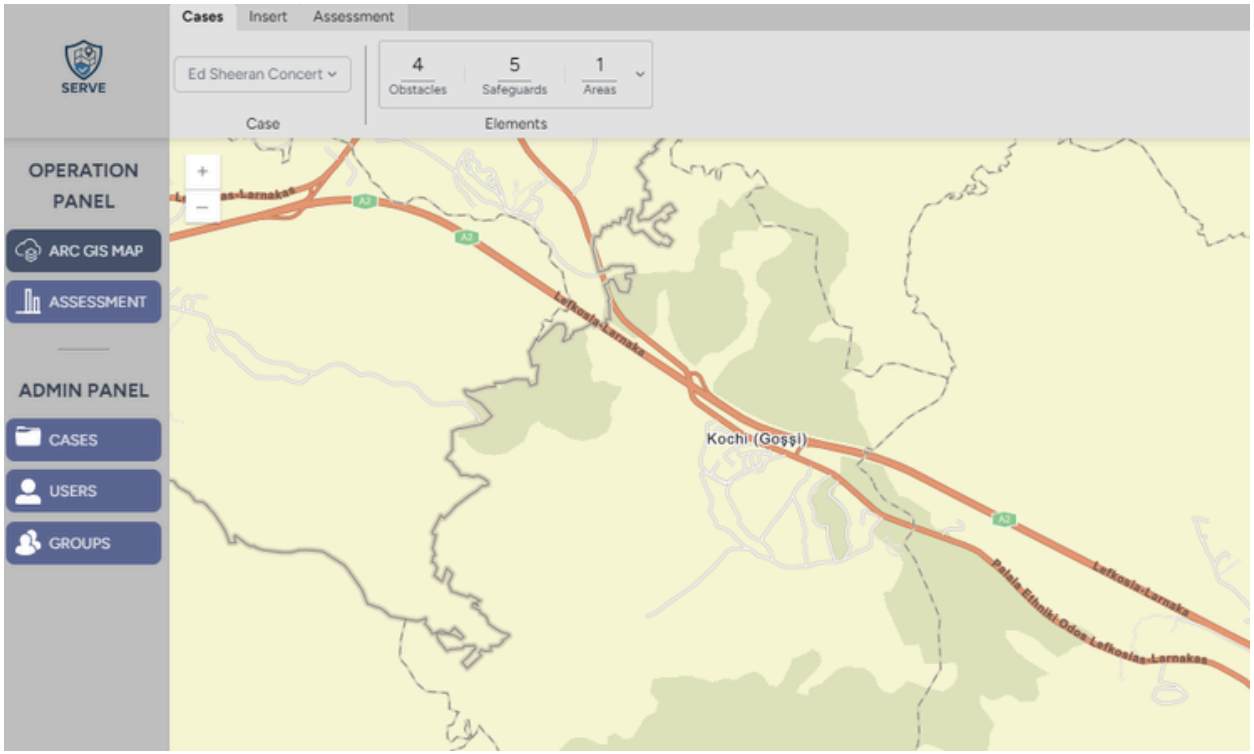
The SERVE platform supports a structured workflow for performing cyber-physical vulnerability assessments. This workflow guides users through the process of defining infrastructure assets, configuring risk parameters, modeling threat scenarios, and analyzing the resulting security impacts.

The assessment process is organized into a sequence of steps that reflect the logical progression of a risk evaluation. Each stage builds upon the previous one, allowing users to progressively refine the analysis and generate meaningful results.

A typical workflow in SERVE consists of:

1. Creating a new **case** environment
2. Modeling potential **threat** scenarios
3. Defining infrastructure assets (**areas**) and components
4. Configuring area **attractiveness**, **vulnerability** & **impact** parameters
5. Running analysis tools
6. Reviewing and exporting assessment results

Following this workflow ensures that the platform's analytical capabilities are used in a structured and consistent manner.



# 04
# CORE PLATFORM WORKFLOW

SECTIONS:
4.2 CREATING A NEW CASE

## 4.2 CREATING A NEW CASE

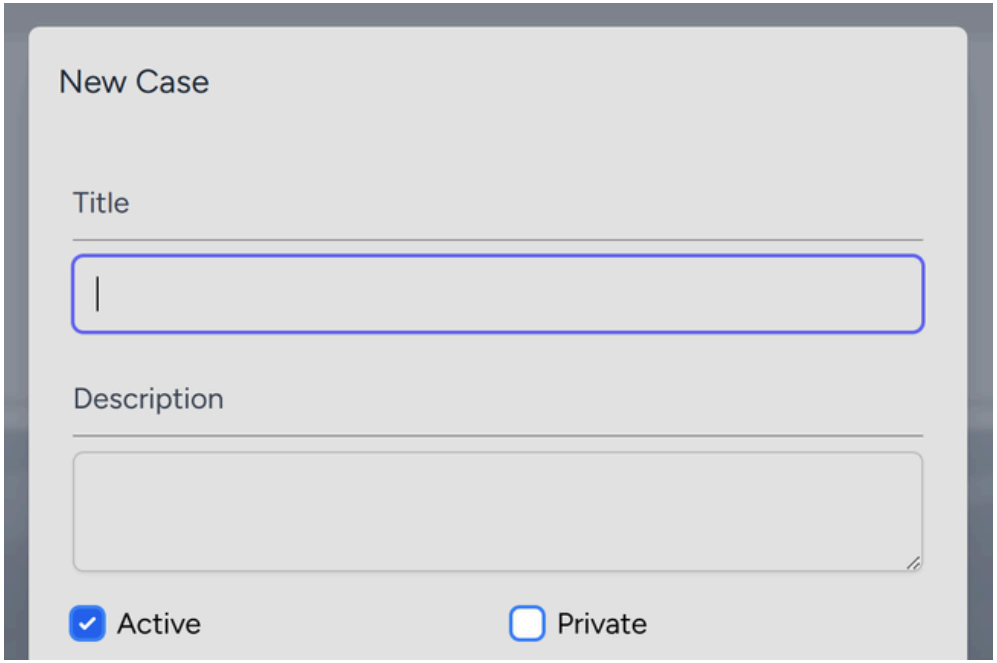
A **case** represents a working environment where users define threat conditions, configure infrastructure elements, and perform risk evaluations. Each case typically corresponds to a specific facility, system, or operational scenario being analyzed.

A case can be set to be “Private”, allowing access only to members of the selected **Organization**, ensuring sensitive info remain accessible to authorized Users.

Procedure

1. Navigate to the **Case** management module.
2. Select the option to create a new **Case**.
3. Enter the required information.
4. (Optional) Set case accessibility as “Private”.
5. Confirm creation.

Once created, the assessment becomes the central workspace where all related assets, scenarios, and analysis activities are configured.



# 04
# CORE PLATFORM WORKFLOW

SECTIONS:
4.3 CONFIGURING THREATS

## 4.3 CONFIGURING THREATS

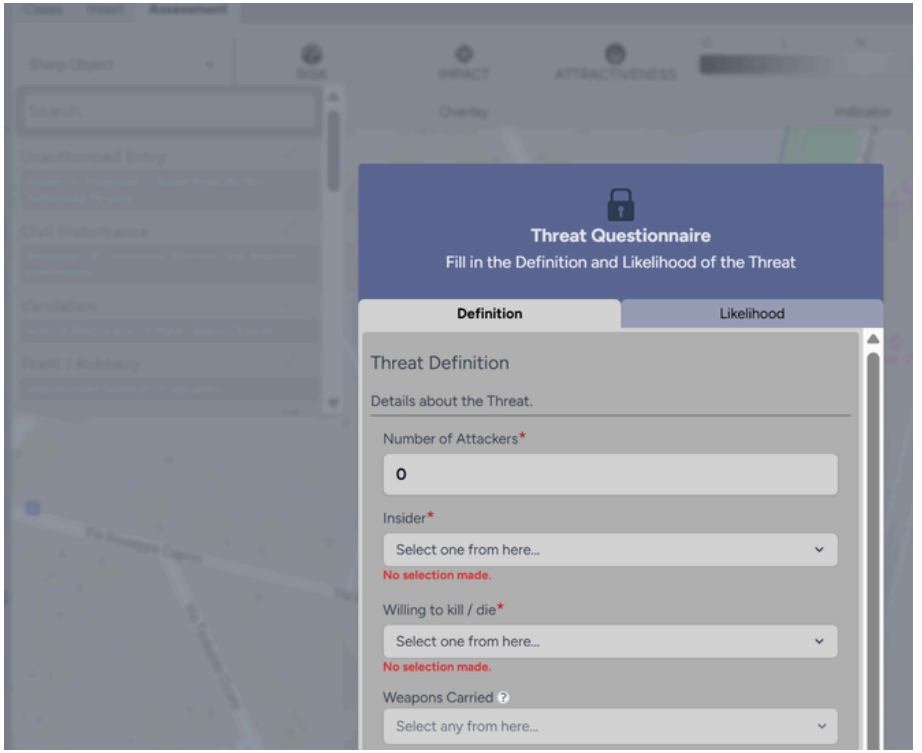
**Threat** profiles describe the definition and likelihood associated with each specific threat. These configurations determine how the platform evaluates area **Risk**.
Users configure threat parameters assuming a theoretical scenario of very low through very high danger.

Procedure

1. Access the map management module.
2. Navigate to the **Assessment** tab.
3. From the dropdown, select the specific **threat** to run the assessment on.
4. Define the relevant threat parameters.
5. Save the configured threat profile.

This configuration enables the platform to incorporate risk factors into subsequent analysis and simulation processes.

Note: it is possible to run the same asset risk assessments with multiple different threat scenarios, and compare results.



# 04
# CORE PLATFORM WORKFLOW

SECTIONS:
4.4 DEFINING ASSETS

## 4.4 DEFINING ASSETS

Assets represent the infrastructure components or systems that are being evaluated within the case. These may include facilities, technical systems, or operational resources that are relevant to the security analysis.
Defining assets allows the platform to organize the infrastructure elements that will be used in threat modeling and risk analysis.

Procedure

1. Access the map management module.
2. Navigate to the **Insert** tab.
3. Drag an asset from the available categories (Obstacles, Safeguards, Areas) onto the appropriate position on the map.
4. Provide any asset information and attributes where applicable.
5. Save the asset configuration.

Assets defined at this stage become available for use in subsequent modeling and simulation activities.

# 04
# CORE PLATFORM WORKFLOW

SECTIONS:
4.5 CONFIGURING AREA RISK PROFILES

## 4.5 CONFIGURING AREA RISK PROFILES

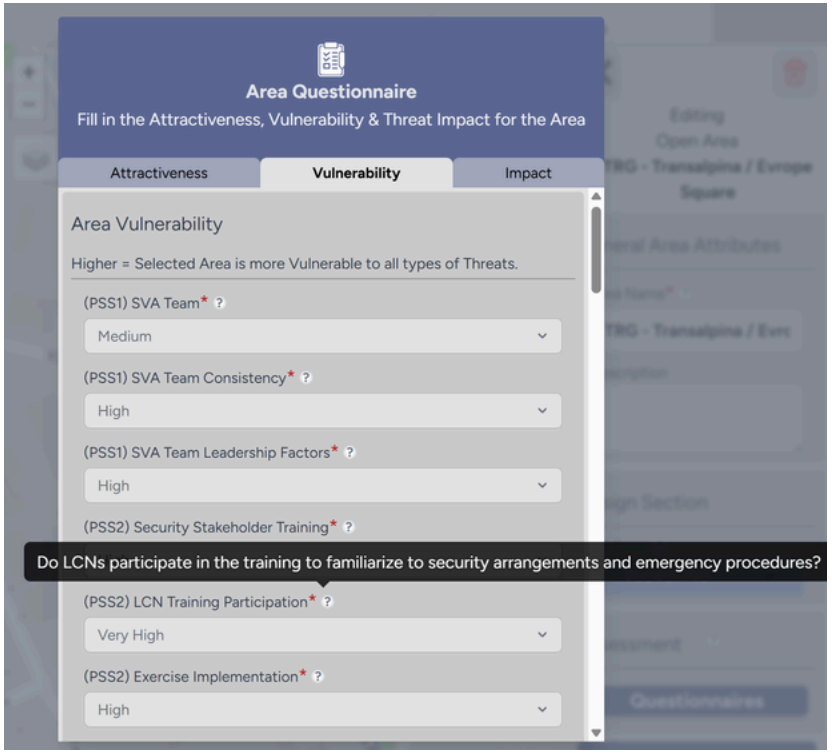
Risk profiles describe the vulnerability characteristics and security conditions associated with the defined assets. These configurations determine how the platform evaluates potential threats and their impact.
Users configure risk parameters according to the operational context of the infrastructure being assessed.

Procedure

1. Navigate to the map module.
2. Select the **area** component.
3. Define the relevant **attractiveness**, **vulnerability** and **impact** indicators.
4. Save the configured risk profile.

This configuration enables the platform to incorporate risk factors into subsequent analysis.

Note: the **impact** questionnaire is threat-specific, since different threat types would have different impact to an area.



# 04
# CORE PLATFORM WORKFLOW

SECTIONS:
4.6 REVIEWING ASSESSMENT RESULTS

## 4.6 REVIEWING ASSESSMENT RESULTS

After each questionnaire is completed, the platform generates analytical outputs that summarize the evaluated risks and potential impacts on the assessed areas.
Users can review these results through dashboards, visualizations, and generated reports.

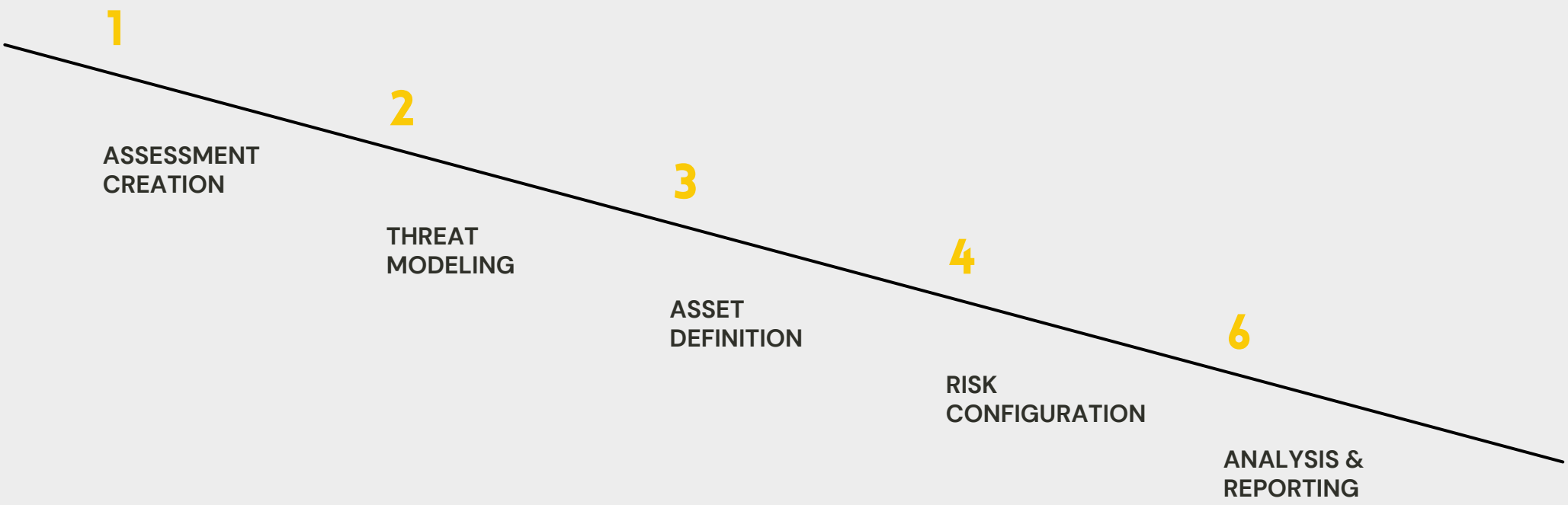
Procedure

1. Open the assessment module.
2. (Optional) Select other **cases** and or **threats** to compare outputs with.
3. Review the generated risk indicators and visual outputs.
4. Export the results if required.

These outputs support decision-making and provide insights into vulnerabilities and potential mitigation priorities.

Note: the assessment outputs are split in 3 categories, Case, Threat and Area assessments.
Category Case Assessment shows the best-case and worst-case scenario of the selected threat types occuring in ANY area of the case (and compared cases & threats).
Category Threat Assessment shows the assessment values of the threat (and compared threats).
Category Area Assessments holds the values for each assessed area of the case (and compared cases & threats)

# 04
# CORE PLATFORM WORKFLOW (OVERVIEW)



# 05
# ASSET MANAGEMENT

**SECTIONS:**



## 5.1 Overview of Asset Management

Asset management in the SERVE platform refers to the process of defining, organizing, and maintaining the infrastructure components that are included in an assessment. Assets represent the systems, facilities, or resources whose security posture is being evaluated within the platform.

By creating structured asset entries, users establish the foundation for threat modeling, and vulnerability assessment. Each asset can include descriptive information and configuration parameters that are later used by the platform's analytical modules.

Effective asset management ensures that infrastructure elements are consistently represented and properly linked to risk and assessment models.

## 5.2 Creating Assets

Creating assets is the first step in building the infrastructure model within an assessment. Each asset entry represents a specific component or system that may be subject to cyber or physical threats.

Procedure

1. Open the map module.
2. Navigate to the **Insert** tab.
3. **Drag** the desired asset onto the appropriate place on the map.
4. Define the asset spacial geometry and/or relevant data.
5. Confirm and save the entry.

Once created, the asset becomes available for configuration.

Note: risk assessments apply to only **area** asset types.

# 05
# ASSET MANAGEMENT

**SECTIONS:**

**5.3 EDITING ASSET INFORMATION**

**5.4 ORGANIZING AND MANAGING ASSETS**

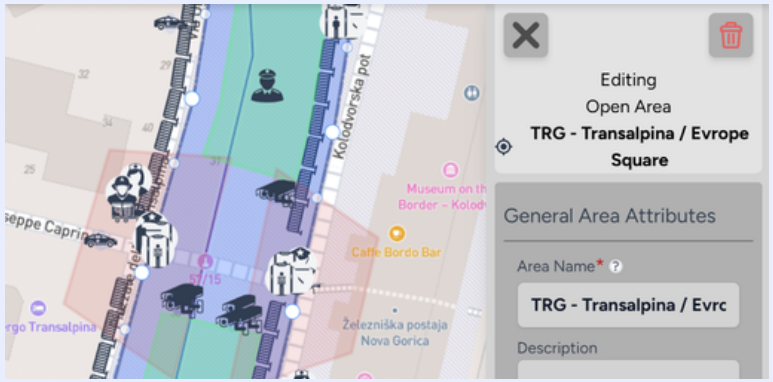
## 5.3 Editing Asset Information

During the assessment process, it may be necessary to update asset information in order to reflect new data, corrected parameters, or changes in infrastructure conditions.

Procedure

1. Locate the asset on the map.
2. Enter the asset edit mode to open its configuration window.
3. Modify the required information or parameters.
4. Save the updated configuration.

Maintaining accurate asset data improves the reliability of the platform's analytical results.

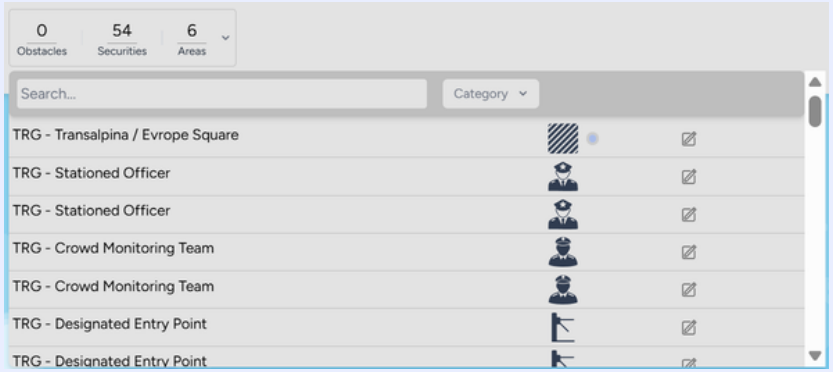



## 5.4 Organizing and Managing Assets

As the number of assets within an assessment grows, organizing them becomes important for maintaining clarity and efficient navigation. The platform provides mechanisms for structuring and managing asset entries.

Typical management actions may include:

- Grouping assets according to infrastructure categories
- Filtering or searching asset lists
- Reviewing asset attributes and relationships
- Maintaining consistent naming and classification



# 05
# ASSET MANAGEMENT

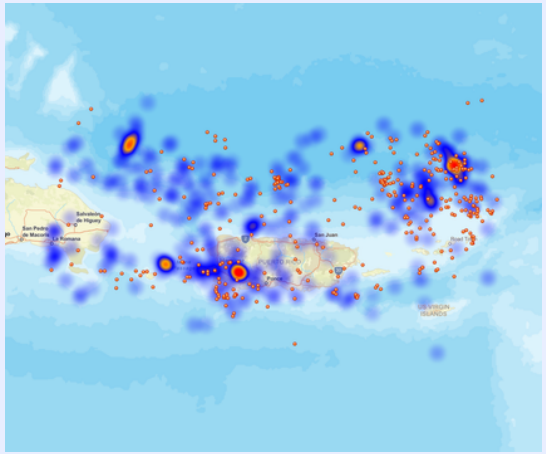
**SECTIONS:**

**5.5 GEOGRAPHIC DATA INTEGRATION (ARCGIS MAP)**

**5.6 MANAGING MAP LAYERS (ARCGIS MAP)**

---

## 5.5 Geographic Data Integration (ArcGIS Map)

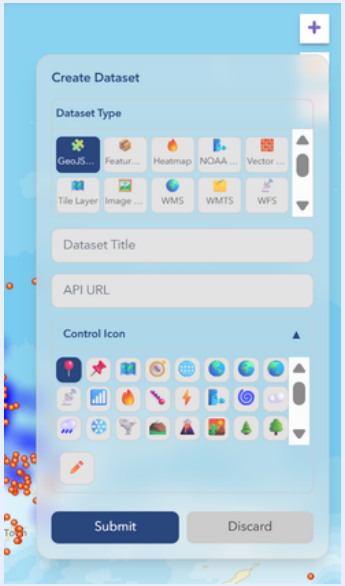


The geographic data displayed within the map environment provides contextual information that may assist analysts during the assessment process. By visualizing infrastructure assets alongside relevant spatial datasets, users can better understand environmental conditions and spatial relationships that may influence security considerations.

At the current stage, external geographic layers are used primarily for visualization and contextual reference within the assessment workspace. The integration of such data into automated risk calculations or analytical models may be considered in future developments of the platform.

## 5.6 Managing Map Layers (ArcGIS Map)

Imported datasets are displayed as individual layers that can be controlled directly within the map interface. Users can enable or disable layers in order to focus on specific geographic information during the assessment process.




Procedure

1. Open the map layer control panel.
2. Locate the desired data layer in the layer list.
3. Enable or disable the layer visibility as required.
4. Adjust the viewing configuration to focus on relevant information.

This functionality allows users to explore different spatial datasets without modifying the underlying assessment data.

# 06
# THREAT AND RISK MODELING

SECTIONS:

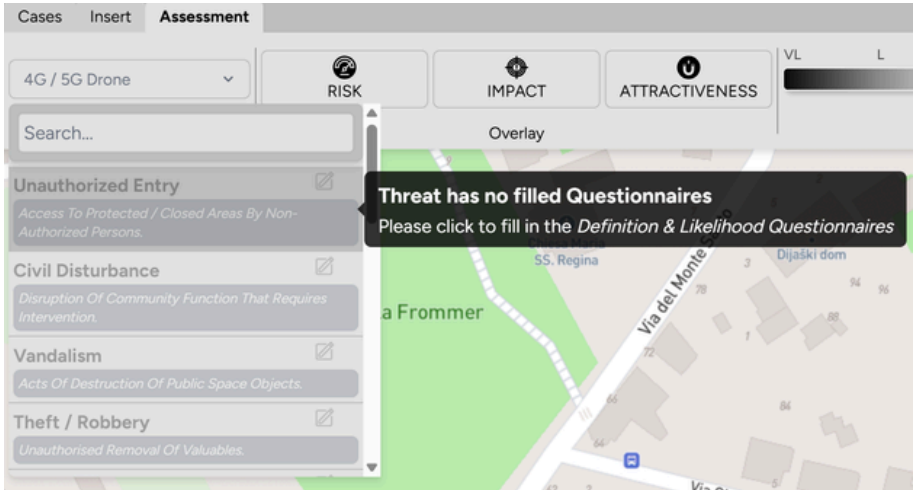
6.1 OVERVIEW OF THREAT MODELING

## 6.1 OVERVIEW OF THREAT AND RISK MODELING

Threat modeling within the SERVE platform enables users to evaluate potential vulnerabilities affecting defined infrastructure assets. This process involves identifying possible threat sources, defining relevant risk **parameters**, and assessing how these threats could impact the assets under evaluation.

By **combining** asset information with configured threat conditions, the platform generates analytical insights that help users understand the likelihood and potential consequences of security incidents. This modeling process forms the basis for subsequent analysis.

The objective of this stage is to establish a structured representation of potential security risks, making the assessment more accurate.



# 06
# THREAT AND RISK MODELING

SECTIONS:
6.2 DEFINING THREATS

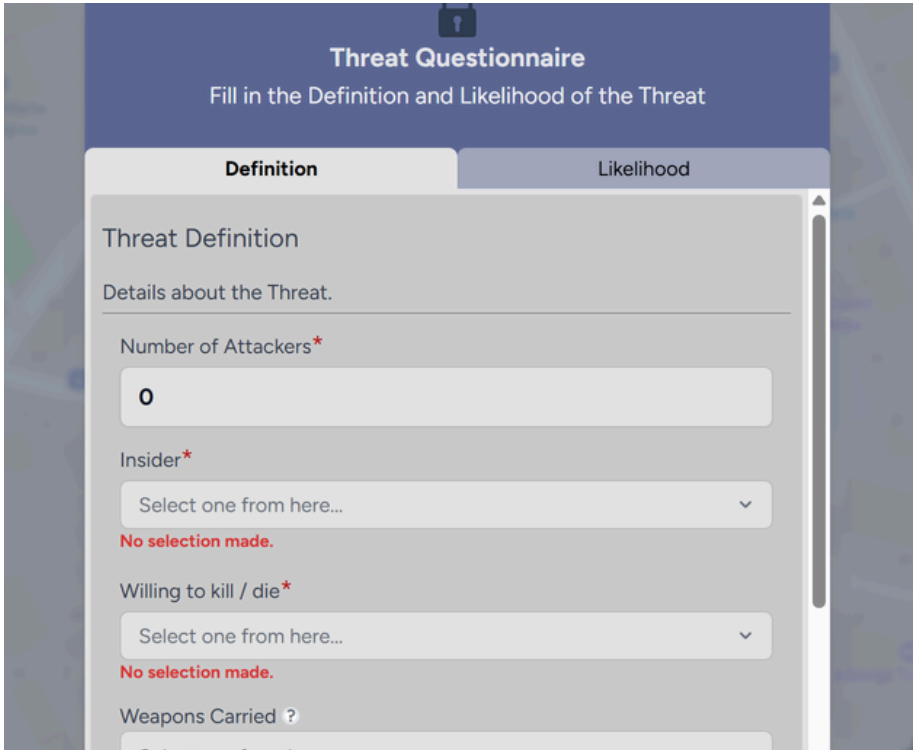
## 6.2 DEFINING THREATS

Threat describe potential events or attack conditions that may affect the infrastructure assets defined in the assessment. These threats represent possible security incidents that can be analyzed through the platform's modeling and simulation tools.
Each threat includes parameters that describe the conditions under which the event may occur.

Procedure

1. Open to the map module.
2. Navigate to the **Assessment** tab.
3. From the drop down, select a threat type.
4. Define the relevant characteristics and conditions.
5. Save the configured threat.

Once defined, the overall case assessment can begin. The selected threat now applies to all areas defined for assessment.



# 07
# ANALYSIS AND VISUALIZATION

SECTIONS:

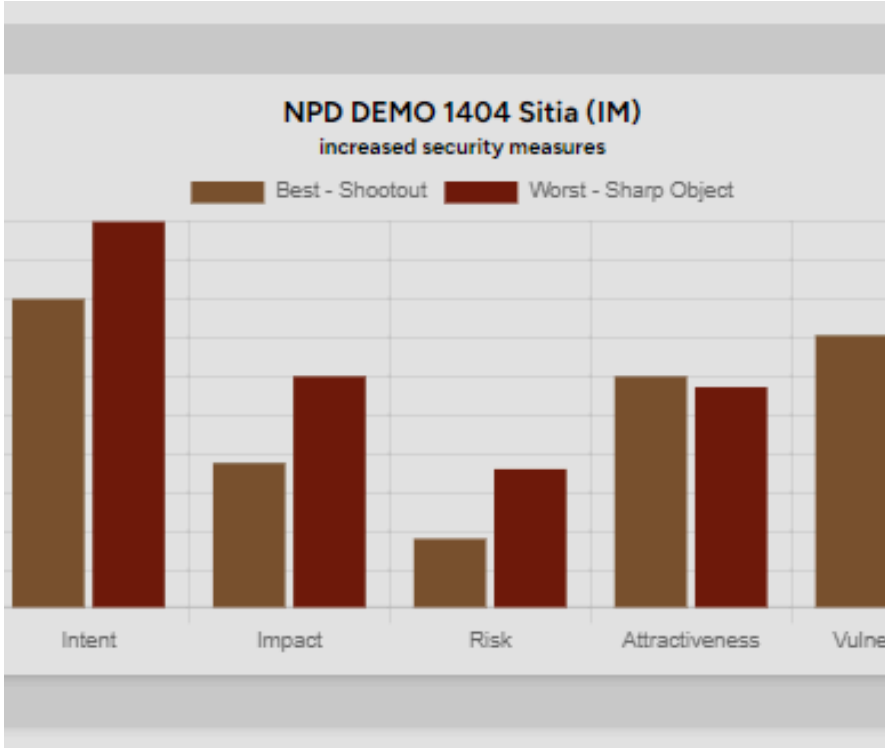
7.1 OVERVIEW OF ANALYSIS TOOLS

## 7.1 OVERVIEW OF ANALYSIS TOOLS

The SERVE platform provides analytical tools that allow users to interpret the results produced during threat modeling and simulation activities. These tools transform raw assessment outputs into structured indicators and visual representations that support decision-making.

Through the analysis environment, users can examine risk levels, identify vulnerable assets, and evaluate the potential impact of defined threat scenarios. The analysis tools help users understand how different risk factors interact and how vulnerabilities propagate across the infrastructure model.

The goal of this stage is to convert analytical results into clear and actionable insights.



# 07
# ANALYSIS AND VISUALIZATION

SECTIONS:

7.2 DASHBOARD OVERVIEW

## 7.2 DASHBOARD OVERVIEW

The platform dashboard provides a centralized view of assessment results and key indicators. It presents summarized information about configured assets, evaluated threats, and calculated risk levels.

The dashboard allows users to quickly review the current state of an assessment and identify areas requiring further analysis. Information is typically presented using visual elements such as charts, indicators, and structured summaries.

Dashboard components include:

- Overview of assessed assets
- **Risk**, **Impact** & **Attractiveness** level indicators
- Visualization panels displaying analytical results

This overview enables users to quickly monitor the overall security posture of the analyzed environment.

# 07
# ANALYSIS AND VISUALIZATION

SECTIONS:

7.3 INTERPRETING ASSESSMENT INDICATORS

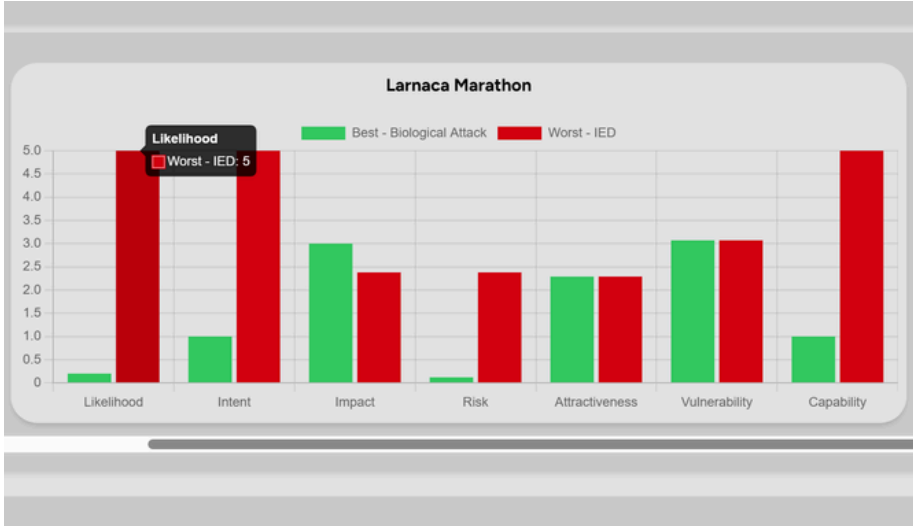
## 7.3 INTERPRETING ASSESSMENT INDICATORS

Assessment indicators represent the analytical outputs generated by the platform's modeling and simulation processes. These indicators provide a structured representation of the potential severity and impact of identified threats.
Users can analyze these indicators to identify critical vulnerabilities, evaluate the relative importance of different risks, and prioritize mitigation efforts.

Procedure

1. Open the **Assessment** module.
2. Review the displayed indicators and associated metrics.
3. (Optional) Expand **Threat** & **Areas** categories for more data.
4. (Optional) Compare with other Threats & Cases.
5. Identify assets or scenarios that present elevated risk levels.

Understanding these indicators allows users to interpret the analytical results produced by the platform.



# 07
# ANALYSIS AND VISUALIZATION

SECTIONS:

7.4 VISUALIZATION TOOLS

## 7.4 VISUALIZATION TOOLS

Visualization tools within the platform help users explore analytical results in a graphical format. These tools present assessment outputs in a way that highlights relationships between assets, threats, and risk conditions.

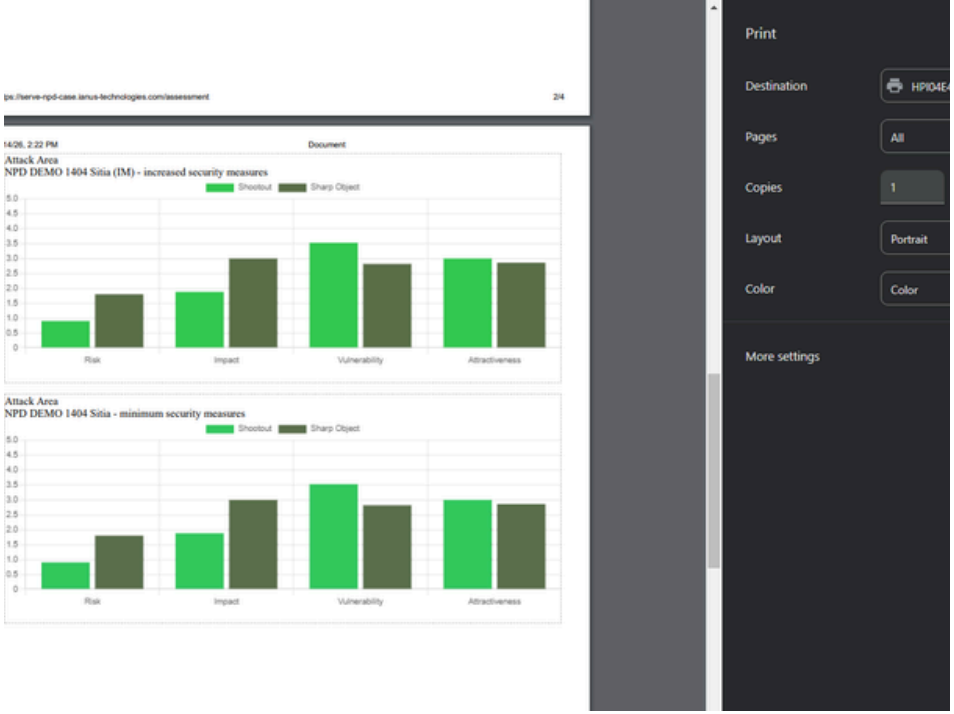
Visual representations can make complex analytical results easier to understand and communicate, particularly when dealing with large infrastructure models or multiple threat scenarios.

Visualization tools include:

- Graphical representations of asset relationships
- Charts displaying risk distributions
- Interactive exploration of assessment data

These visualizations assist users in examining patterns, identifying vulnerabilities, and communicating findings to decision-makers.

# 08
# REPORTING AND DATA EXPORT




**SECTIONS:**



## 8.1 Overview of Reporting Tools

The SERVE platform includes reporting and data export capabilities that allow users to document and share the results of their assessments.

Reports can summarize risk levels, asset vulnerabilities, and threat scenarios, making them suitable for decision-making, audits, or communication with stakeholders.

Reporting tools transform complex analytical outputs into structured documents or visual summaries that can be interpreted without requiring direct interaction with the platform.

## 8.2 Generating Reports

Users can generate reports directly from completed assessments or simulation results.

Reports include:

- Asset summaries and classifications
- Assessment indicators and scores
- Graphical visualizations

Procedure

1. Navigate to the reporting module.
2. Select the assessment or scenario for which a report is required.
3. Choose the desired report format and content options.
4. Generate the report.
5. Review and save the report for distribution.

## 8.3 Customizing Report Content

The platform allows users to tailor the contents of generated reports according to the audience or purpose. Users can select which assets, scenarios, or analytical results to include, as well as adjust the type of graphs to export.

Procedure

1. Open the **Assessment** module.
2. (Optional) Select compared Cases & Threats.
3. Adjust visualization options as needed.
4. Press the PDF button (top-right).

Customizing reports ensures that stakeholders receive information in a clear and relevant format.

# FROM PLATFORM TO DECISION-MAKING

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| ASSESSMENT & SIMULATION | ANALYSIS & VISUALIZATION | REPORT GENERATION | DATA EXPORT | DECISION / ACTION |

IANUS
TECHNOLOGIES

# THANK YOU FOR EXPLORING **SERVE**


## CONTACT US

Spyrou Kyprianou 85 | Larnaca 6051 | Cyprus
ianus-technologies.com
secretary@ianus-technologies.com

IANUS
TECHNOLOGIES

THE PROJECT NPD-CAPBLD/0225/0001 WAS FUNDED BY THE RESEARCH AND INNOVATION FOUNDATION, UNDER THE «ENTERPRISES CAPACITY BUILDING IN NEW PRODUCT DEVELOPMENT» PROGRAMME AND THROUGH THE RECOVERY AND RESILIENCE FACILITY OF THE NEXTGENERATIONEU INSTRUMENT.