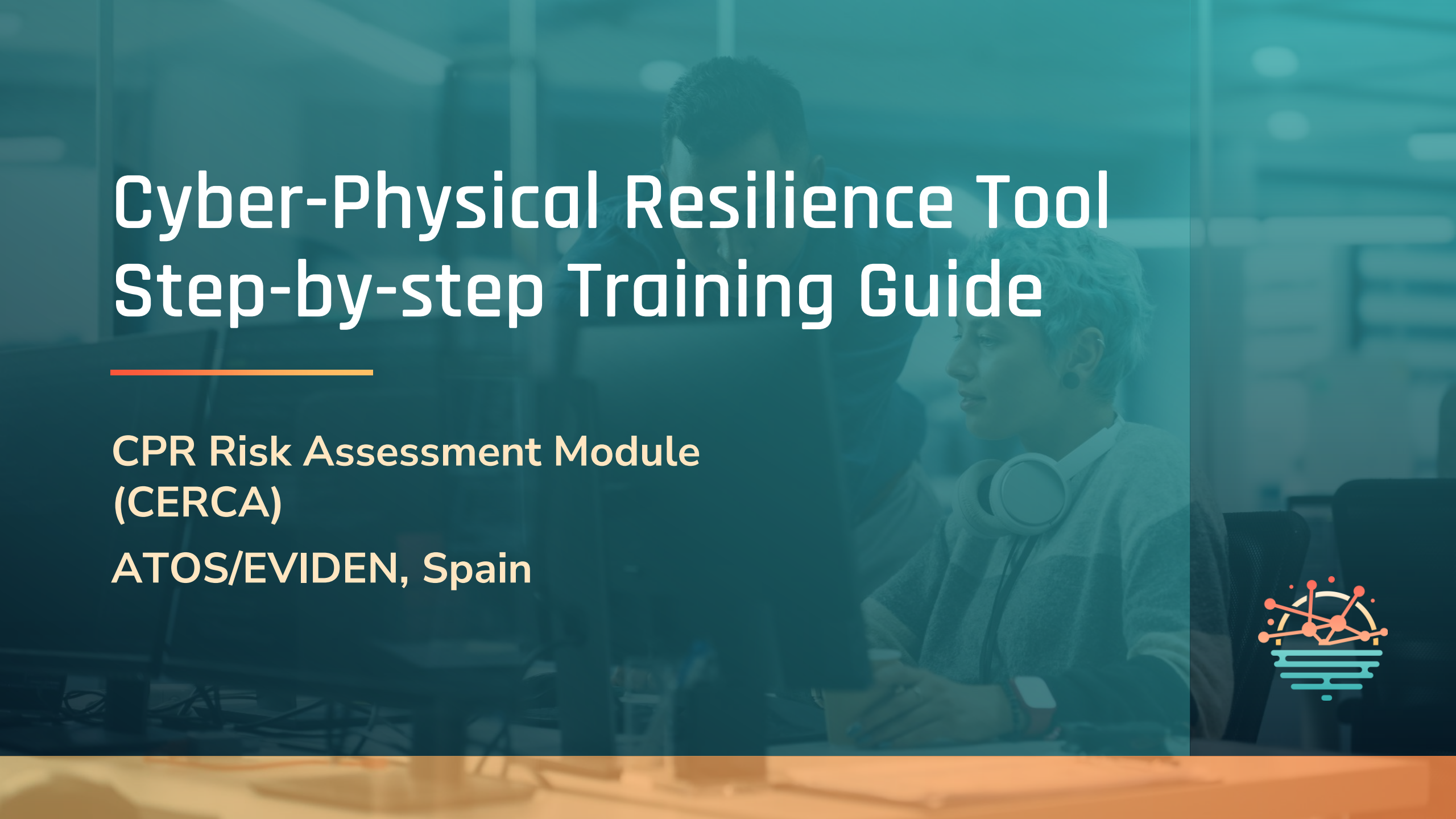
Cyber-Physical Resilience Tool Step-by-step Training Guide

CPR Risk Assessment Module (CERCA)

ATOS/EVIDEN, Spain



Overview of the Cyber-Physical Resilience Tool

- **CPR (Cyber-Physical Resilience) Tool** is developed under the SUNRISE project to enhance the cybersecurity posture of critical infrastructure (CI), particularly during complex events like pandemics. It aims to support security teams in managing digital threats that may arise alongside other challenges such as staff shortages or operational disruptions.

- **CPR integrates multiple modules** to provide a holistic view of cyber threats. These include an anomaly detection system validated with real CI logs, a risk assessment module that incorporates temporary conditions and physical activity alarms, and a threat intelligence scoring component enhanced with source confidence evaluation.

- **The tool aligns with known frameworks** such as MITRE ATT&CK for mapping Indicators of Compromise (IoCs), helping security analysts understand attack patterns more efficiently. It also includes features that support NIS 2 Directive compliance through its structured incident reporting module.

- **The CPR dashboard** enables users to access risk reports, simulate mitigation strategies, and evaluate the effectiveness of cyber defense mechanisms in real-time. It is designed for ease of use, allowing operators to visualize and respond to threats across cyber and physical domains quickly and effectively.

- **CPR is especially valuable for operators of essential services**, offering capabilities that strengthen incident awareness, improve response times, and support decision-making during both normal operations and crisis scenarios.

Content Overview

SUNRISE

This step-by-step training guide provides an overview of the **CPR Risk Assessment Module (CERCA)**, part of the SUNRISE Cyber-Physical Resilience Tool. It is designed to help users understand and navigate the key features. It forms part of the training materials provided for the solution, alongside the training video.

01 Accessing the Dashboard

02 Completing Questionnaires

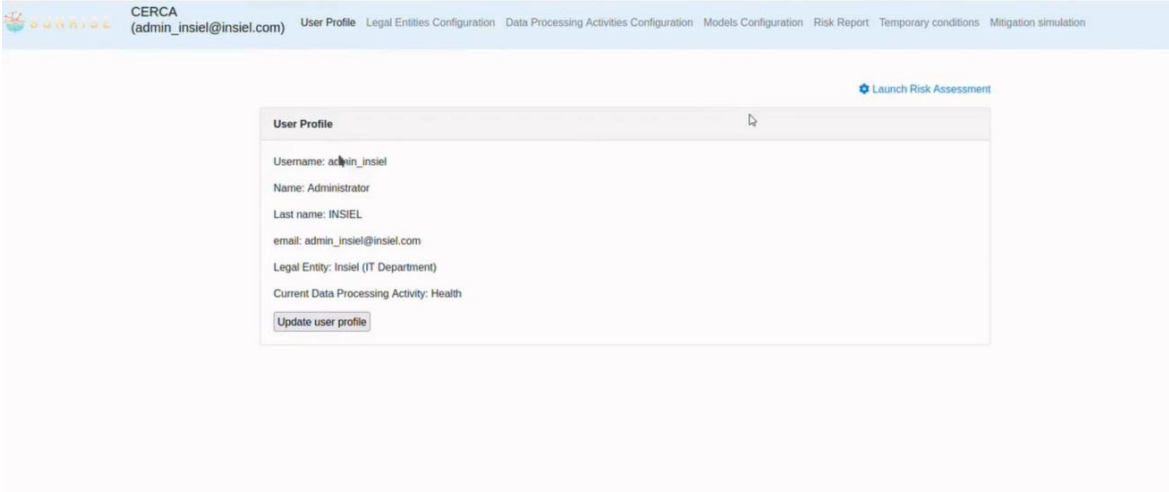
03 Configuring Data Processing & Assets

04 Reviewing Risk Models & Conditions

05 Understanding Risk Reports

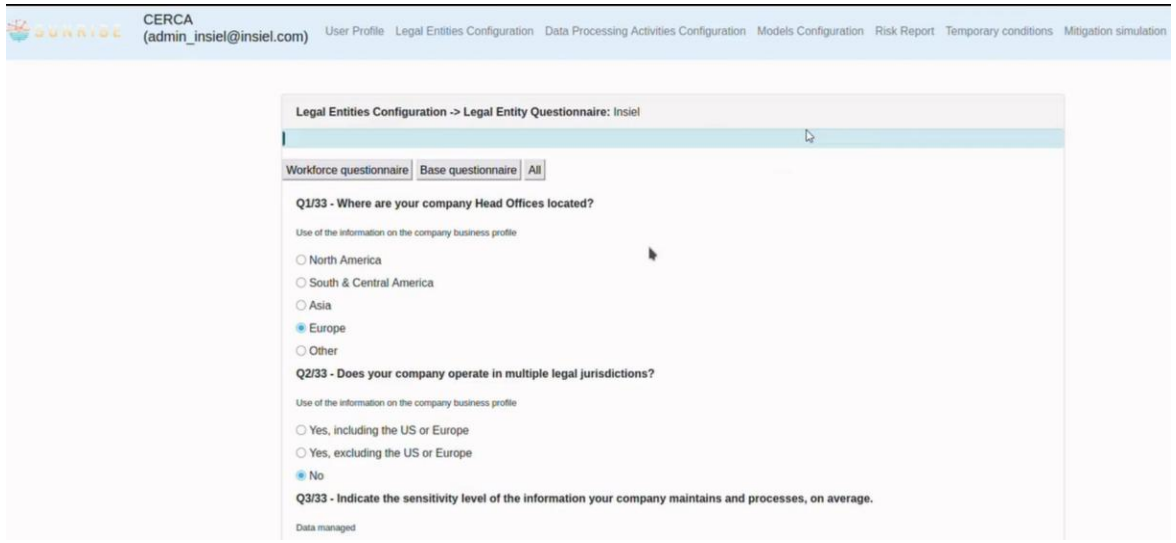
06 Running Mitigation Simulations

Accessing the Dashboard



- Log in to the Risk Assessment module (CERCA) via the CPR Tool.
- From the dashboard, you can:
- Edit your user and legal entity profiles.
- Access the organisational and workforce questionnaires.
- View mapped indicators used in risk calculations.

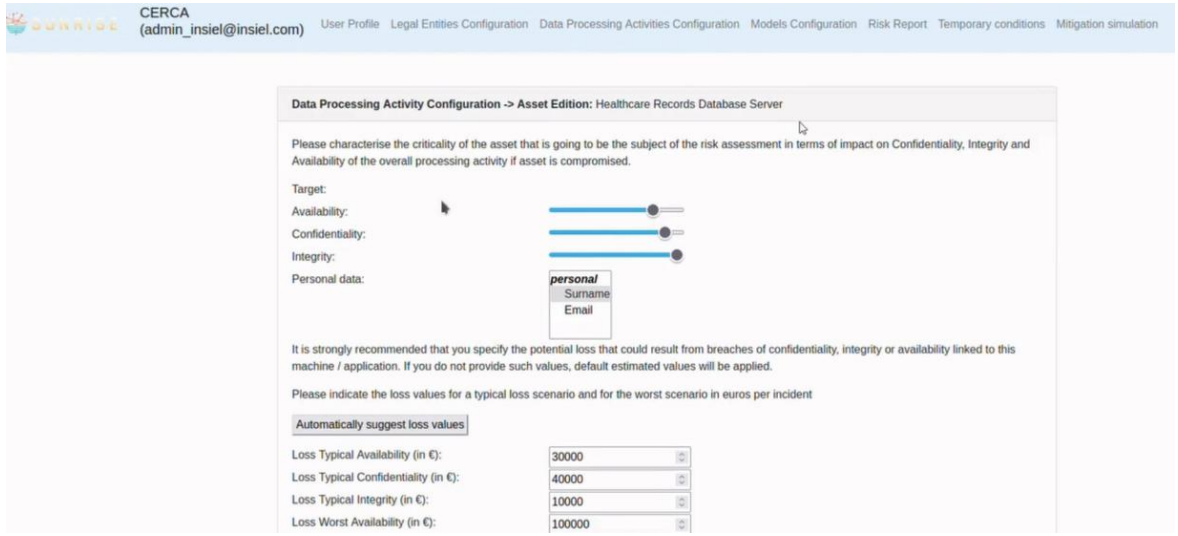
Completing Questionnaires



SUNRISE

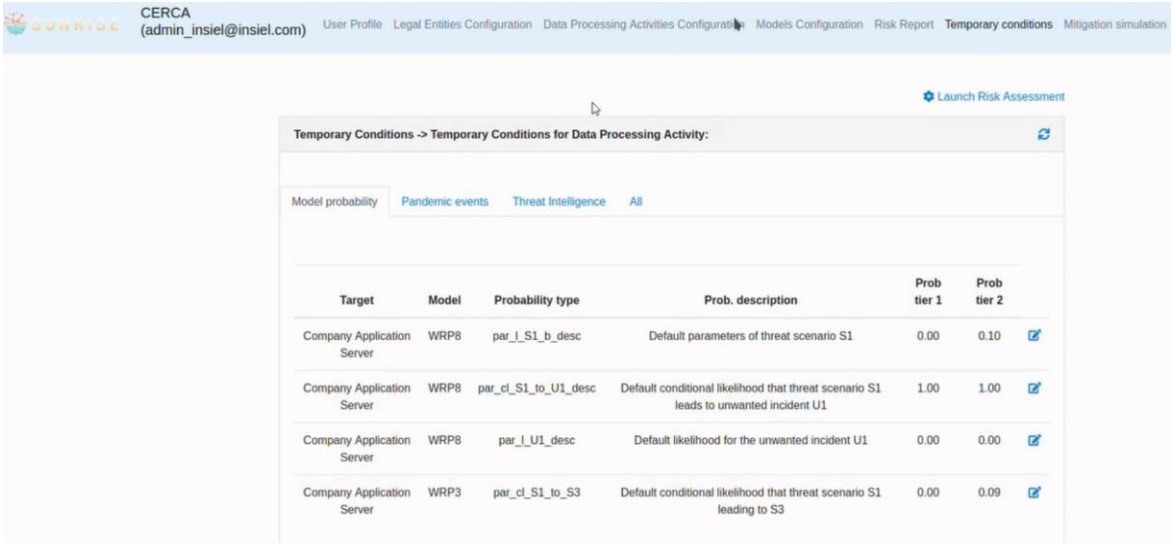
- Complete the **Organisational Questionnaire** with company
- Fill in the **Workforce Questionnaire.** Each response links to indicators reflecting temporary conditions such as staffing levels or operational capacity.

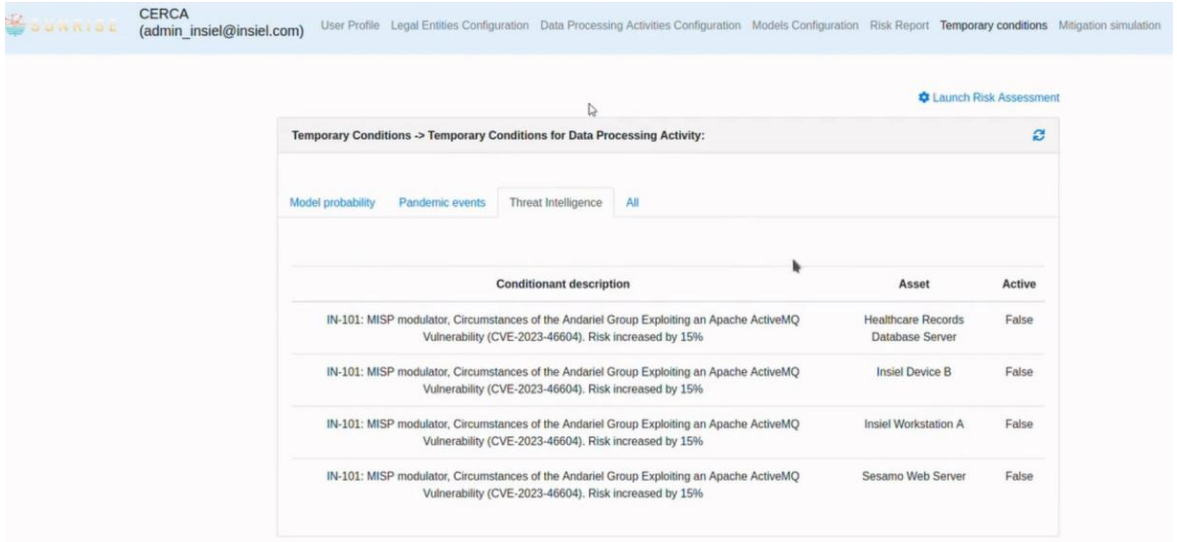
Configuring Data Processing & Assets



- Define **Data Processing Activities** (e.g. “Health”) and list involved digital assets.
- For each asset, set:
- **CIA levels** (Confidentiality, Integrity, Availability)
- **Loss estimates** (typical and worst-case, in euros)
- Select applicable risk models (e.g. SQL Injection) to generate an initial risk report.

Reviewing Risk Models & Conditions

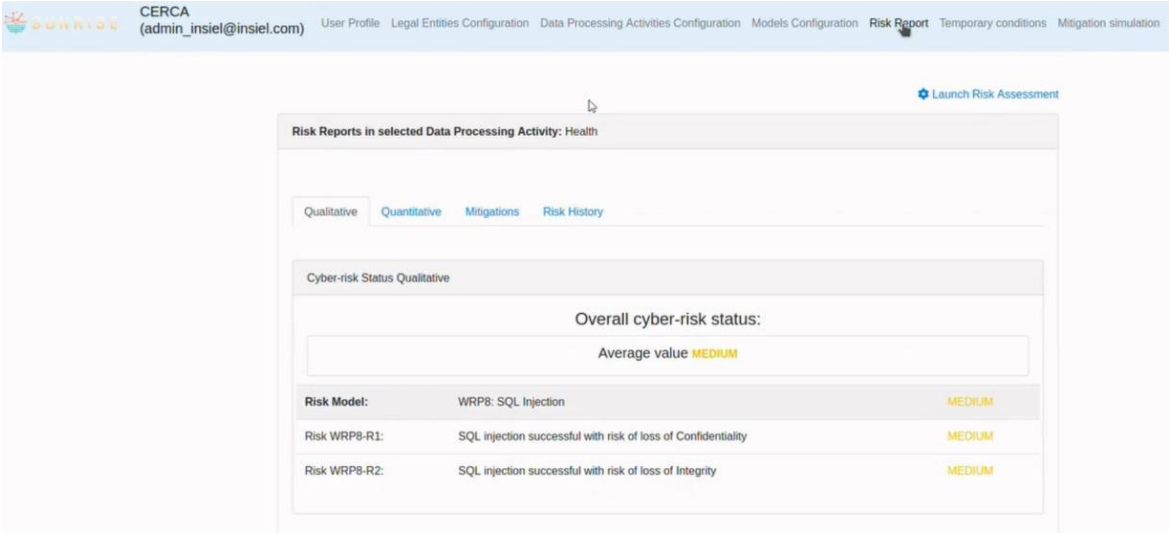


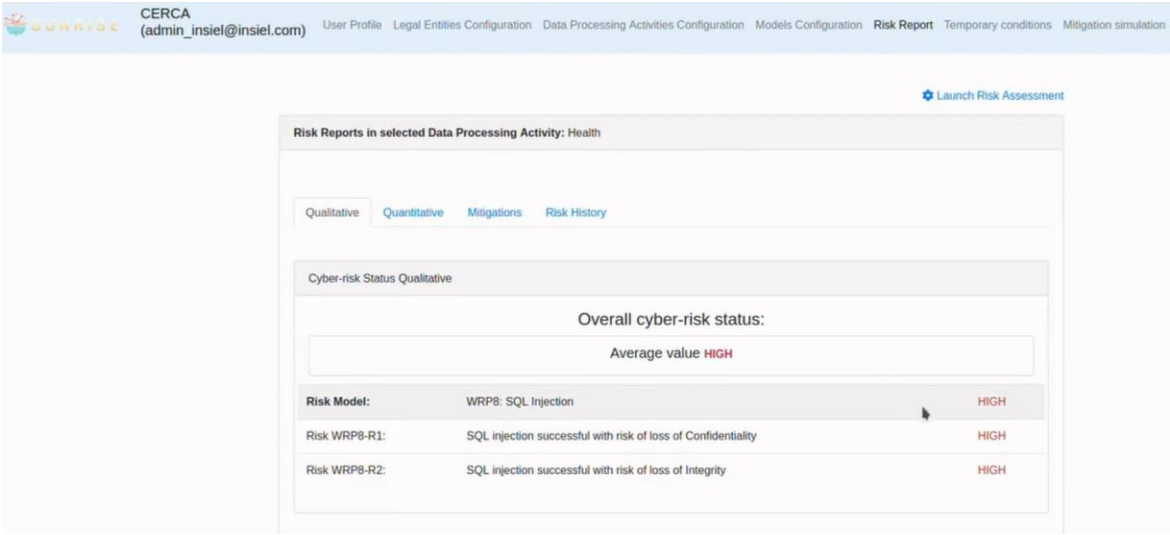


SUNRISE

- Explore visual **attack models** (e.g. CORAS diagrams) showing attack paths and potential impacts.
- Set or adjust **conditional probabilities** (likelihood of attack success), including confidence ranges.
- External threat intelligence (e.g. MISP events) may raise these probabilities (e.g. +15% for a known exploit).

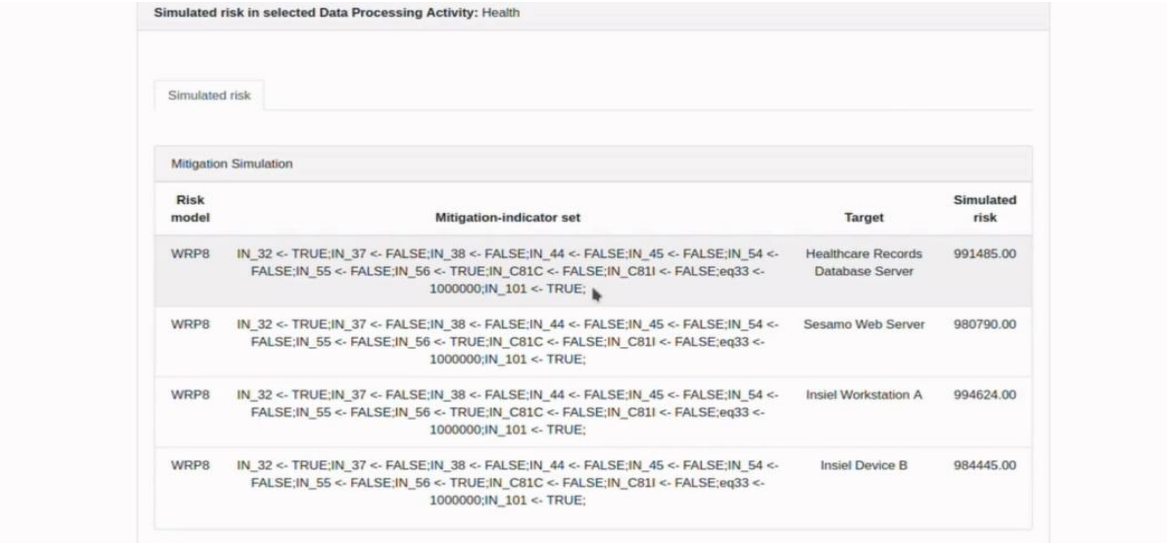
Understanding Risk Reports





- View **initial risk reports**, which show:
- Overall risk level (e.g. Medium or High)
- Breakdown by asset and by risk model
- Estimated financial impact (typical vs. worst case)
- When new alerts arrive (e.g. from Wazuh), CERCA automatically updates indicator values and generates new reports reflecting the latest status.

Running Mitigation Simulations



Simulated risk in selected Data Processing Activity: Health

Simulated risk

Mitigation Simulation

Risk model	Mitigation-indicator set	Target	Simulated risk
WRP8	IN_32 <- TRUE;IN_37 <- FALSE;IN_38 <- FALSE;IN_44 <- FALSE;IN_45 <- FALSE;IN_54 <- FALSE;IN_55 <- FALSE;IN_56 <- TRUE;IN_C81C <- FALSE;IN_C81I <- FALSE;eq33 <- 1000000;IN_101 <- TRUE;	Healthcare Records Database Server	991485.00
WRP8	IN_32 <- TRUE;IN_37 <- FALSE;IN_38 <- FALSE;IN_44 <- FALSE;IN_45 <- FALSE;IN_54 <- FALSE;IN_55 <- FALSE;IN_56 <- TRUE;IN_C81C <- FALSE;IN_C81I <- FALSE;eq33 <- 1000000;IN_101 <- TRUE;	Sesamo Web Server	980790.00
WRP8	IN_32 <- TRUE;IN_37 <- FALSE;IN_38 <- FALSE;IN_44 <- FALSE;IN_45 <- FALSE;IN_54 <- FALSE;IN_55 <- FALSE;IN_56 <- TRUE;IN_C81C <- FALSE;IN_C81I <- FALSE;eq33 <- 1000000;IN_101 <- TRUE;	Insiel Workstation A	994624.00
WRP8	IN_32 <- TRUE;IN_37 <- FALSE;IN_38 <- FALSE;IN_44 <- FALSE;IN_45 <- FALSE;IN_54 <- FALSE;IN_55 <- FALSE;IN_56 <- TRUE;IN_C81C <- FALSE;IN_C81I <- FALSE;eq33 <- 1000000;IN_101 <- TRUE;	Insiel Device B	984445.00

SUNRISE

- Use the **Mitigation Simulation** module to apply and test actions that reduce risk.
- Simulations adjust specific indicators to show how mitigations affect the risk level.
- Helps prioritise which actions most effectively reduce exposure.

SUNRISE

Thank you for following the training.

For more information:
https://sunrise-europe.eu/

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101073821