

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

04

Reviewing Risk
Models &
Conditions

02

Completing
Questionnaires

05

Understanding
Risk Reports

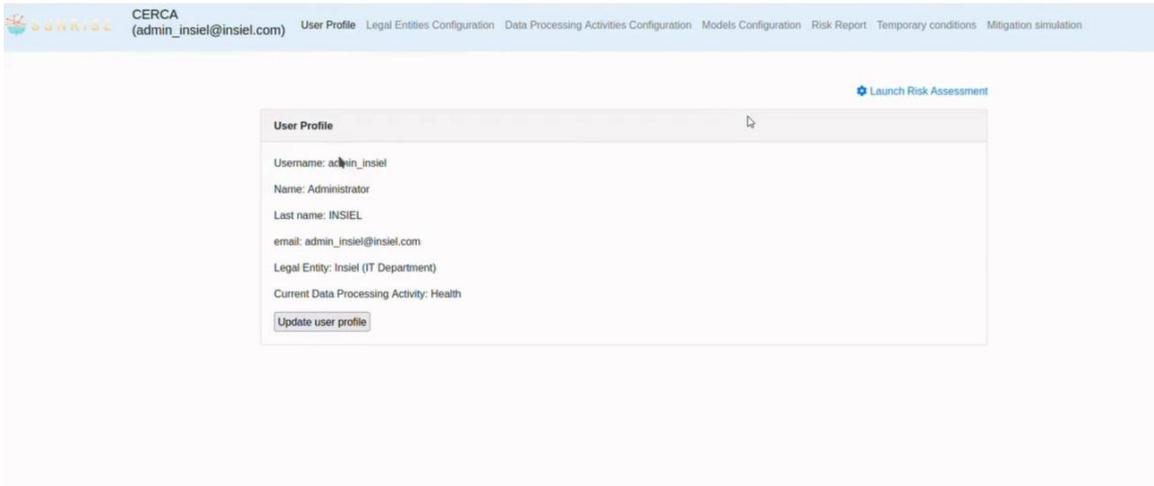
03

Configuring Data
Processing &
Assets

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.

The screenshot shows the SUNRISE web application interface. At the top, the user is identified as CERCA (admin_insiet@insiet.com) with navigation links for User Profile, Legal Entities Configuration, Data Processing Activities Configuration, Models Configuration, Risk Report, Temporary conditions, and Mitigation simulation. The main content area is titled 'Legal Entities Configuration -> Legal Entity Questionnaire: Insiet'. It features three tabs: 'Workforce questionnaire', 'Base questionnaire', and 'All'. The 'Workforce questionnaire' tab is active, displaying two questions. The first question, 'Q1/33 - Where are your company Head Offices located?', has radio button options for North America, South & Central America, Asia, Europe (selected), and Other. The second question, 'Q2/33 - Does your company operate in multiple legal jurisdictions?', has radio button options for Yes, including the US or Europe; Yes, excluding the US or Europe; and No (selected). A third question, 'Q3/33 - Indicate the sensitivity level of the information your company maintains and processes, on average.', is partially visible at the bottom. A 'Data managed' link is located at the bottom left of the questionnaire area.

Configuring Data Processing & Assets



SUNRISE

- + 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.

The screenshot shows the 'Data Processing Activity Configuration -> Asset Edition: Healthcare Records Database Server' interface. It includes a navigation bar with 'CERCA (admin_insiel@insiel.com)' and various menu items. The main content area contains instructions to characterize the asset's criticality and CIA levels. It features three sliders for Availability, Confidentiality, and Integrity. A 'Personal data' section lists 'personal', 'Surname', and 'Email'. Below, there are instructions on loss values and a table with dropdown menus for 'Loss Typical Availability (in €): 30000', 'Loss Typical Confidentiality (in €): 40000', 'Loss Typical Integrity (in €): 10000', and 'Loss Worst Availability (in €): 100000'.

Reviewing Risk Models & Conditions



SUNRISE

CERCA (admin_insiel@insiel.com) User Profile Legal Entities Configuration Data Processing Activities Configuration Models Configuration Risk Report Temporary conditions Mitigation simulation

Launch Risk Assessment

Temporary Conditions -> Temporary Conditions for Data Processing Activity:

Model probability Pandemic events Threat Intelligence All

Target	Model	Probability type	Prob. description	Prob tier 1	Prob tier 2
Company Application Server	WRP8	par_l_S1_b_desc	Default parameters of threat scenario S1	0.00	0.10
Company Application Server	WRP8	par_cl_S1_to_U1_desc	Default conditional likelihood that threat scenario S1 leads to unwanted incident U1	1.00	1.00
Company Application Server	WRP8	par_l_U1_desc	Default likelihood for the unwanted incident U1	0.00	0.00
Company Application Server	WRP3	par_cl_S1_to_S3	Default conditional likelihood that threat scenario S1 leading to S3	0.00	0.09

- + 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).

CERCA (admin_insiel@insiel.com) User Profile Legal Entities Configuration Data Processing Activities Configuration Models Configuration Risk Report Temporary conditions Mitigation simulation

Launch Risk Assessment

Temporary Conditions -> Temporary Conditions for Data Processing Activity:

Model probability Pandemic events Threat Intelligence All

Conditionant description	Asset	Active
IN-101: MISP modulator, Circumstances of the Andariel Group Exploiting an Apache ActiveMQ Vulnerability (CVE-2023-46604). Risk increased by 15%	Healthcare Records Database Server	False
IN-101: MISP modulator, Circumstances of the Andariel Group Exploiting an Apache ActiveMQ Vulnerability (CVE-2023-46604). Risk increased by 15%	Insiel Device B	False
IN-101: MISP modulator, Circumstances of the Andariel Group Exploiting an Apache ActiveMQ Vulnerability (CVE-2023-46604). Risk increased by 15%	Insiel Workstation A	False
IN-101: MISP modulator, Circumstances of the Andariel Group Exploiting an Apache ActiveMQ Vulnerability (CVE-2023-46604). Risk increased by 15%	Sesamo Web Server	False

Understanding Risk Reports

CERCA (admin_insiel@insiel.com) User Profile Legal Entities Configuration Data Processing Activities Configuration Models Configuration Risk Report Temporary conditions Mitigation simulation

Launch Risk Assessment

Risk Reports in selected Data Processing Activity: Health

Qualitative Quantitative Mitigations Risk History

Cyber-risk Status Qualitative

Overall cyber-risk status:

Average value MEDIUM

Risk Model:	WRP8: SQL Injection	MEDIUM
Risk WRP8-R1:	SQL injection successful with risk of loss of Confidentiality	MEDIUM
Risk WRP8-R2:	SQL injection successful with risk of loss of Integrity	MEDIUM

CERCA (admin_insiel@insiel.com) User Profile Legal Entities Configuration Data Processing Activities Configuration Models Configuration Risk Report Temporary conditions Mitigation simulation

Launch Risk Assessment

Risk Reports in selected Data Processing Activity: Health

Qualitative Quantitative Mitigations Risk History

Cyber-risk Status Qualitative

Overall cyber-risk status:

Average value HIGH

Risk Model:	WRP8: SQL Injection	HIGH
Risk WRP8-R1:	SQL injection successful with risk of loss of Confidentiality	HIGH
Risk WRP8-R2:	SQL injection successful with risk of loss of Integrity	HIGH

- + 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



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.

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;	Sesame 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;	Insief 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;	Insief Device B	984445.00



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

The material presented and views expressed here are the responsibility of the author(s) only.
The EU Commission takes no responsibility for any use made of the information set out.