

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

CPR Dashboard Overview

ATOS/EVIDEN, Spain

XLAB, Slovenia



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 Dashboard**, 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

Dashboard
Overview

04

Threat Intelligence
TINTED

02

Risk Assessment
CERCA

05

Anomaly Detection
LOMOS

03

Incident Reporting
AIRE

06

System
Integration

Dashboard Overview



SUNRISE

- + The CPR Dashboard presents a summary of key cybersecurity activity:
 - › Latest anomalies from LOMOS
 - › Recent alerts from WAZUH
 - › Most recent risk assessment (CERCA)
 - › Incoming threat intelligence (IoCs)
 - › Ongoing incident reports
- + You can also access each module directly from the dashboard interface.


Risk Assessment – CERCA Module

Threat	High level threat	Threat details
Denial of service	Nefarious Activity/ Abuse	Distributed Denial of network service (DDoS) (network layer attack i.e. Protocol exploitation / Malformed packets / Flooding / Spoofing), of application service (DDoS) (application layer attack i.e. Ping of Death / XDoS / WinNuke / HTTP Floods) or both
Malicious code/ software/ activity	Nefarious Activity/ Abuse	Abuse of resources (incl. Cryptojacking); Search Engine Poisoning; Exploitation of fake trust of social media; Worms/ Trojans; Rootkits; Mobile malware; etc
Brute force	Nefarious	Attempt to gain access to an asset protected by a finite secret value by using trial-and-error to exhaustively



- › Define the organisation and configure it as a **legal entity**
- › Complete both the main and workforce **questionnaires**
- › Create **data processing activities** and link relevant assets
- › Set **criticality levels** for each asset (CIA: Confidentiality, Integrity, Availability)
- › Input or auto-generate **financial loss values** per asset
- › Select and apply appropriate **risk models** (e.g. SQL injection, session fixation)
- › View **results** in the Risk Report, showing both qualitative and quantitative risk
- › Check **Risk History** for past assessments
- › Review **suggested mitigations** for each model

Incident Reporting – AIRE Module

Incident Reports registered in the Incident Reporting Smart Engine: 

Summary Ready ManagerialJudgement Ready DataConversion Ready Green-lightReporting Ready Reporting Reported All

Incident	Type	Status	Phase	IR Workflow	Registration Date
Insiel_001_Test	Cyber Security Incident	In progress	M1	DataConversion	April 30, 2025, 9:04 a.m.
Test3	Cyber Security Incident	In progress	M1	DataConversion	May 5, 2025, 8:37 a.m.
LOMOS_alarm	Cyber Security Incident	In progress	M1	DataCollection	Nov. 5, 2024, 3:47 p.m.
INSIEL_EventDemo_1	Cyber Security Incident	In progress	M1	DataConversion	Nov. 6, 2024, 8:25 a.m.
Event001	Cyber Security Incident	In progress	M1	DataConversion	July 15, 2024, 6:52 a.m.

- + AIRE helps track and report security incidents, following regulatory requirements.
- + **Steps:**
- + Access reports from the “**Reports**” tab
- + Open cases using the **TheHive** interface
- + View **incident data** in “Incidents Additional Info”
- + **Configure** impacted essential services and personal data breach details
- + Add affected processes under “**Impacted Processes**”
- + **Monitor incident** workflows and tasks

Threat Intelligence – TINTED Tool



OSINT - GreyNoise Observes Active Exploitation of Cisco Vulnerabilities

Tied to Salt Typhoon Attacks

Event ID: 1454
UUID: 18c55588-626c-4e78-8840-456014d195c
Creator org: CIRCL
Protected Event (experimental): Event is in unprotected mode.
Tags: type:OSINT, osint:lifetime="perpetual", osint:certainty="50", tip:white, tip:clear, related-to: misp-galaxy-threat-actor="UNC3236", created-by: misp-galaxy-producer="GreyNoise", TINTED:Source-Score=68.97, admiralty-scale:source-reliability="b", TIE-trending=0.00, TIE-timeliness=0.00, TIE-completeness=0.80, TIE:Threat-Score="Low"
Date: 2025-03-06
Threat Level: Medium
Analysis: Completed
Distribution: All communities
Published: No (last published at 2025-05-09 10:41:35)
#Attributes: 58 (5 Objects)
First recorded change: 2025-03-06 10:36:15
Last change: 2025-05-09 10:41:39
Modification map
Sightings: 0 (0) - restricted to own organisation only

Related Events

Order by date

2. Active exploitation of Cisco IOS XE Software Web Management Use
2023-10-23
OSINT - Cisco IOS CVE-2018-0171 attack
2018-04-07

—Pivots — Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports —Attributes —Discussion

- + TINTED enriches threat intelligence and aligns technical data to known attack methods.
- + Access the MISP dashboard via the CPR interface
- + View MISP events enriched with:
 - › Threat scoring
 - › Source confidence
 - › Admiralty scale ratings
 - › MITRE ATT&CK mapping (“galaxies”)
- + Explore all received IoCs under “Threat Intelligence Monitoring”

Anomaly Detection - LOMOS

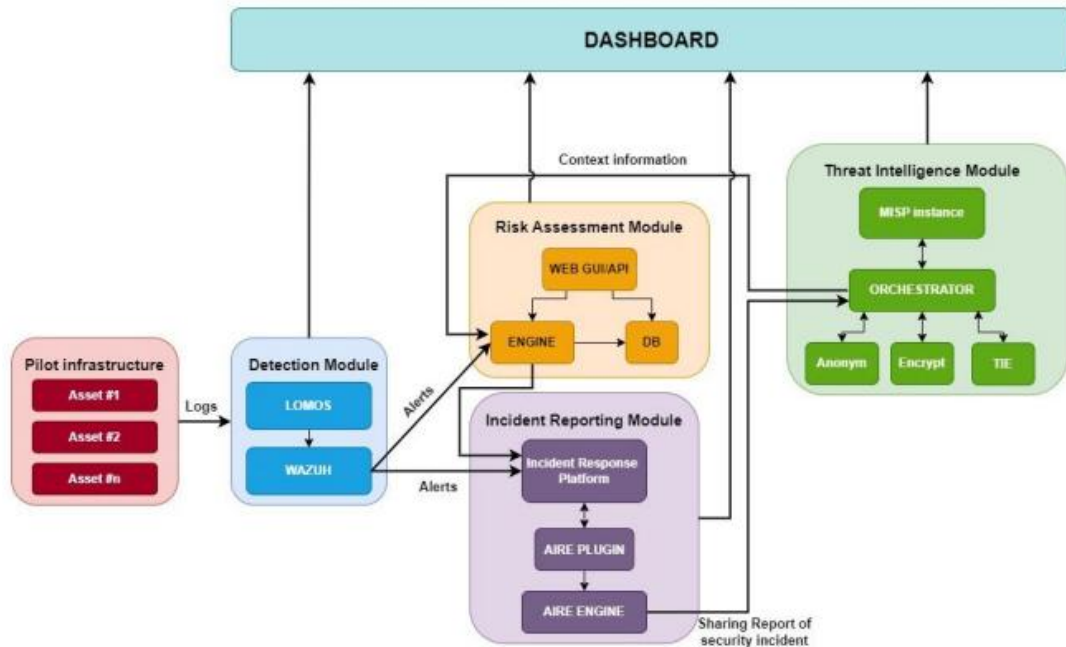


SUNRISE



- + LOMOS monitors system logs to detect behavioural anomalies in real time.
- › More details about the LOMOS functionalities are presented in the dedicated training video and step-by-step training guide.

Health Credential Validation



- + CPR modules are connected to allow cross-functional responses:
 - › LOMOS anomalies and WAZUH alerts feed into CERCA and AIRE
 - › CERCA uses threat data and organisational inputs to assess evolving risks
 - › AIRE manages incidents from detection through to reporting
 - › TINTED enhances threat context and feeds this back to CERCA



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.