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

CPR Threat Intelligence Module (TINTED)

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.

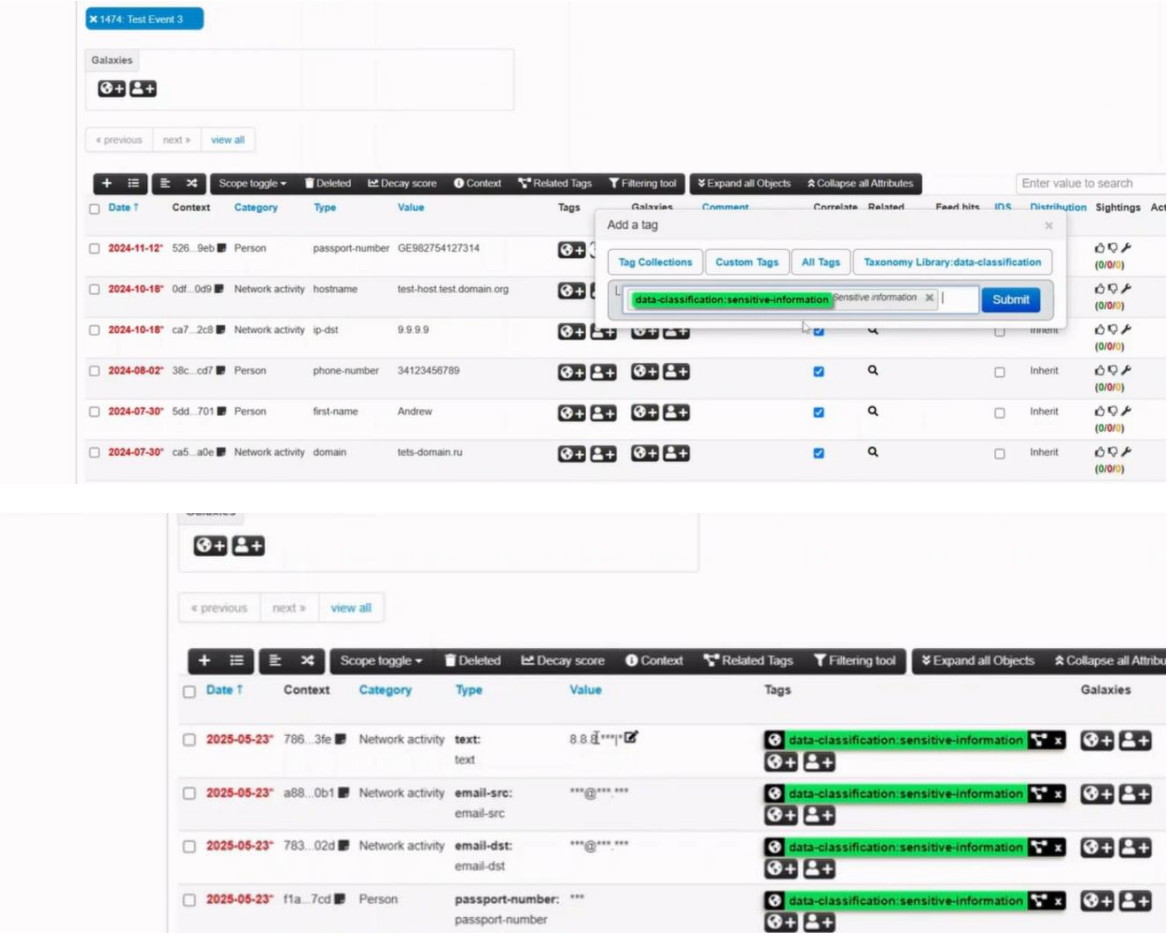
- **CPR is especially valuable for operators of essential services**, offering capabilities that strengthen incident awareness, improve response times, and support decision-making during both normal operations and crisis scenarios.

Content Overview

SUNRISE

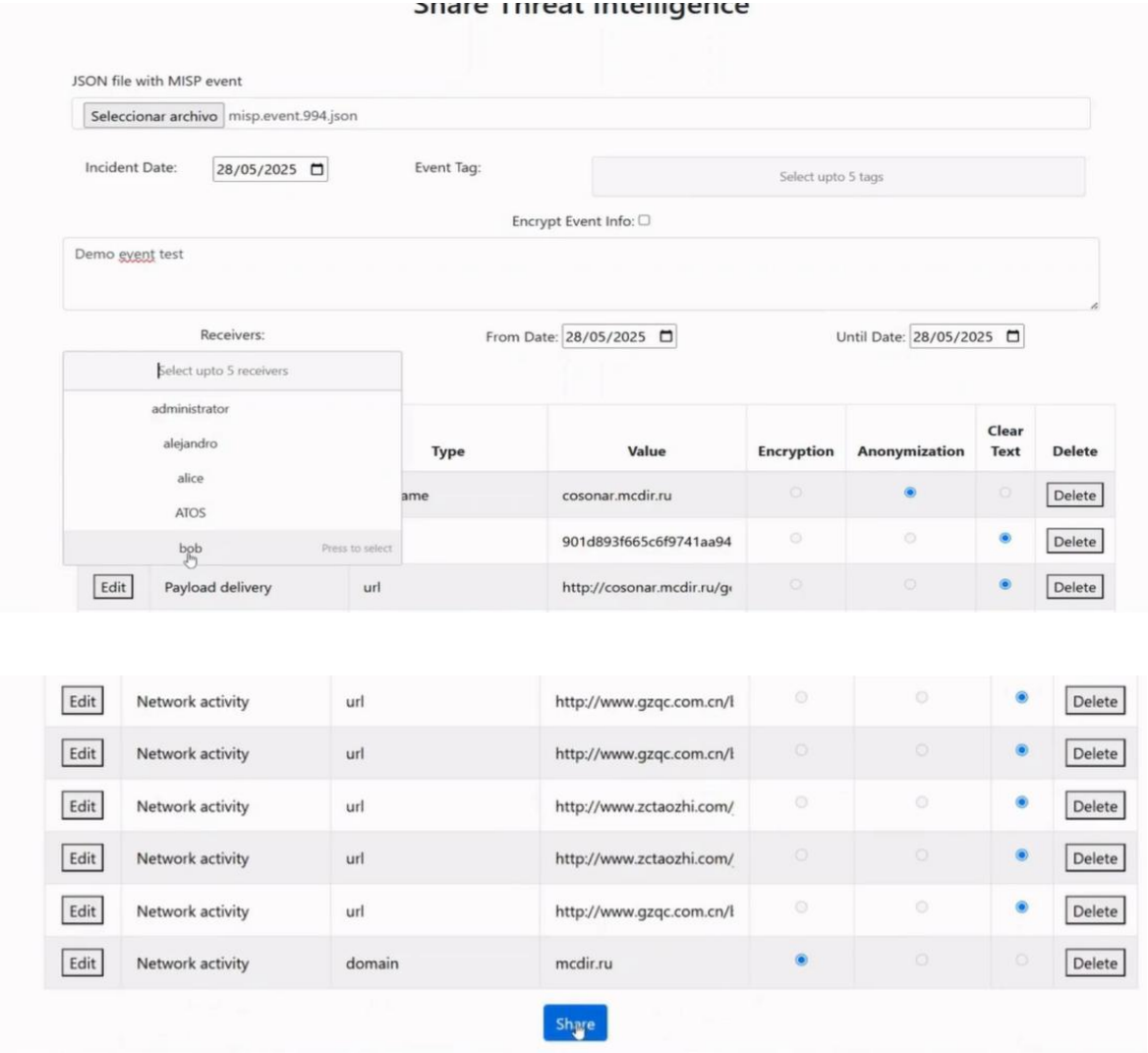
This step-by-step training guide provides an overview of the **CPR Threat Intelligence Module (TINTED)**, part of the SUNRISE Cyber-Physical Resilience Tool. It is designed to help users understand and navigate the key features. It forms part of the training materials provided for the solution, alongside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

Anonymising Sensitive Attributes



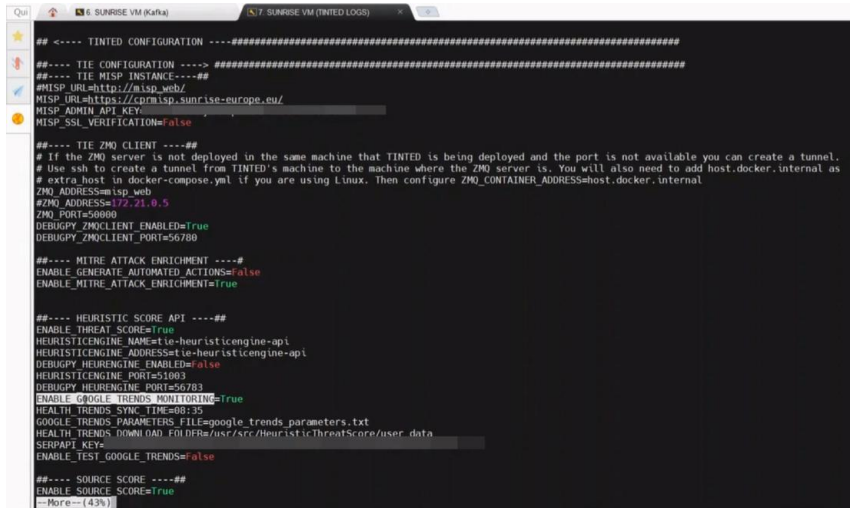
- TINTED supports **fine-grained anonymisation** of selected data points.
- Set anonymisation options in the environment file:
  - **Replace** source organisation name
  - **Choose** whether to keep or remove the original event
  - **Tag** specific attributes (e.g. IP, passport number, email) for anonymisation
- On publishing:
  - A new **anonymised event** is created
  - Original attribute types are replaced with text, with type noted in the comment.

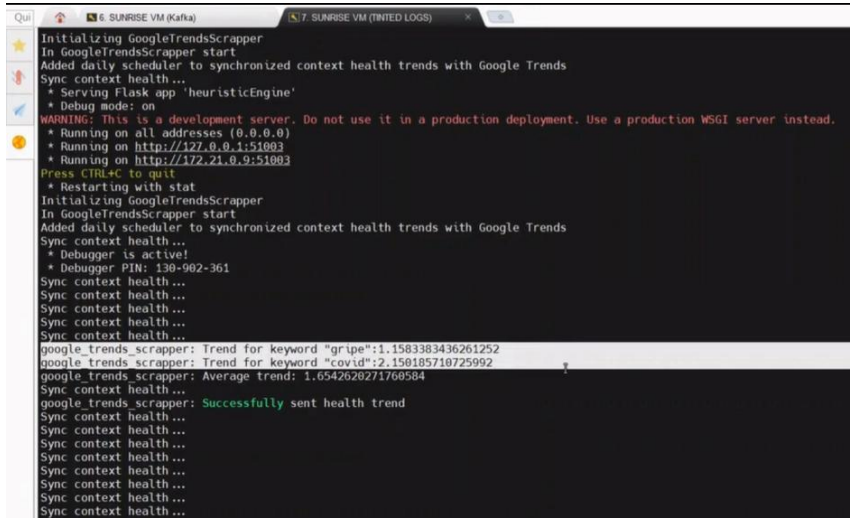
Sharing Threat Intelligence



- From the **Events** tab, view existing events created or received.
- To share an event:
  - Select it from the Share tab
  - Choose **specific attributes** to encrypt or anonymise (e.g. domain, hostname)
  - Select the **recipient** (e.g. another user like Bob)
  - Click Share to send securely
  - Shared events become visible only to designated recipients.

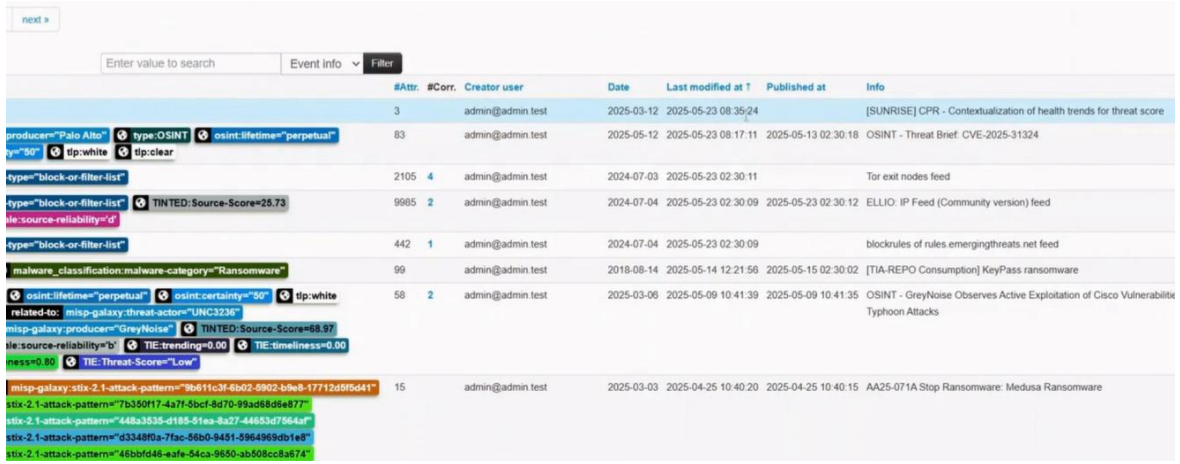
Enabling Contextual Health Trend Data





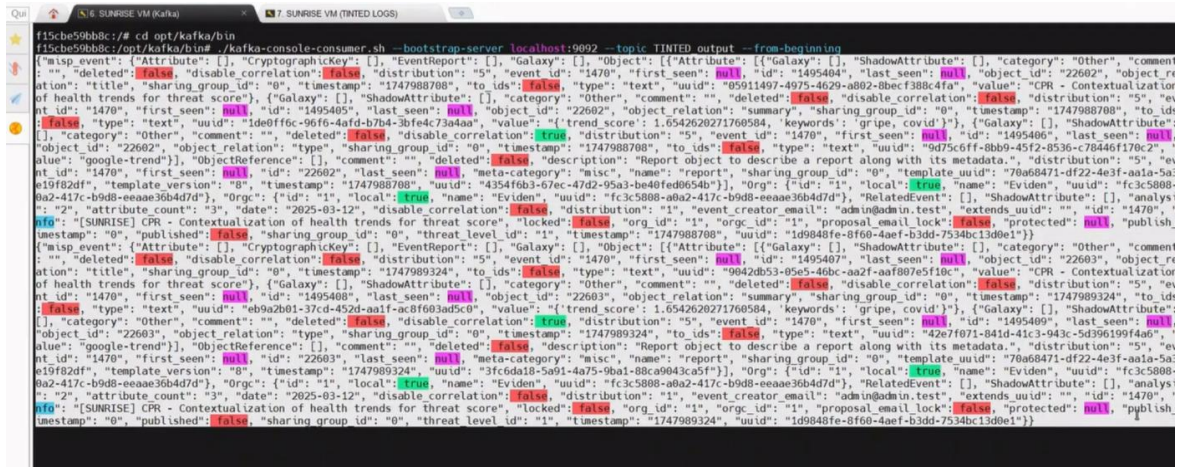
- Health trends (e.g. flu, COVID) are used to enrich threat scores
- Enable in the configurations:
  - GOOGLE_TRENDS_MONITORING = true
  - Set a **daily sync** time
  - Add a list of **search terms** (with **language** and **region**) and a Google API key
  - Trend data is retrieved and scored daily

Generating & Reviewing Trend Events



- Trend scores are packaged into a MISP event
- These include:
  - Average **scores** for each keyword
  - Event metadata and search parameters
  - The event is displayed in the MISP dashboard and passed to the CPR risk engine via Kafka

Verifying Logs & Threat Data Flow



- TINTED logs show:
  - Daily health trend sync operations
  - Kafka messages confirming MISP event forwarding
  - Monitor logs to confirm:
  - Successful event creation
  - Transmission to the Risk Assessment module

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