

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](#).

01

Anonymising
Sensitive Attributes

02

Sharing Threat
Intelligence

03

Enabling
Contextual Health
Trend Data

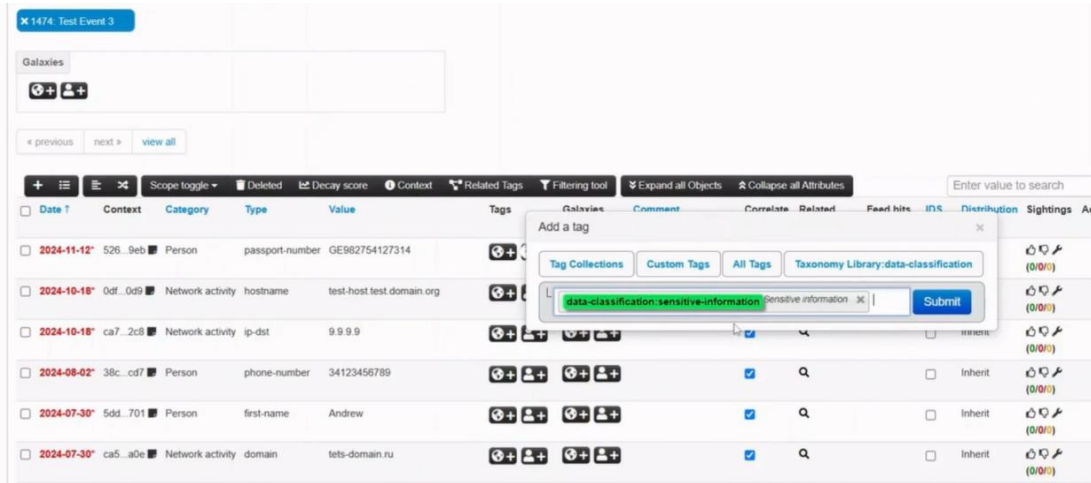
04

Generating &
Reviewing Trend
Events

05

Verifying Logs &
Threat Data Flow

Anonymising Sensitive Attributes



1474: Test Event 3

Galaxies

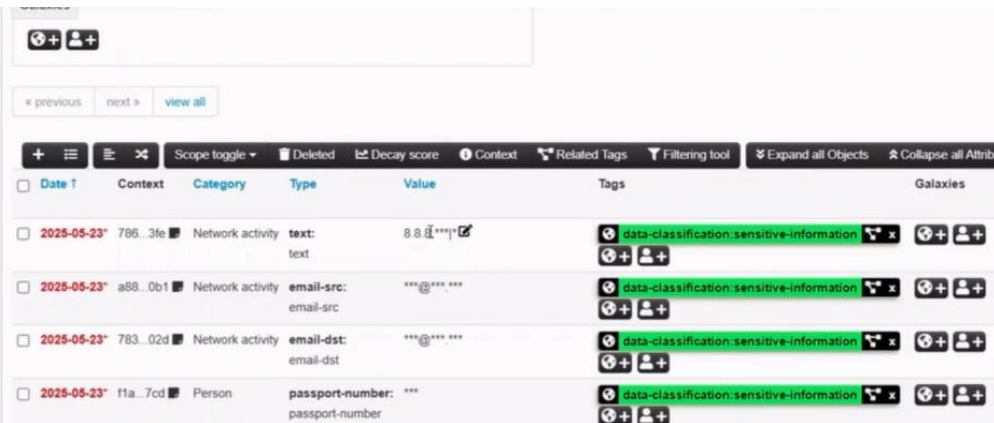
« previous next » view all

	Date ↑	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related	Feed hits	INS	Distribution	Sightings	Act
☐	2024-11-12*	526...9eb	Person	passport-number	GE982754127314										
☐	2024-10-18*	0df...0d9	Network activity	hostname	test-host-test domain.org										
☐	2024-10-18*	ca7...2c8	Network activity	ip-dst	9.9.9.9										
☐	2024-08-02*	38c...cd7	Person	phone-number	34123456789										
☐	2024-07-30*	5dd...701	Person	first-name	Andrew										
☐	2024-07-30*	ca5...a0e	Network activity	domain	lets-domain.ru										

Add a tag

Tag Collections Custom Tags All Tags Taxonomy Library: data-classification

data-classification: sensitive-information sensitive information x Submit



« previous next » view all

	Date ↑	Context	Category	Type	Value	Tags	Galaxies
☐	2025-05-23*	786...3fe	Network activity	text:	8.8.8.8	 data-classification: sensitive-information 	
☐	2025-05-23*	a88...0b1	Network activity	email-src:	***@***.***	 data-classification: sensitive-information 	
☐	2025-05-23*	783...02d	Network activity	email-dst:	***@***.***	 data-classification: sensitive-information 	
☐	2025-05-23*	f1a...7cd	Person	passport-number:	***	 data-classification: sensitive-information 	

- + 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



Share Threat Intelligence

JSON file with MISP event

Seleccionar archivo misp.event.994.json

Incident Date: 28/05/2025 Event Tag: Select upto 5 tags

Encrypt Event Info: ☐

Demo event test

Receivers: From Date: 28/05/2025 Until Date: 28/05/2025

Select upto 5 receivers

administrador
alejandra
alice
ATOS
bob

Press to select

Edit Payload delivery url

Type	Value	Encryption	Anonymization	Clear Text	Delete
name	cosonar.mcdir.ru	☐	☒	☐	Delete
	901d893f665c6f9741aa94	☐	☐	☒	Delete
	http://cosonar.mcdir.ru/g	☐	☐	☒	Delete

Edit	Network activity	url	http://www.gzqc.com.cn/l	☐	☐	☒	Delete
Edit	Network activity	url	http://www.gzqc.com.cn/l	☐	☐	☒	Delete
Edit	Network activity	url	http://www.zctaozhi.com/	☐	☐	☒	Delete
Edit	Network activity	url	http://www.zctaozhi.com/	☐	☐	☒	Delete
Edit	Network activity	url	http://www.gzqc.com.cn/l	☐	☐	☒	Delete
Edit	Network activity	domain	mcdir.ru	☒	☐	☐	Delete

Share

- + 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

```
## --- TINTED CONFIGURATION ---#####
##--- TIE CONFIGURATION ---#####
##--- TIE MISP INSTANCE---##
#MISP_URL=http://misp_wsb/
MISP_URL=https://cpr.misp.sunrise-europe.eu/
MISP_ADMIN_API_KEY=
MISP_SSL_VERIFICATION=False

##--- TIE ZMQ CLIENT ---##
# If the ZMQ server is not deployed in the same machine that TINTED is being deployed and the port is not available you can create a tunnel.
# Use ssh to create a tunnel from TINTED's machine to the machine where the ZMQ server is. You will also need to add host.docker.internal as
# extra_host in docker-compose.yml if you are using Linux. Then configure ZMQ_CONTAINER_ADDRESS=host.docker.internal
ZMQ_ADDRESS=ip_wsb
#ZMQ_ADDRESS=172.21.0.5
ZMQ_PORT=50000
DEBUGPY_ZMQCLIENT_ENABLED=True
DEBUGPY_ZMQCLIENT_PORT=50700

##--- MITRE ATTACK ENRICHMENT ---##
ENABLE_GENERATE_AUTOMATED_ACTIONS=False
ENABLE_MITRE_ATTACK_ENRICHMENT=True

##--- HEURISTIC SCORE API ---##
ENABLE_THREAT_SCORE=True
HEURISTICENGINE_NAME=ie-heuristicengine-api
HEURISTICENGINE_ADDRESS=ie-heuristicengine-api
DEBUGPY_HEURISTICENGINE_ENABLED=False
HEURISTICENGINE_PORT=51003
DEBUGPY_HEURISTICENGINE_PORT=50703
ENABLE_GOOGLE_TRENDS_MONITORING=True
HEALTH_TRENDS_SYNC_TIME=00:30
GOOGLE_TRENDS_PARAMETERS_FILE=google_trends_parameters.txt
HEALTH_TRENDS_DOWNLOAD_FOLDER=/usr/src/HeuristicThreatScore/user_data
SERVAPI_KEY=
ENABLE_TEST_GOOGLE_TRENDS=False

##--- SOURCE SCORE ---##
ENABLE_SOURCE_SCORE=True
| More... (43%)
```

```
Initializing GoogleTrendsScraper
In GoogleTrendsScraper start
Added daily scheduler to synchronized context health trends with Google Trends
Sync context health...
* Serving Flask app 'heuristicEngine'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://172.0.0.1:51003
* Running on http://172.21.0.9:51003
Press CTRL+C to quit
* Restarting with stat
Initializing GoogleTrendsScraper
In GoogleTrendsScraper start
Added daily scheduler to synchronized context health trends with Google Trends
Sync context health...
* Debugger is active!
* Debugger PIN: 130-902-361
Sync context health...
Sync context health...
Sync context health...
Sync context health...
Sync context health...
google_trends_scrapper: Trend for keyword "gripe":1.1583383436261252
google_trends_scrapper: Trend for keyword "covid":2.150185710725992
google_trends_scrapper: Average trend: 1.0542620271760584
Sync context health...
google_trends_scrapper: Successfully sent health trend
Sync context health...
Sync context health...
Sync context health...
Sync context health...
Sync context health...
Sync context health...
Sync context health...
Sync context health...
```

- + 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

next »

Enter value to search

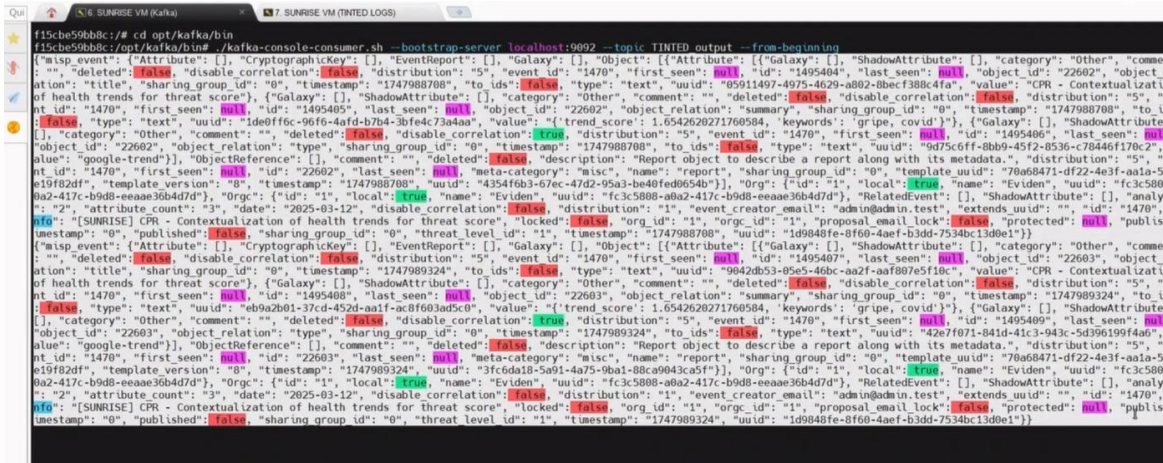
Event info Filter

	#Attr	#Corr	Creator user	Date	Last modified at ↑	Published at	Info
	3		admin@admin test	2025-03-12	2025-05-23 08:35:24		[SUNRISE] CPR - Contextualization of health trends for threat score
producer:"Palo Alto" type:OSINT osint:lifetime:"perpetual" y:"90" ttp:white ttp:clear	83		admin@admin test	2025-05-12	2025-05-23 08:17:11	2025-05-13 02:30:18	OSINT - Threat Brief: CVE-2025-31324
type:"block-or-filter-list"	2105	4	admin@admin test	2024-07-03	2025-05-23 02:30:11		Tor exit nodes feed
type:"block-or-filter-list" TINTED:Source-Score=25.73	9985	2	admin@admin test	2024-07-04	2025-05-23 02:30:09	2025-05-23 02:30:12	ELLJO: IP Feed (Community version) feed
type:"block-or-filter-list"	442	1	admin@admin test	2024-07-04	2025-05-23 02:30:09		blockrules of rules emergingthreats net feed
malware_classification:malware-category:"Ransomware"	99		admin@admin test	2018-08-14	2025-05-14 12:21:56	2025-05-15 02:30:02	[TIA-REPO Consumption] KeyPass ransomware
osint:lifetime:"perpetual" osint:certainty:"90" ttp:white related-to: misp-galaxy:threat-actor:"UNC3236" misp-galaxy:producer:"GreyNoise" TINTED:Source-Score=68.97	58	2	admin@admin test	2025-03-06	2025-05-09 10:41:39	2025-05-09 10:41:35	OSINT - GreyNoise Observes Active Exploitation of Cisco Vulnerability Typhoon Attacks
le:source-reliability="b" TIE:trending=0.00 TIE:timeliness=0.00 ness=0.86 TIE:Threat-Score="Low"							
misp-galaxy:stix-2.1-attack-pattern:"B6f11c3f-4b02-8902-b1eb-17712d8f6d41" stix-2.1-attack-pattern:"7b350f17-4a7f-5b6f-8d70-93ac68d6e677" stix-2.1-attack-pattern:"448a3535-d185-51ea-8a17-44653d7064a9" stix-2.1-attack-pattern:"d334870a-7fac-586b-8451-5964969db1e3" stix-2.1-attack-pattern:"46b6fd46-e4fe-54ca-9650-ab508cc8a674"	15		admin@admin test	2025-03-03	2025-04-25 10:40:20	2025-04-25 10:40:15	AA25-071A Stop Ransomware: Medusa Ransomware

Verifying Logs & Threat Data Flow



+ TINTED logs show:





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.