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

CPR Anomaly Detection Module (LOMOS)

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 Anomaly Detection Module (LOMOS)**, 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 Dataset Review & Anomaly Scores

02 Log Data Structure Inspection

03 Chart Anomaly Spotting

04 High-Scoring Log Line Investigation

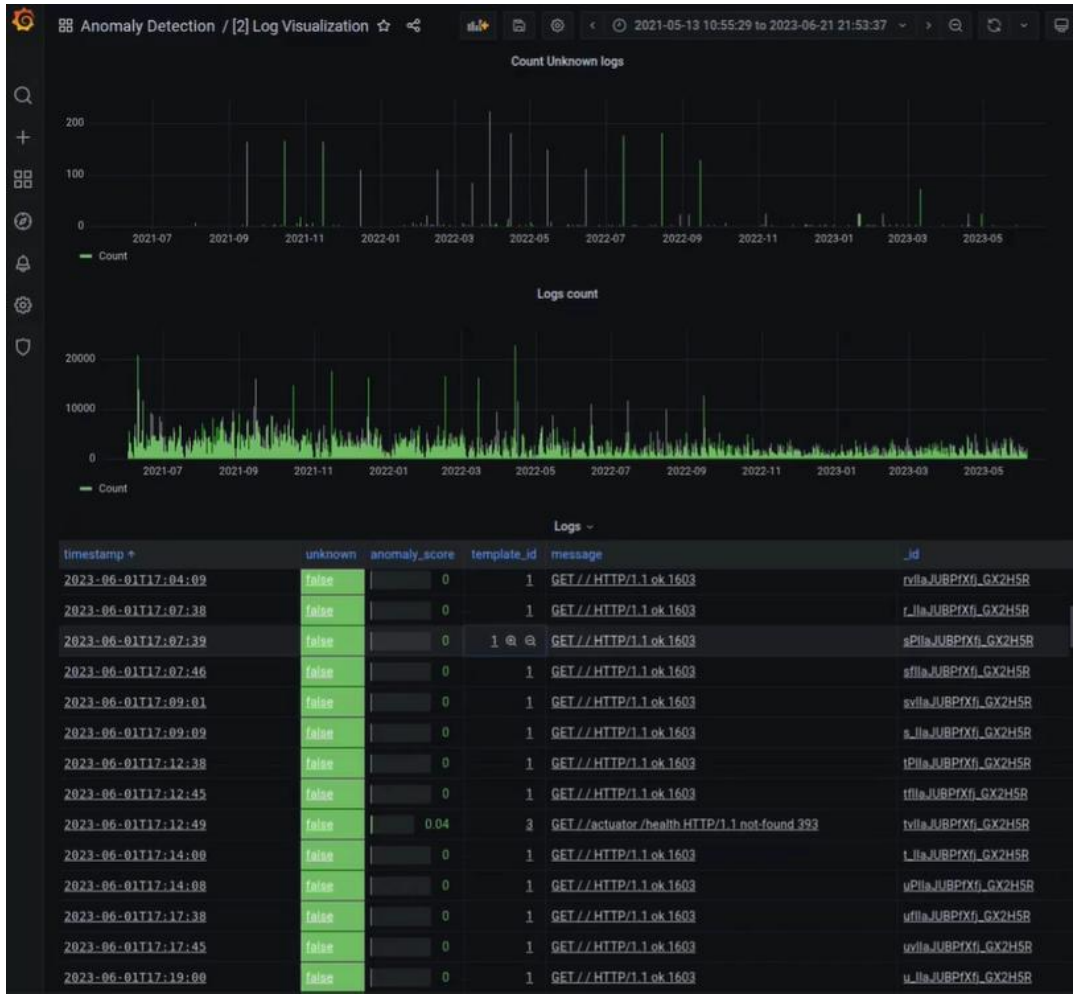
05 Keywords Interpretation

06 Kafka Message Alert

Dataset review & Anomaly Scores

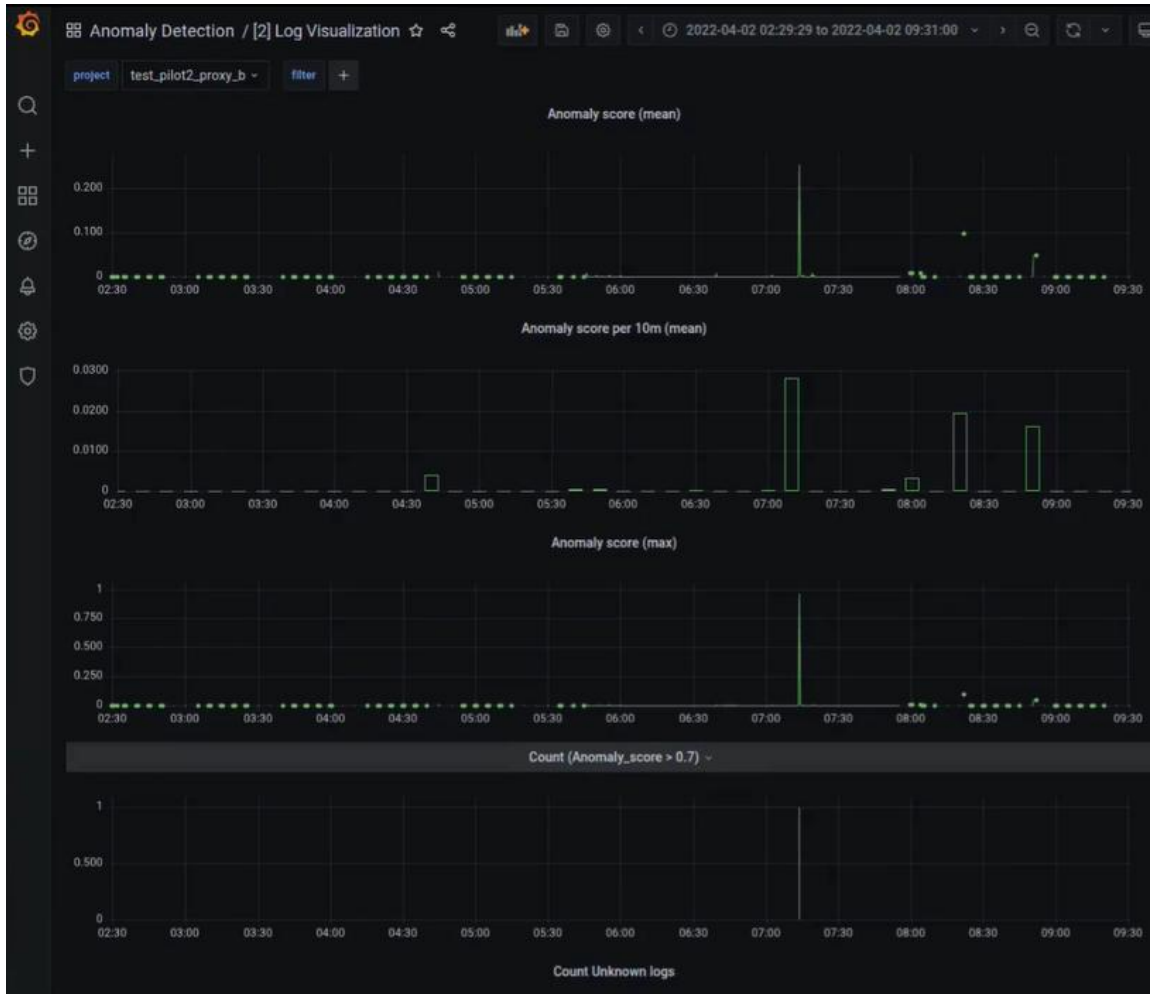
- Open the *Anomaly Score (Max)* chart.
- Observe that the **first two months** were used for training the model. During this period, **few anomalies are detected**.
- After the training period ends, the system begins detecting **more frequent anomalies** as real-time analysis starts.

Log Data Structure Inspection



- Review how individual **log lines** appear in the interface.
- These entries are primarily plain-text and may appear repetitive at first glance, but they contain the raw data used for anomaly analysis.

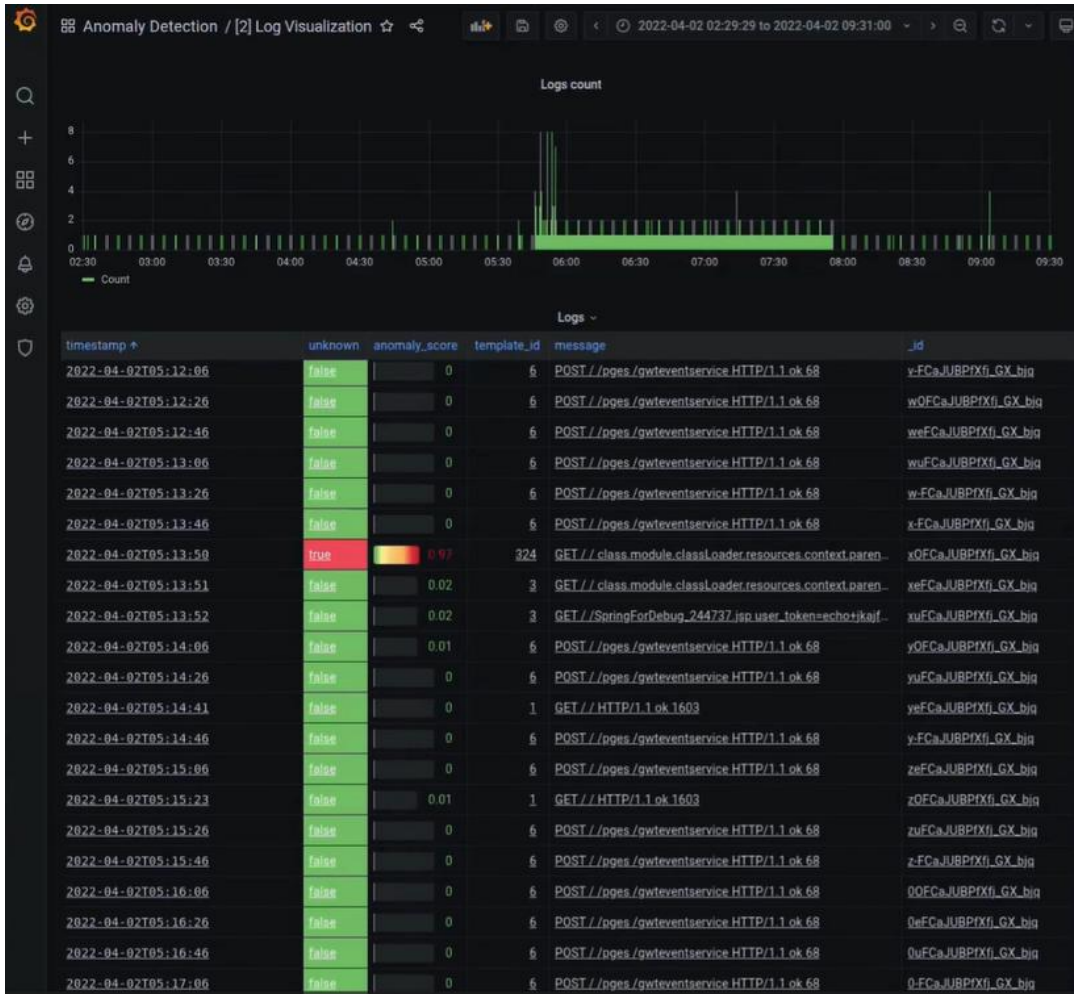
Chart Anomaly Spotting



SUNRISE

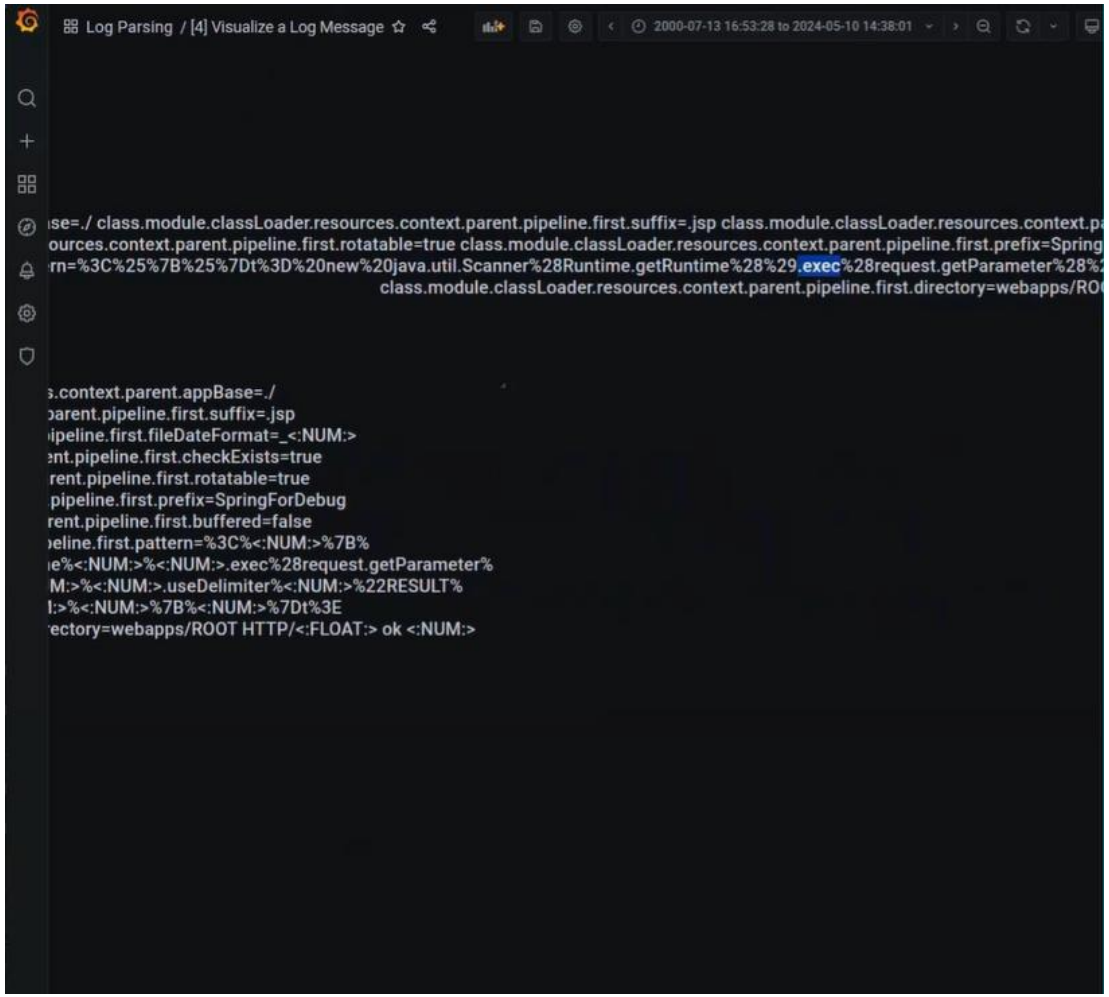
- Look again at the *Anomaly Score (Max)* chart.
- Identify a **spike** where one log line stands out with a **high anomaly score**.
- Most other log lines show **near-zero scores** and are not considered significant.

High-Scoring Log Line Investigation



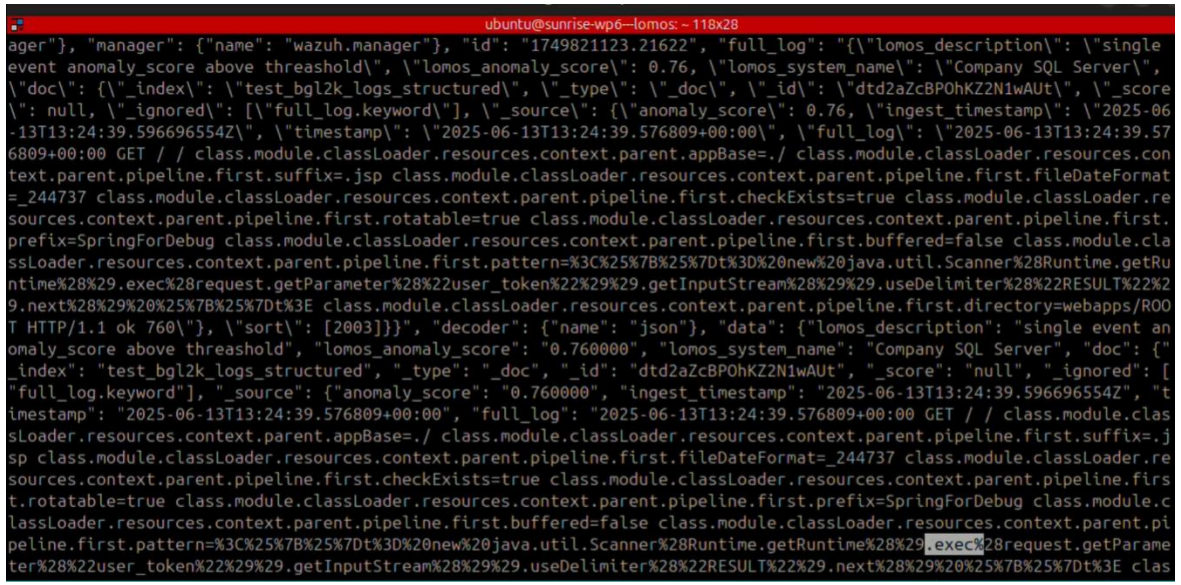
- Click on the **highlighted red log line** with the high anomaly score to inspect it further.

Keywords Interpretation



- In the detailed view, notice that the **URL** in the log line looks unusual and **more like Java code** than a normal web address.
- Within the log line, spot the keyword **"exec"**, which indicates a potential **execution attempt**.
- This keyword is part of what led LOMOS to mark this log line as anomalous.

Kafka Message Alert



SUNRISE

- As a response to this detected anomaly, LOMOS sends a message across the system using the **Kafka message bus**.
- In the **debug version** of this Kafka message, the **original log line** is included exactly as it appeared.
- A portion of the log line is **highlighted**, specifically the **"exec"** keyword, to draw attention to the suspicious part.

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