KR08 – Cyber-Attack Detection Framework

Purpose

The Cyber-Attack Detection Framework (CADF) key result aims to **detect and trace complex cyber-attacks** against applications and systems.

The CADF provides a set of **heterogeneous security probes**, including a network intrusion detection system, a host-based intrusion detection system and file integrity monitor, a malware scanner, a system-level monitor, and a network traffic monitor, and an Electro Magnetic parameters analyser.

Furthermore, the events from the probes are processed, analytics on the status of the system are provided and **alerts** are raised in case of incoming cyber-attacks. It allows to design and deploy **detection rules** which provide the logic for the events' **correlation**.

Scope

CADF has been proposed to improve the security of the ground segment through a set of tools for cyber-attack detection.

The CADF is integrated in the 7SHIELD framework via a **Message Broker** and the interface is included in one of the main **7SHIELD Graphical User Interface** (GUI).

Additionally, the **authentication** to the GUI of the CADF is using the secure mechanism implemented in the 7SHIELD project.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883284

Partners

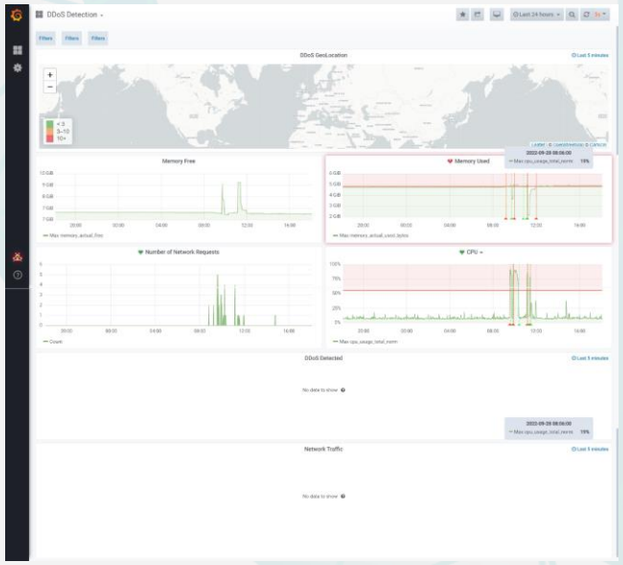
CeRICT
Italy

CeRICT is a research consortium founded in 2005 as a no-profit organization to foster the cooperation of Italian computer scientists and engineers in ICT. The Research Team involved in 7SHIELD is the FITNESS Research Group (www.fitnesslab.eu), which consists of researchers who are currently at the University of Naples Parthenope. CeRICT has a valuable track record in fields like critical infrastructure protection, network resilience, cloud security, risk management, and data collection.

Detection

Sensors Technologies

Situational Awareness



All the modules developed in the frame of 7SHIELD have been designed with the consultancy of identified external stakeholders, first responders and following the **requirements** provided by the partners working in the space sector acting as Pilots, who provided the Critical Infrastructures for **testing and demonstration**.

Contribution

CeRICT has been responsible for the CADF implementation and the design of correlation rules according to the project needs.

The task has been assigned to CeRICT due to its long track experience and expertise in the **cybersecurity domain**, gained thanks to its participation to several European funded research projects.

Stakeholders

The CADF can provide great improvement of the overall security and resilience of cyber and hybrid systems, which can benefit from the **real-time security monitoring** functionality.

The CADF could be customized to be used by:

- **Critical Infrastructure operators**
- **IT companies**
- **Cloud Service Providers**
- **Public Administration**

due to its highly scalable and elastic architecture which can easily be integrated inside existing systems of organizations. Moreover, the major strength of the framework lies in the possibility to create ad **hoc correlation rules, detecting complex attacks**.

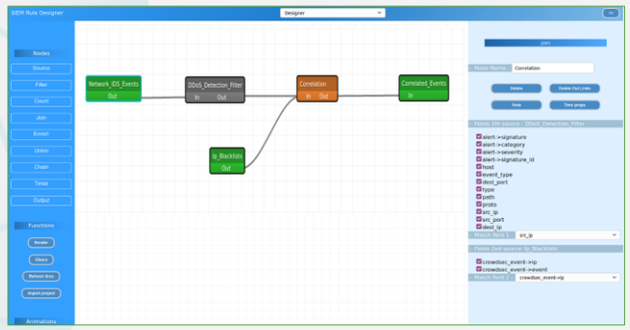
Contact

- luigi.coppolino@uniparthenope.it

Technology

All the components of the framework have been deployed in Docker. The data is collected by the probes and correlated through pre-defined rules. The framework adopts a selection of best-of-breed open-source software tools such as Suricata, Metricbeat, Filebeat, ClamAV, Logstash, Elasticsearch, Flink, along with internal developed solutions. The GUI consists of a set of custom Grafana dashboards

The usage of **open-source** technologies **simplifies the maintenance** of the framework in order to let it be **always updated**.



Future Improvements

The CADF can be enriched with the implementation of **new software probes** that would allow for obtaining a wider picture of the security status of the infrastructure being monitored.

In the next future, the CADF could be integrated with a **tamper resistant storage system**, based on blockchain, to ensure protection against attacks targeting data integrity.

www.7shield.eu