7SHIELD

KR11 – Correlators
Combined C/P Threat Detection and Early Warning module

Modules

- Geospatial Complex Event Processing Engine (G-CEP)
- Availability Correlator (AC)
- Hyper Combined Correlator / SIEM correlator (HCC)
- Situational Picture Generation and Update (SPGU)

Detection

Situational Awareness

Semantic Reasoning

Partners

SATWAYS
Greece

Satways LTD (STWS) develops solutions for Security and Public Safety, with the aim to provide effective decision support, simplify operations, provide a Common Operational Picture (COP) and collaboration tools across organizations, collect and disseminate data in the field, and coordinate response units and system users.

CS Novidy's
France

CS Novidy's (CSNov) is a company specialised in Cybersecurity and IT Transformation solutions and services.

ENGINEERING
Italy

Engineering Group (ENG) is a global player in the digital transformation sector, with relevant expertise in business integration and Critical infrastructure protection against cyber and physical (c/p) attacks, for example providing resources to c/p situational awareness and threat intelligence

Scope

Correlators are backend services that provide first-level correlation functionalities. They **correlate the events from the cyber and/or physical threats and availability** that have been detected by the several detection tools that the project provides.

These correlation results are forwarded to HCC and SPGU components for the detection of complex C/P events and the preparation of the infrastructure's situational picture.

The SPGU module, integrated into the 7SHIELD framework, is the **CORE module**, acting as a "middleware" through which the messages that the modules of the framework intend to exchange between themselves pass. It is very useful for keeping all systems aligned and providing **awareness** to the structure of the **current situational picture**.

Contribution

STWS has designed and implemented a new version of the G-CEP, based on its long experience in the field of physical security and safety. Within 7SHIELD, G-CEP is used as a backend service that collects all events produced by the physical detection tools and forwards the correlation results to the HCC and SPGU components. For that, the G-CEP has been enhanced to align with the operational requirements of the specific Space Ground Segment.

CSNov is specialist for the Network Operations Center (NOC) services and Security Operations Center (SOC) services designed and developed the AC and HCC;

ENG rules the design and development of the SPGU, by using a Unified Alert Format in order to allow the communication between modules, analyzing and finding a standard format based on a standard format that is IDMEF v2.03 format.

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**.

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

Purpose

The Combined C/P threat early warning and geospatial event correlator tool developed by 7SHIELD includes 4 modules:

- The **G-CEP** allows high-speed event processing, the correlation and identification of physical threats detected by 7SHIELD detectors;
- **AC** monitors the availability of devices, servers, services and 7SHIELD infrastructure modules and alert the HCC in case of availability status changes;
- The **HCC** correlates Physical and/or Cyber-attack and/or Availability alerts and reports correlated alerts to SPGU;
- **SPGU** module collects all the data from 7SHIELD modules and provides an overview of the current status of the general security of the Critical Infrastructure (CI), including the severity level of the events verified.

Stakeholders

Any **infrastructure**, whether **public or private**, whether **large or small**, needs to guarantee and monitor its level of security and criticality. Having a constant monitoring of the status of the critical infrastructure is a great advantage as we use the latest technologies and a variety of devices to monitor this state and always be aware of what happens to prevent or take mitigation actions with respect to critical events.

These modules are able to communicate and to transmit both physical and cyber information. Devices such as video cameras, thermal cameras, motion sensors, laser fences, drones, cyber modules, firewalls, etc. can be involved.

Contacts

- info@satways.net
- info@eng.it
- charlelie.morineau@csnovidys.com
- gaetan.dedobbeleer@csnovidys.com

Technology

The communication through all the modules takes place mostly via a bus based on open-source **Apache Kafka Broker** that allows over 2 million writes per second.

Besides further technologies, we have **JAVA language** and **SPRING framework**. The Object Relational Mapping (ORM) technique is used with **JPA, Hibernate, Spring Data technology**. It uses a standard geospatial representation as Geometry for the persistence of data on **PostGIS** databases, **JTS** libraries for business logic and **GEO-Json** for data rendering. A Web Socket is used to aid in communication with the frontend. Custom sockets are used for handshaking with URLs that use SSL protocol for automatic certificate retrieval. The application runs behind **NGINX** web server for **reverse-proxy**. All modules are distributed in **docker** containers.

The G-CEP service, based on **open-source technologies**, is a high-performance correlator, able to receive, handle, correlate and identify complex events, using the events produced by the multiple physical detection tools of 7SHIELD.

Future Improvements

The 7SHIELD CORE system can be further improved through a more advanced management of the exchanged messages, in which the message that updates all the modules of the current state of the CI through the Situational Picture, is not a single large message, rather a logical structure which allows third-party systems to use microservices to reconstruct the situational picture by retrieving only the necessary information using a Lazy strategy. This would greatly **improve performance** by avoiding bottlenecks due to clogging of messages sent on the bus, problems related to heap memory and greater speed in managing information for all modules of the framework.

Moreover, in the future it is planned to improve the HCC in order to enable the triggering of alerts based on AI detected anomalies.

www.7shield.eu