Network Intrusion Detection Network Application

SUMMARY

Experimentation with the 5G-EPICENTRE requires the guarantee of security which is necessary for building trust, both for all parties, both the vertical PPDR users and the testbeds, as well as the platform itself.

To this end, a new Network Intrusion Detection Network Application has been developed, based on the architecture of the Holistic Security and Privacy Framework (HSPF) for the identification of possible threats; their evaluation; and prevention of any type of malicious software in the E2E chain.

Follow Us on our social media for more Network Applications updates::

LESSONS LEARDNED

The Framework aims to :

- **The overall HSPF aims to meet the 5G challenges for Public and Private Networks.** The use of private networks does not gurantee a high-level of security for virtual infrastructures and cloud-based architectures.
- **The framework provide a proactive design of a comprehensive security plan, which guarantees both the network's advancement (delivering high-bandwidth and low-latency) in terms of both KPIs and UX**.

For more information, do not hesitate to visit the website https://www.5gepicentre.eu/ and/or contact the 5G-EPICENTRE team.

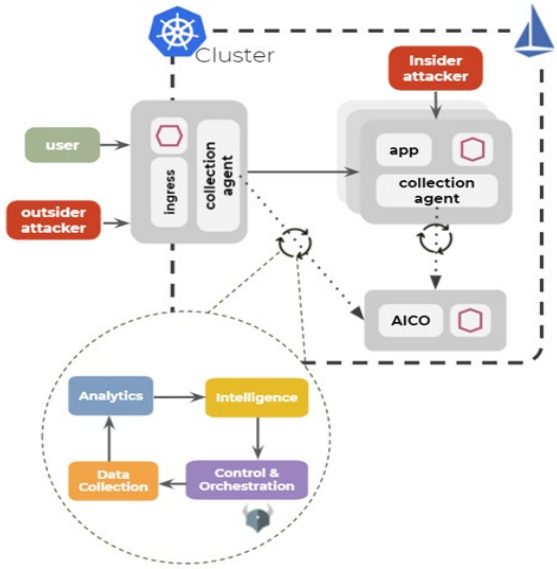
Contact the 5G-EPICENTRE team by filling in the **form** provided. Apply **here**!

SERVICES & VALUE FOR END-USERS

Within the context of the 5G-EPICENTRE, the tecnhical partners developed the architecture of the the Holistic Security and Privacy Framework (HSPF) for securing the protection of all parties involved from malacious software and guarantee trust.

The HSPF has evolved to a Network Intrusion and Detection System (NIDS), which can be exposed to vertical experimenters to detect traffic anomalies related to security incidents. It can also trigger security policies. The was validated with different 5G-EPICENTRE UCs and made available via 5G-EPICENTRE Portal to be instantiated next to any vertical Network Application (even 3rd pary experimentiers).

The deployment of HSPF Network Application assumes a Kubernetes environment with Istio's implementation of the Service Mesh. The injection of collection-agents during run-time is allowed by Kubernetes, thus enabling the possibility of deploying this framework next to an already executing Network Application, without disrupting its normal behaviour. The NIDS is composed of four major NFs: the Collector, the Agent, the Aggregator and the Dashboard. Both the HSPF Collector and the HSPF Agent components correspond to sidecars that are automatically deployed next to each application micro-service, with the former having the objective of collecting the inbound and outbound traffic and the latter the objective of continuously classifying network traffic, perform federated training rounds, thus keeping the ML models up to date and also to report KPI metrics and the detection of anomalies through the HSPF Reporting Interface. The HSPF Aggregator manages the different micro-services, stores the ML models used for network traffic classification, and orchestrates the federated process.



5G-EPICENTRE's Holistic Security and Privacy Framework (HSPF)

This project has received funding from the European Union's Horizon 2020 Innovation Action programme under Grant Agreement No 101016521.