KER 2: TRUST & INCIDENT MANAGER

UNIQUE VALUE PROPOSITION

Improve your monitoring and gathering metrics all across your supply chain infrastructure, performing analysis, raising alerts, proposing mitigation actions

KER 2: TRUST & INCIDENT MANAGER

SOLUTION BENEFITS

CONTINUOUS MONITORING OF INFRASTRUCTURE

An array of both open-source and custom built solutions cast a wide net of detection and assessment, covering a variety of cybersecurity concerns of administrators of IT systems

IMMEDIATE NOTIFICATION OF ANOMALIES

Detected events and generated alerts are not only stored, but immediately propagated through a notification channel, enabling both prompt informing of system administrators and immediate mitigations of other automated systems in the platform.

AUTOMATED RECOMMENDATIONS

Providing automated recommendations to address detected events over mitigating actions

KER 2: TRUST & INCIDENT MANAGER

INNOVATION SCOPE

INNOVATION

Architecture designed for supply chains, instead of single network, storage component with an integrated pub-sub layer, and a ML-based incident detection system.

PROBLEM

The vulnerability assessment spread across several components of different technologies, owned by different parties and with different objectives cannot be done in an individual way but covering all the different aspects and constraints together.

SOLUTION

Monitoring and gathering metrics from supply chain infrastructure, performing analysis, raising alerts, proposing mitigation actions

VALUE

Combination of multiple different tools (vuln. estimation, IDS, SIEM) to provide as large of a coverage of cybersecurity as possible.

KER 2: TRUST & INCIDENT MANAGER

REFERENCES FROM OUR EARLY ADOPTERS

FARM 2 FORK

The Trust and Incident Manager is able to detect diverse types of attacks based on continuous monitoring of specific points/security probes defined by the F2F IT systems' operators which deliver to the TIM information about the current operation (in the format of log files) and define rules based on which incident/threats are detected, triggering notification delivery to the operator/ID administrator (appropriate user) of the FISHY platform

SMART FACTORIES

The component is used to continuously perform vulnerability scans, classify vulnerabilities (risk-based) and send reports to the IRO component. Specifically, TIM will open incidents when an IoT device not registered to FISHY is detected and escalate the level of criticality if the incident is not dealt with

CONNECTED AUTOMOTIVE

The component is used to assess the risk of attacks by analysing the logs that the SADE services will have available. It is expected that the component will collect the logs from one of the enabled services, analyse them and generate a mitigation response which can be via REST API or by passing messages in a specific RabbitMQ queue. Another possible use case is to generate intents in the IRO in such a way that the mitigation policies are acted upon by this component