KER 4: Security Assurance & Certification

UNIQUE VALUE PROPOSITION

Auditing and reasoning security metrics tailored to the pilots infrastructure, and collecting certifiable evidence from the pilots infrastructure

KER 4: Security Assurance & Certification

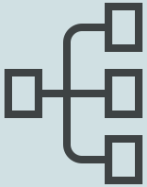
SOLUTION BENEFITS

CUSTOM RULES AUDIT

The custom-based rules are described using a high level language named Event Calculus logic

EVENT COLLECTION ENGINE

Using the Elasticsearch stack as main pool of data collection, connecting with external data pools using message broker AMQTP technologies



SMART RULE MANAGEMENT

The audit component is integrated in Drools rules management system

KER 4: Security Assurance & Certification

INNOVATION SCOPE

INNOVATION

Component architecture tailored to supply chains needs focussing especially to regulatory obligations (e.g., GDPR) and violations/compliance of service level agreements

PROBLEM

The SACM is trying to address the real-time monitoring (in terms of violation or satisfaction) problem of custom-based rules regarding security aspects (including the Confidentiality, Integrity, Availability triangle). Furthermore, it addresses the lack of evidence-based, certifiable view of the security posture of complex ICT systems.

SOLUTION

SACM has 4 main components : The Security Metrics, the auditing component, the evidence-collection engine and the certification component.

VALUE

Easy management of evidence produced by monitoring and assistance with compliance to certification standards, and ensure the truthfulness of the collected data

KER 4: Security Assurance & Certification

EARLY ADOPTERS

FARM 2 FORK

The SACM decides whether the security rules defined by the IT systems' operators have been violated or not in a certain timeframe, and provides details about any incident detected based on this rules as well as about policies that have been enforced as a response to an incident.

SMART FACTORIES

This component can check if the volume of telemetry is lower as the minimum historic and communicates with the Trust Incident Manager to analyze the impacts.

CONNECTED AUTOMOTIVE

This component certifies the software versions installed on each vehicle managed on the FISHY platform, and obtains the installed devices from the vehicles and the list of versions certified as safe by the manufacturer, comparing the version with the listing. When it does not match, the module sends a message to the SADE REST API to control the risk