KER 3: Intent-based Resilience Orchestration

UNIQUE VALUE PROPOSITION

Automation of the interactions between the user defining high level intents and the system applying high level policies

KER 3: Intent-based Resilience Orchestration

SOLUTION BENEFITS

CONFIGURABLE AUTOMATION

Set, modify or delete security policies at scale using high level intent language

TRANSPARENCY AND CONTROL

Using other modules of FISHY to monitor the IT infrastructure, IRO shows notifications and alerts about the network condition, recommand actions, and react based on the situation

SECURITY ENFORCEMENT

Using predefined policies, IRO can react to detected threats automatically or after confirmation from the user, and enforce security rules using other FISHY components

KER 3: Intent-based Resilience Orchestration

FiSHY

INNOVATION SCOPE

INNOVATION

Solution translating high-level intents into configured policies, and interact with the system response using AI techniques, and able to incorporate smart contracts

PROBLEM

The continuous detection of vulnerabilities in production infrastructures and during software development phases, appearing in the infrastructure when new services or features are added, or simply when new vulnerabilities are discovered in existing (outdated) services.

SOLUTION

Automation of the interactions between the user defining high level intents and the system applying high level policies
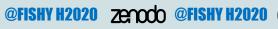
VALUE

The user does not need to know the intermediate technical steps to perform an intent

KER 3: Intent-based Resilience Orchestration

REFERENCES FROM OUR EARLY ADOPTERS

FARM 2 FORK

The IRO offers to the administrators of the F2F IT solutions: a) the capability to register their system and define the rules to be monitored; and b) to receive notifications, alerts and suggestions for actions and security audits of their systems

SMART FACTORIES

This component allows for the registration of systems and devices to FISHY, to be communicated to the EDC and SPI components respectively. It will also, together with the Dashboard, to send notifications, alerts and suggestions for actions and security audits to users according to their profile

CONNECTED AUTOMOTIVE

The use of this component is indirect and allows the generation of policy definitions to be applied by the EDC. The intents are generated by other components based on the analysis and processing of the data obtained from the infrastructure of the SADE use case by these other components