



<https://fishy-project.eu/>

Key Innovations in Supply Chain Cybersecurity and Resilience that Make Sense in Today's Industry

FISHY White Paper #2



This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 952644

1. What are our main results

The pertinence of runtime security is rapidly engaging companies and institutions worldwide, that are becoming more aware of their vulnerabilities and consequences of attacks, in the age of digital transformation affecting workflows across industries. With the different skillsets and expertise of the FISHY consortium partners, the impact of the novelty developed in this project is already affecting highly relevant domains in the context of supply-chain cybersecurity and resilience, such as vulnerability management and risk/integrity assessment; security assurance & certification management; intrusion and detection or cloud-native networking.

KER 1. FISHY Platform: Single window to a complete cybersecurity workflow and technology focusing supply chain resilience

KER 2. Trust & Incident Manager: Advanced tool suit dedicated to vulnerability and impact assessment, risk estimation and mitigation

KER 3. Intent-based Resilience Orchestration : Solution translating high level intents into configured policies, and interact with the system response using AI techniques

KER 4. Security Assurance & Certification Manager: Component tailored to supply chains assessing to regulatory obligations and compliance of service level agreements

KER 5. Security & Privacy Dataspace Infrastructure: Enhanced framework for system events' management, including metrics from different sources and promoting co-relation with added semantics





KER 6. Enforcement & Dynamic Configuration: Framework leveraging a capability model instead of the traditional refinement techniques based on logic rules

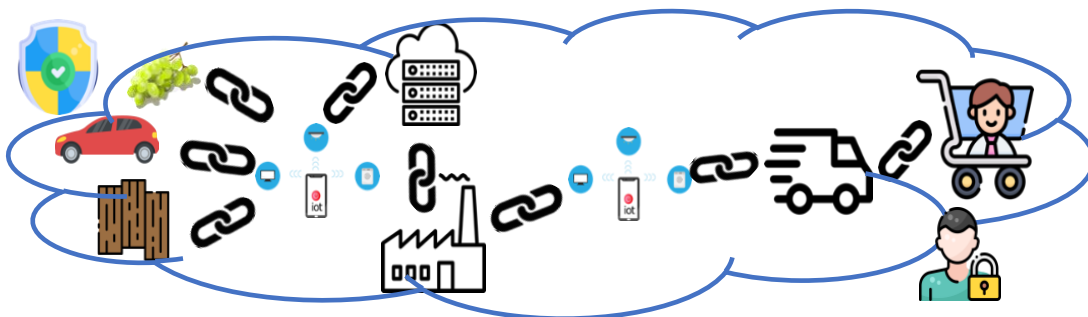
KER 7. Secure Infrastructure Abstraction: Standardised API for network infrastructure abstraction expanding the interfaces to increase orchestration resilience and security monitoring

2. How are they impacting the industry

The FISHY framework considers all the **supply chain** components, from the **IoT ecosystem** to the **infrastructure** connecting them, addressing **security and privacy** functionalities related to **risks** and **vulnerabilities** management, accountability, and **mitigation strategies** as well as **security metrics** and evidence-based **security assurance**

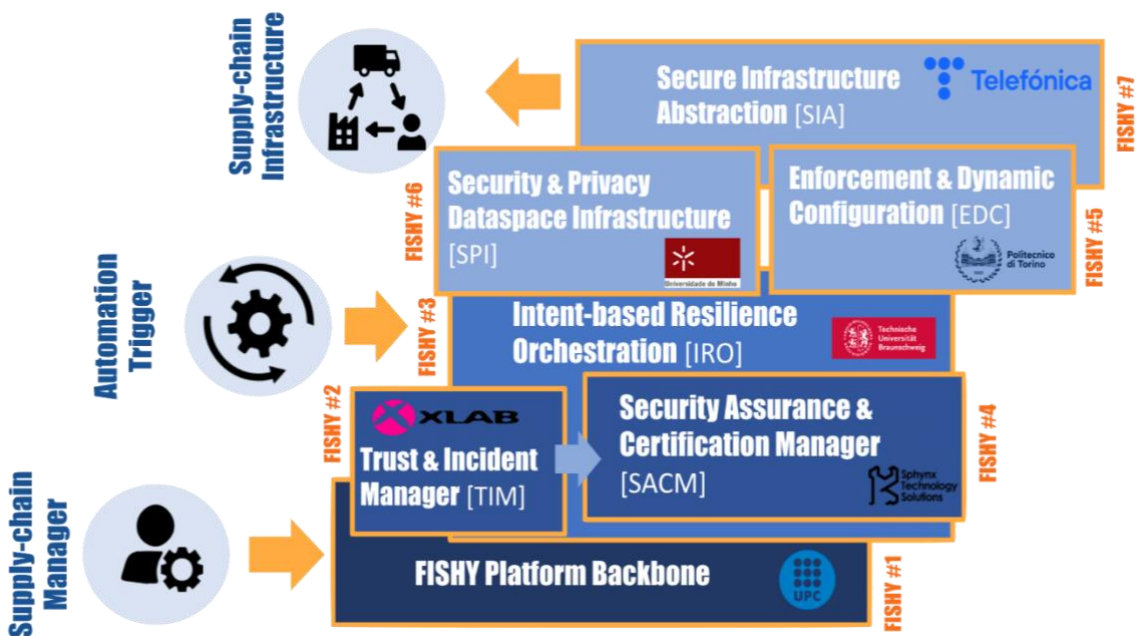
We are helping industries:

-  Design and develop a functional platform for cyber resilience provisioning for supply chains of complex ICT systems, leveraging trust and security management.
-  Establish an evidence-based security assurance and certification methodology identifying security claims and metrics.
-  Develop a metrology model and system for ICT supply chains leveraging trust among parties relying on distributed interledger technologies as well as forecasting and estimation concepts based on artificial intelligence methods.
-  Deploy, validate and demonstrate the FISHY platform in heterogeneous, real-world pilots.



3. What is the FISHY innovation

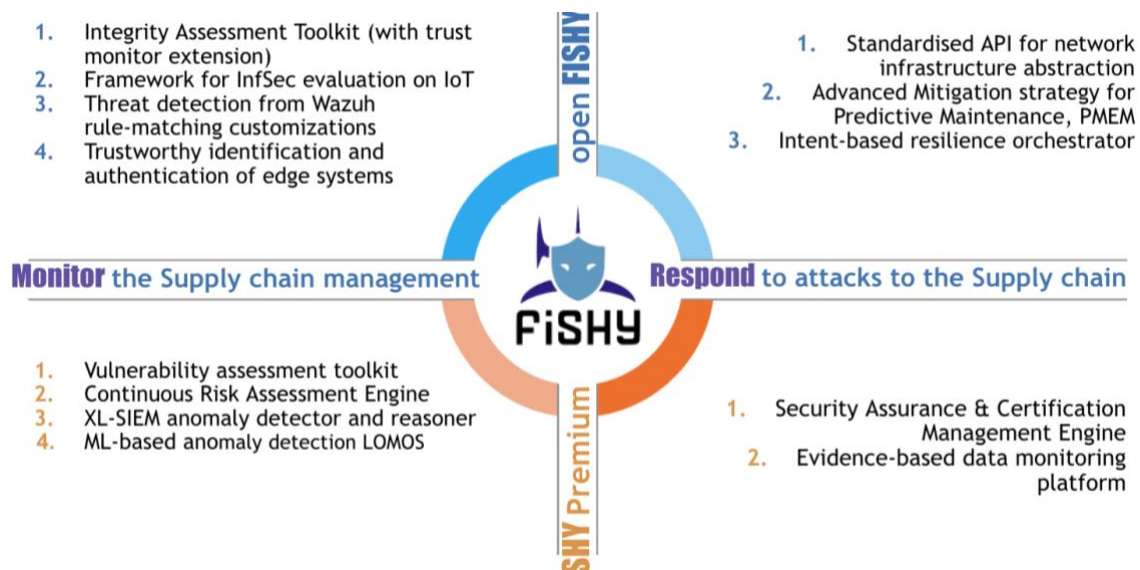
The FISHY coordinated cyber resilient platform provides the appropriate set of tools and methods towards establishing trusted supply chains of ICT systems through novel evidence-based security assurance methodologies and metrics as well as innovative strategies for risk estimation and vulnerabilities forecasting leveraging state-of-the-art solutions, leading to resilient complex ICT systems, comprising the complete supply chain, particularly focusing on the IoT devices at the edge and the network systems connecting them.



This end-to-end technology is covered by technological enablers and core technologies developed within FISHY, covering the following domains: Vulnerability Assessment; Risk Assessment, Privacy enhancement, Data Management, Data Quality Control, API/network monitoring API/network monitoring, Orchestration, Security Assesment, Data Quality Control, and finally platform security.

4. What is the Open FISHY

The importance of Open Source Software and of the Communities associated with it highly contributes to the excellence of European research and development, and for the health and prosperity of the European industrial landscape. In line with the European Commission's Open Source Software Strategy, FISHY contributes to the innovation and autonomy of Europe's digital infrastructure, particularly in the security and resilience of supply chains.



To guide these contributions, we defined the five pillars of open research - (1) a FISHY public repository, (2) KER-specific upstreaming, (3) community engagement, (4) contribution to standards and (5) open research - that promotes the collaboration between researchers, the dissemination and reuse of innovation, and the sustainability of the technology developed in this project. To follow the progress of this community engagement, we use several metrics: GitHub contributors to KER; social media followers of lead partner; and research papers and conferences exposing the KER.

Project results have been contributed to different standardization efforts to maximize their industrial impact, and more specifically their application to the scenarios identified in the use cases. Standards activities of all nature (SDOs, industry associations, open-source communities) have been tracked, analysing the most relevant opportunities, and bringing not only results as direct contributions to existing activities, but also supporting the emergence of new activities based on relevant FISHY outcomes. The project team has sought the collaboration with other related research projects.

5. Which are the Opportunities

KER1. FISHY Platform



CYBERSEC INFORMATION READINESS

Offers enhanced security and real time monitoring of all elements of IT chain, providing security from blockchain-oriented threats with interledger components



AUTOMATION OF CYBERSEC PIPELINES

Guaranteeing data security in a manufacturing context, ensuring data sharing with external entities and cybersecurity of IoT devices, as well as edge and cloud infrastructures.



FLEXIBLE AND RESOURCEFUL FRAMEWORK

The FISHY framework considers all the supply chain components, from the IoT ecosystem to the infrastructure connecting them, addressing security and privacy functionalities related to risks and vulnerabilities management, accountability, and mitigation strategies as well as security metrics and evidence-based security assurance.

FISHY is a platform that is not vendor-specific, with a modular approach to ensuring cybersecurity that offers monitoring, and security and resilience enforcement all-in-one tool (these functionalities are typically separate and vendor-specific).

The OSS functionality extends across the end-to-end prototype of FISHY platform ready with validation in a real context. Potential premium features can be added as pay-per-use or licensed services from the specific value added of the KER-specific technology associated to commercial IP.

Commercial Opportunities:

- Tailor fit solution to a specific domain (e.g., smart logistics);
- Build specific add-ons to benefit a specific domain (e.g., smart logistics).

The FISHY Platform will be an entry point for users and will centralise certain security aspects of the supply chain of software versions of IoT devices embedded in vehicles. It will also enable the management of in-vehicle user identities and facial identities. The platform is expected to have appropriate forms for the management of this data.

Capgemini, Connected Cars Industry

KER2. Vulnerability Forecast & Risk Estimation (TIM)



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

TIM enables users to set up custom scans based on any user-provided script or by using the integrated vulnerability scanners to run the scanning tasks on-demand immediately or set up automatic repeated schedules, being alerted to new vulnerabilities discovered.

Its OSS functionality includes: (i) detection and protection components to verify the application of a predefined patch in a given network, supporting routing verification and topology attestation AI-based anomaly detection; (ii) integrity Assessment Toolkit (Trust Monitor) relying on a physical root-of-trust (the TPM chip) and creating problems in virtualized environments or devices with limited capabilities that lack this chip; and (iii) advanced mitigation strategy (PMEM) AI-assisted tool that suggests maintenance actions to mitigate potential attacks effects based on data analytics and predictive models.

Added to that, TIM also offers Premium Features including: (i) anomaly detector and reasoning (XL-SIEM) capable of applying correlation rules to data coming from heterogeneous sources to launch warnings and alarms about cyber incidents taking place in the monitored infrastructure, following the action of a cyber-criminal; (ii) Continuous Risk Assessment Engine (RAE) calculating and tracking in real-time the economic cyber risk exposure linked to a set of digital assets composing a corporate infrastructure; and (iii) AI/ML-based anomaly detection on application and infrastructure logs (LOMOS).

Commercial Opportunities:

- new security rules;
- integrations for new security tools,
- integrations for 3rd party eg automatic Jira or Kamban,

The trust and Incident Manager is required to be 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. The detection of the events should trigger notification delivery to the operator/ID administrator (appropriate user) of the FISHY platform.

Synelixis, Farm2Fork Industry

KER3. Intent-based Resilience Orchestration (IRO)



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

This technology is translating high level intents into configured policies, and interacts with the system response using AI techniques. It is mostly open source, offering AI/ML-based intent-based resilience orchestration responsible for mapping high-level intents given by a user into configured policies that can run by a lower-level system controller. In FISHY, the IRO receives intents from users as plain text and uses ML techniques to translate user requirements into structured policies compatible with the FISHY enforcer component.

Additional premium features include evidence-based data monitoring platform with enhanced functionalities based on the requirements from the new domains introduced by the use case in this project.

Commercial Opportunities:

- Build specific intent templates for new security rules based on tailored metrics from tools, considering business specifications
- Adjust the IRO Dashboard solution to fit specific use cases

The IRO 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, send notifications, alerts and suggestions for actions and security audits to users according to their profile.

SONAE, Smart Factory

KER4. Security Assurance and Certification Manager (SACM)



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

The SACM is a component focussing especially to regulatory obligations (e.g., GDPR) and violations/compliance of service level agreements, tailored to supply chains needs. It is based on a framework leveraging a capability model instead of the traditional refinement techniques based on logic rules. It is responsible for collecting certifiable evidence from the pilots infrastructure, and auditing/reasoning security metrics tailored to the pilots infrastructure.

The OSS functionality includes Blockchain-based trustworthy identification and authentication of edge solution aimed at enabling a proper authentication of edge devices specifically designed for mobile scenarios and highly constrained devices. On the other hand, SACM offers premium features based on machine learning and incident response capabilities.

Commercial Opportunities:

- Tailor metrics to specific needs of ICT infrastructures
- Complex rules representation using EventCalculus approach
- Resource minimization due to the auditing module Drools implementation

The SACM certifies the software versions installed on each vehicle managed on the FISHY platform. The module is expected to obtain the installed devices from the vehicles and the list of versions certified as safe by the manufacturer. The module will compare the version with the listing. When it does not match, the module is expected to send a message to the SADE REST API to control the risk.

Capgemini, Connected Cars Industry

KER5. Security & Privacy Dataspaces Infrastructure (SPI)



ACCESS CONTROL

Advanced policy and rules definition and enforcement technology



IDENTITY MANAGEMENT

Identity Management strategy, which is fundamental in a supply chain environment where different users' perspectives and demands must coexist



DATA SANITIZATION AND FLOW CONTROL

Data sanitization and flow control from low-level on-premise components, according to previously defined privacy rules.

The EDC is a solution able to translate high level intents into configured policies, and interact with the system response using AI techniques. In FISHY it is responsible for organizing data related to infrastructure events and enforcing privacy and Access Control rules, including Identity Management

The OSS functionality of the SPI is based on a framework for InfSec evaluation with a focus on IoT, including a metrics taxonomy addressing all types of information (security, performance, environmental, and operational) and a model for establishing relation with attacks, aiming at providing automatic (as best as possible) security assessment.

Commercial Opportunities:

- Risk Analysis oriented towards IoT-based architectures
- Attack modelling and security assessment for IoT-based architectures
- Continuous certification aiming to assure a predefined security level for technology infrastructures

The SPI applies security policies to mitigate risks, attacks or intrusions detected, applying security configurations when a non-compliance situation is detected. The request is expected to come from the IRO or the SACM.

SONAE, Smart Factory

KER6. Enforcement & Dynamic Configuration (EDC)



SUPPORT FOR NEW SECURITY DEVICES

A capability model empowers the core of the EDC, allowing an administrator to add support for new types of security controls with ease. Adding new security devices is performed by describing what they offer (e.g., this device is a stateful firewall, supports traffic rate-limiting) without writing ad-hoc code logic



QUICK & EASY NETWORK DESCRIPTION

The use of a high-level policy language grants the administrators the ability to quickly and easily describe what the network functionalities are in a way closer to the human language, without worrying about their actual implementation, which is demanded to the EDC itself



PHYSICAL AND VIRTUALIZED SECURITY CONTROLS

The EDC seamlessly supports both physical and virtualized security controls and allows the administrators to configure mixed networks containing both types of devices

The EDC allows an administrator to effortlessly configure various security controls (e.g., a firewall or a VPN terminator) through high-level declarative policies that are automatically translated into a series of optimal low-level configurations. Its innovative refinement process will consider the current network landscape topology and its configurations to avoid inconsistencies and issues in the deployed rules.

With the OSS version of the EDC the user can refine high-level policies into low-level configurations. It leverages a modular security capability model to describe the available security controls and an inferential engine to perform

a smart and adaptive generation of the controls' configurations. In addition, the EDC allows a timely reaction to a variety of threats by proposing how to reconfigure the security controls for mitigating the attack.

Commercial Opportunities:

- Easy to add support to new devices via the internal XML representation of security controls
- Complex configuration rules generation for specific domains via the capability model

The EDC is required to decide the banning of specific IPs and blockchain wallet IDs when these are issuing an attack (defined by a predefined rule set by the system operator through the IRO). Other similar policies may be defined based on the specifics of the IT solutions in place.

Synelixis, Farm2Fork Industry

KER7. Secure Infrastructure Abstraction (SIA)



NETWORK FUNCTION ORCHESTRATION

OSM-enabled network function orchestration



VIRTUALIZATION ENVIRONMENTS SUPPORT

Able to support virtualization environments based on VMs (OpenStack) and containers (Kubernetes)



SECURE MULTI-DOMAIN CONNECTIVITY

Secure multi-domain connectivity relaying on IPsec

The connectivity patterns and the North-bound interfaces are designed to support the specific needs inherent to the heterogeneous and diverse supply chain scenario also supporting the hybrid model FISHY is envisioned to support. SIA is fully open source and its functionality includes standardised API for network infrastructure abstraction supporting a consistent connectivity framework, based on a virtual distributed switch.

Commercial Opportunities:

- Support for installation and maintenance.
- Extension to hybrid cloud environments.
- Support to address special deployments.

The module is part of the securitisation of services, facial identity management and certified version management in vehicles. Communication will be done in a secure way through the NED, which will allow restrictions or configurations to be applied if intrusions or risks are detected in the vehicle.

Capgemini

6. What are the **Success Stories**

FISHY early adopters: Securing Autonomous Driving Function at the Edge



The connected cars use case SADE was able to leverage FISHY innovation to ensure the identification of SW Certifications of Components Vehicle. This allowed getting a connection model between manufacturers and vehicles connected, while getting integration with XL-SIEM, a FISHY tool for on-live monitoring of service' logs. This tool allowed also to prevent security issues related with car access and traffic tampering attacks.

1. Significant improvement in safety car because logs and certifications monitoring, difficult to estimate the % by comparing current situation
2. **100%** improvement in knowledge version SW in vehicles and versions certificated by manufacturers
3. Significant reduction in risk attack cars because SW no validated or with unknown errors
4. **80%** achievement FISHY integration on premises and EDGE

The connected car industry is concerned about the cybersecurity posture of automotive technologies provided by third parties, but also about the cybersecurity posture of the industry as a whole.

The expectations

- the FISHY Platform will be an entry point for users and will centralise certain security aspects of the supply chain of software versions of IoT devices embedded in vehicles. It will also enable the management of in-vehicle user identities and facial identities. The platform is expected to have appropriate forms for the management of this data.

The benefits

- automatic generation of events and alarms by reading logs that improve the knowledge of the different actors in the supply chain in case of issue/attack. With this information they will be able to apply mitigation measures (software updates, car deactivation, car blocked)
- on-live add/revoke software certificates by manufacturers
- continuous monitoring of the software certificates deployed in each vehicle, allowing rapid detection of vehicles with revoked certificates and/or camouflaged malware
- role-based access control using centralized FISHY DASHBOARD and SPI for all the suppliers (multi-user for one on-premise cloud, not multi-tenancy for multiple clouds).

The limitations:

- the integration of on-premise environment requires some adaptations that requires high effort
- the automatic reaction to alarms for SADE requires a customized interaction with the central repository
- multi-owner cloud is not included in this version, which implies the limitation to only one cloud owner (a car manufacturer cloud). Multi-user for this cloud if it was considered.

For most organizations, supply chain disruption is seen as the top risk to business growth, ahead of rising commodity prices and the energy crisis. The automotive industry's complex and disparate supply chain is a major culprit in causing quality problems.

FISHY early adopters: Farm-to-Fork Supply Chain



This use case is responsible for the mitigation of five different attacks of different types: brute force attack, network analysis attack, compromised device (wallet ID level and DID level), blockchain node attack, machine-learning based attack detection at endpoint.

In this scenario, FISHY allows for the reduction in downtime (this cannot be calculated but given that **62%** of supply chain attacks exploit the trust of client to their supplier and that **58%** of attacks aim at accessing data, it is obvious that as FISHY protects against these two categories of attacks significantly reduces the downtime).

The expectations

- the FISHY platform needs to support the administrators of the IT systems of the three type of actors of the F2F chain to monitor the security of the IoT solution they operate in a flexible and credible way, supporting also blockchain-relevant trust/security management

The benefits

- protect against multiple types of attacks and minimize down-time
- be able to confirm/certify the absence of attacks or the types of attacks that occurred (e.g. through blockchain based evidence)
- the flexibility of deployment and the flexibility in the way attacks are detected based on logs or traffic analysis or embracing machine learning techniques is very important to ensure the continuous update of the attacks that can be detected and mitigated.

The limitations:

- the current version of the FISHY platform does not offer an intuitive interface for managing the reconfiguration of the IT systems (e.g. introduction of new devices)

Many providers of supply chain-oriented IT platforms are interested in offering a solution that offers enhanced reliability and availability. The FISHY user can request and receive the outcomes of the cyber-security monitoring process (from assessment to mitigation) for the platform he is responsible for and also request a certificate for the platform he operates as a whole or for subsystems. The FISHY user can also access the FISHY dashboard and have the results of the monitoring process visualized.

FISHY early adopters: Wood-based Panels Trusted Value Chain



There was no implemented system for automatic detection of rogue IoT devices. Implementing a system that can successfully identify rogue IoT devices provides a significant improvement in cybersecurity by detecting unauthorized and potentially malicious devices within the network.

1. Automated identification of rogue IoT devices reducing cybersecurity effort by detecting unauthorized and potentially malicious devices within the network.
2. IoT network traffic monitoring improves the threat identification.
3. Recommendations for action in EDI communication attacks reduce impact

Also, there was no control over IoT network traffic, and the standard behaviors were unknown, making it difficult to interpret deviations as potential tampering or deliberate attacks (**100%** improvement). Implementing network traffic monitoring for IoT devices enhances visibility

and allows for the identification of abnormal or suspicious patterns, enhancing the overall security posture.

Moreover, there were no active recommendations in place for handling attacks on electronic data interchange (EDI) communications. Establishing proactive recommendations, such as identifying attack IPs or diverting communication to honeypots, enables a more effective response to EDI communication attacks, reducing the impact and potential compromise of sensitive data.

The expectations

- The FISHY Platform should centralize the management of users, including different user profiles, and support system's administrators in their responsibility of monitoring the security of the IoT devices and systems they operate.

The benefits

- automated identification of rogue IoTs reducing cybersecurity effort by detecting unauthorized and potentially malicious devices within the network;
- IoT network traffic monitoring improves the threat identification;
- recommendations for action in electronic data interchange communication attacks reduces impact potential.

The limitations:

- the addition and configuration of new devices to the current version of the FISHY platform is not centralized in the dashboard

FISHY is a trustworthy and flexible solution in cybersecurity for smart factories. By providing a coordinated framework for advanced security assurance tools, certification methodologies and traceability systems, FISHY empowers organizations to safeguard their ICT supply chains, protect against risks, and drive resilience in an ever-evolving threat landscape, bolstering security, trust, and privacy in the industrial sector.

8. Who are we

The FISHY consortium is composed of experts in different technical areas, with special focus in cybersecurity and supply chain. The project is based in designing and developing innovative solutions that can be intergrated naturally in the supply chain infrastructure, covering the whole life cycle and different elements/characteristics of these systems. The FISHY platform will be a central element for industry organizations that will be able to analyze and identify early threats, vulnerabilities, and the impact of cascading effects in the whole system. Finally, trust and assurance is a key pillar of the project so organizations using FISHY will be able to provide these aspects to their clients, which are also an important aspect of the project.



Project duration

1.9.2020 - 31.8.2023



Project manager

Antonio Alvarez Romero, Eviden
antonio.alvarez@eviden.com



Dissemination manager

Eva Marin, UPC
eva@ac.upc.edu



POLITECNICO DI TORINO

Technical manager

Xavi Masip, UPC
xmasip@ac.upc.edu



Innovation manager

Joao Costa, XLAB
joao.pitacosta@xlab.si



fishy-project.eu



[@fishy-project](https://www.linkedin.com/company/fishy-project)



[@H2020Fishy](https://twitter.com/H2020Fishy)



FISHY H2020



This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 952644