# Unveiling the Cybersecurity Tapestry: Safeguarding Supply Chains with an Innovative Resilience Approach

Supply chains are extremely delicate systems, integrated by heterogeneous components which are distributed in different domains and realms. Being so complex, they are working on daily basis under very demanding requirements, especially in terms of responsiveness. If supply chains do not work properly, our welfare status and quality of life are under risk. They are extremely critical and, at the same time, as they have become more and more complex the attack surface for cyber criminals has become larger and larger.
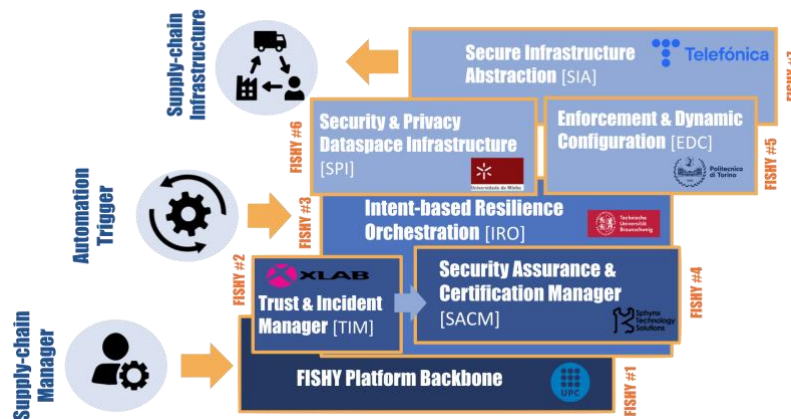
Securing and shielding supply chains from end to end has become an exciting journey, with intense research and development work taking place all over the world. In this context, the European Commission funded the FISHY Project which came to bring its contribution with a huge effort during these last three years. A group of European Institutions got together to imagine the future, to envision how things could be done in order to enhance supply chains preparedness against cyber-attacks.

During these three years the FISHY Consortium has built a flexible and resourceful platform that considers all the supply chain components, addressing the complex problems of the IoT layer in terms of security, as well as protecting the edge and cloud layers that pose their specific challenges, too. Starting with a horizontal approach to the challenge and taking as reference the top well-known cyber-attacks, the Project made the most of the opportunity given for experimentation by the three specific supply chains involved belonging to the food industry, smart manufacturing and connected automotive sector, and made research to identify the main nightmare attacks per vertical, tailoring the solution to their specific needs.

FISHY has offered a combination of highly innovative functionalities to move the protection of the supply chains to the next level. The open source FISHY functionality, which includes most of the technologies developed in the lifetime of the project, is available at https://fishy-project.eu/open-fishy as the Open FISHY initiative. FISHY has covered the whole cycle of cybersecurity, from the detection to the application of countermeasures.

It starts with the deployment of diverse data collectors gathering a set of relevant metrics about the activity in the supply chain. This data is used at a higher intelligence layer in which different monitoring techniques have been applied, performing analysis, raising alerts and eventually proposing mitigation actions, experiencing with trustworthy collaboration mechanisms among stakeholders. In this area the results have been very satisfactory, with enhanced detection capabilities adapted to each single supply chain. FISHY also uses this knowledge to carry out a security assurance and certification process which involves both auditing and reasoning stages, relying on the collection and usage of certifiable evidence.

But it is not only about knowing what is abnormal in a supply chain and why it is happening, with the identification of the incident. It is also important to know how to react. In this sense FISHY has made research on the (semi) automation of responses leveraging intent-based networking techniques. FISHY has explored the definition of security policies by means of intents that use close-to-human language. The value is double, on one side the definition of policies to be applied in certain cyber risk scenarios is eased thanks to the intuitive and easy-to-learn language used in the process of creating such policies, while on the other hand FISHY sets the ground for (semi) automatic reconfiguration of the supply chain to mitigate the effects of attacks. By using predefined policies, FISHY can react to detected threats automatically or after confirmation from the user, and enforce security rules.

As a foundation for the platform, the FISHY Consortium has managed to establish a solid connectivity pattern that, on one side, can cope with a very wide range of needs posed by the supply chains and, on the other hand, allowing for great flexibility when it comes to deploying FISHY on a specific client infrastructure and is definitely a differentiator and a winner point in order to commercialize the platform.

Finally, FISHY has established the basis for an end-to-end protection of supply chains that is also fully compliant with GDPR and fully able to meet demanding privacy requirements.

From the human perspective, along with the joy for the satisfactory technical results, we feel fortunate for having had the chance to work together during these three years. FISHY has given us the opportunity to meet an excellent team of professional and nice people, always willing to lend a helping hand especially in the most complex tasks. FISHY has been a team of skilled people coming from industry and academia, with long experience and starting their careers, managers and technicians, with different cultural backgrounds. At the beginning of the project, with the pandemic hitting the world, we must say it was difficult. We had to work with the worrisome of the global developments and with the difficulty of the 100% online interaction. Despite all difficulties, we obtained positive feedback in two evaluations with the European Commission in October 2021 and May 2022 and then, some months later, at last the travel restrictions were lifted and we had the chance to meet together for the first time in October 2022 and later two more times April and June 2023. Sevilla, Vilanova I La Geltrú and Porto will be in our memories with great moments spent together. We wish we had had the chance to visit all the countries and cities represented in the Consortium. It goes without saying that the face-to-face interaction had a strong positive effect and the project geared up during its last months.

Everyone has learnt a lot from the others and very likely we are now better than before the project. To me, as coordinator, it was a honor and a pleasure to coordinate the team and work with each one its members. I definitely hope for new opportunities to collaborate in the future.

I cannot finish without showing gratitude to the European Commission for giving us the opportunity to carry out this project, for trusting this Consortium and for their support in the management of the project during this time.

Antonio Álvarez Romero

FISHY Project Coordinator