LSP#3 Overview:

- CXB is the leading beneficiary for the Large-Scale Pilot #3 (LSP#3) and coordinates the development of the different use cases involved in the financial pilot.

- LSP#3 focuses on increasing cybersecurity awareness and resilience among CIs within the financial sector across Spain and Germany. This LSP involve banking institutions that have a very large and complex CIs, which should robust, constantly evolving and follows many regulatory guidelines and strict security frameworks. Also, the Pilot counts with researchers that engage in economic and financial analysis to safeguard the asset in marketplace and expose disinformation campaigns.

Each organization faces unique challenges based on their processes, capabilities, and the threats they encounter. LSP#3 goals involve identifying specific hazards and threats, analysing operations to document interdependencies, and identifying and calculate risks based on detected alerts and trends in a real-time environment. Therefore, giving information to the end-users to better understand and make decisions based on real-time information and risk score.

- To accomplish the hole objective of the Pilot, LSP#3 divides in 3 main use cases that each aim towards a specific aim:

Use case 3.1, aims to test the resiliency of the Critical Infrastructure (CI) of JRC by simulating a real-life scenario of threat vs opportunity detection of dis/mis/mal-information through the consumption of data and content from social media, news sources (sites, blogs, podcasts transcripts, video posts etc) that traders and customers of JRC are visiting -following on a daily basis not only to ensure the integrity of JRC's investment ecosystem but also to provide traders and clients with timely and accurate information for making investment decisions, especially in the cryptocurrency market, given the volatile cryptocurrency landscape.

Use case 3.2, aims to establish a near real-time risk reporting solution in response to cyber-attacks targeting bank systems and operations (focusing mainly on the network intrusion threat and potential linked attacks or consequences derived from the attack). The solution will leverage Cyber Threat Intelligence (CTI) information and logs from CXB's Security Information and Event Management (SIEM) system to promptly identify, assess, and report risks and their criticality. By doing so, the developed tool will provide CXB with a comprehensive view of potential threats, vulnerabilities, and malicious activities, enabling proactive risk management and mitigation strategies that can be later implemented by SOAR or recommended playbooks for the analysts.

Use case 3.3, aims to detect spoofing and DoS attacks against PNT services, generally provided by GNSS. Considering the financial sector, the use case focuses on timing. Detecting this type of attacks is essential to start mitigation actions promptly and reduce possible problems and complications that derive from time desynchronization such as data corruption and service denial, legal actions, and regulatory compliance.

Key Contributions:

- LSP#3 main focus is on Artificial Intelligence (AI) applied in cybersecurity resilience. Meaning that this Pilot aims to use AI tools in order to improve cybersecurity resilience by enhancing a better understanding of the risks involving a financial entity or sector. Furthermore, LSP#3 dives into the detection of spoofing attacks to PTN services via GNSS to mitigate possible consequences regarding time dyssynchronization.

- LSP#3 will develop a new method of risk management involving interdependencies between assets to be aware of possible lateral movements and visibility from the point of view of a potential attacker and correlate risks and new vulnerabilities with the corporative SIEM logs to update the risk level and adapt it to reality.
- The tools involved in this LSP which use AI are:

1. Truly Media, which uses AI engines to detect Deepfakes, Disinformation Campaigns and possible frauds.
2. SAFER, which together with the Decision Support System (DSS) will catalogue and create the risk assessment of emerging threats and incidents.
3. RRIM, the intelligent Risk Reduction Incident Mitigation system counter-measuring recommendations for the different risks.

Consortium of Companies

Engineering
Ingegneria Informatica S.p.A.
[Italy]

CS Group
[France]

SIXENSE ENGINEERING
[France]

Netcompany-Intrasoft
[Luxembourg]

SingularLogic
[Greece]

Telekom Slovenije d.d.
[Slovenia]

SIEMENS AG
[Romania]

Synelixis Solutions S.A.
[Greece]

NetU Consultants Ltd.
[Cyprus]

Byte computer S.A.
[Greece]

Sneep Asset Management d.o.o.
[Slovenia]

Athens Technology Center S.A.
[Greece]

Cybercrime Research Institute GmbH
[Germany]

Luka Koper
[Slovenia]

Port of Rijeka Authority
[Croatia]

DARS
[Slovenia]

Slovenske Železnice
[Slovenia]

Petrol d.d.
[Slovenia]

Ferrovie dello Stato Technology S.A.
[Italy]

JRC Capital Management
[Germany]

CaixaBank S.A.
[Spain]

Hygeia
[Greece]

SITAF S.p.A.
[Italy]

Service Départemental d'Incendie et de Secours de la Savoie
[France]

KEMEA – Centre for Security Studies
[Greece]

Institute for Corporative Security Studies, ICS
Ljubljana
[Slovenia]

European Union Satellite Centre
[Spain]

University of Rijeka,
Faculty of Maritime Studies
[Croatia]

Josef Stefan Institute
[Slovenia]

CEA List Institute
[France]

Centre of Research & Technology Hellas
(CERTH)
[Greece]

Links Foundation
[Italy]

Vicomtech Foundation
[Spain]

Ministero Dell' Interno, Dipartimento di
Pubblica Sicurezza, Polizia di Stato
[Italy]

Ministry of Infrastructure
of the Republic of Slovenia
[Slovenia]

Republic of Slovenia,
Government Information Security Office
[Slovenia]

Ministry of Citizen Protection,
Hellenic Police
[Greece]

This project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909

ATLANTIS

Contact us

Project Coordinator
Mr. Gabriele Giunta
Engineering, Italy
gabriele.giunta@eng.it

Technical Manager
Mr. Artemis Voulkidis
Synelix, Greece
voulkidis@synelix.com

Web

LinkedIn

www.atlantis-horizon.eu

ATLANTIS

LSP#3:
"Cross-Country Large-Scale Pilot in FinTech/Financial"