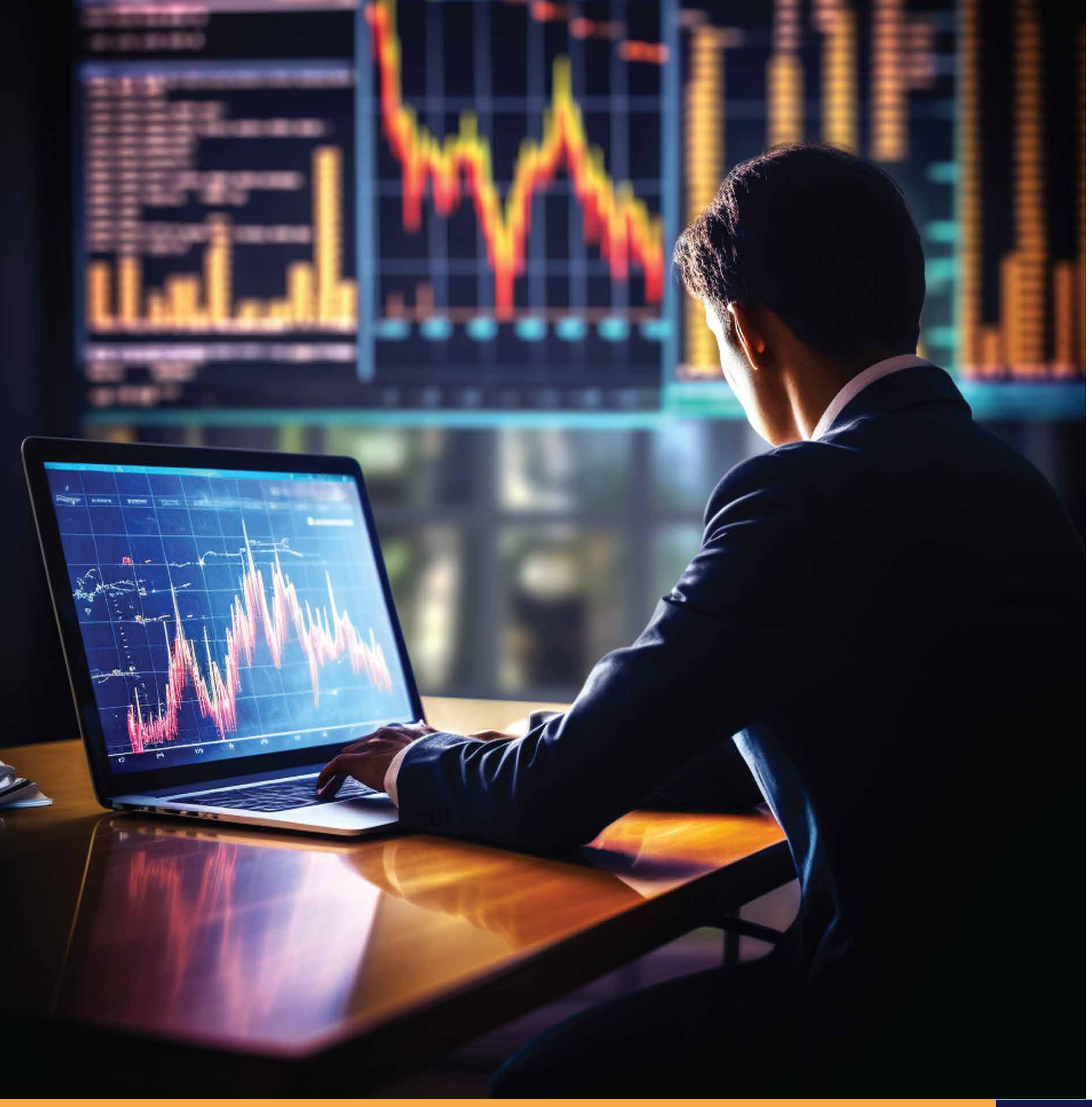

ATLANTIS

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

www.atlantis-horizon.eu

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 LSP counts with researchers that engage in economic and financial analysis to safeguard the asset in marketplace and expose disinformation campaigns.

Challenges:
- Unique to each organization's processes, capabilities, and threats.

LSP#3 Goals:
- Identify hazards and threats.
- Analyze operations and interdependencies.
- Calculate risks from real-time alerts and trends.

End-User Impact:
- Provides real-time info and risk scores for better decision-making.

Objective of LSP#3:

Divided into three main use cases, each targeting a specific aim.

Use Case 3.1:
- **Focus:** Test resiliency of JRC's Critical Infrastructure (CI).
- **Scenario:** Simulates detection of dis/mis/mal-information by monitoring social media, news sources (blogs, podcasts, videos, etc.) frequently visited by JRC traders and customers.
- **Goals:**
  - Ensure integrity of JRC's investment ecosystem.
  - Provide traders and clients with timely, accurate information for investment decisions.
  - Support decision-making in the cryptocurrency market, given its volatility.

Use Case 3.2:
- **Focus:** Establish near real-time risk reporting for cyber-attacks targeting bank systems.
- Threats Monitored: Primarily network intrusion and linked attack consequences.
- **Solution Features:**
  - Uses Cyber Threat Intelligence (CTI) and data from CXB's SIEM system.
  - Identifies, assesses, and reports on risk levels and criticality.
- **Outcome:**
  - Provides CXB with a comprehensive view of threats, vulnerabilities, and malicious activities.
  - Supports proactive risk management and mitigation through SOAR or recommended analyst playbooks.

Use Case 3.3:
- **Focus:** Detect spoofing and DoS attacks on PNT services (mainly GNSS) in the financial sector.
- **Importance:** Timely detection is crucial to mitigate risks related to timing desynchronization.
- **Potential Issues Prevented:**
  - Data corruption, service denial, legal actions, and regulatory compliance issues.

Key Contributions:

- LSP#3 main focus is on Artificial Intelligence (AI) applied in cybersecurity resilience. Meaning that this LSP 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]

European Union Satellite Centre
[Spain]

CaixaBank S.A.
[Spain]

Links Foundation
[Italy]

Ministry of Citizen Protection,
Hellenic Police
[Greece]

SingularLogic
[Greece]

Telekom Slovenije d.d.
[Slovenia]

SIEMENS AG
[Romania]

Synelix Solutions S.A.
[Greece]

Vicomtech Foundation
[Spain]

CEA List Institute
[France]

Institute for Corporative Security Studies, ICS
Ljubljana
[Slovenia]

NetU Consultants Ltd.
[Cyprus]

Byte computer S.A.
[Greece]

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

Athens Technology Center S.A.
[Greece]

SITAF S.p.A.
[Italy]

Jozef Stefan Institute
[Slovenia]

JRC Capital Management
[Germany]

Ferrovie dello Stato Technology S.A.
[Italy]

Cybercrime Research Institute GmbH
[Germany]

Luka Koper
[Slovenia]

Port of Rijeka Authority
[Croatia]

DARS
[Slovenia]

Hygeia
[Greece]

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

KEMEA – Centre for Security Studies
[Greece]

Slovenske Železnice
[Slovenia]

Petrol d.d.
[Slovenia]

Republic of Slovenia,
Government Information Security Office
[Slovenia]

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

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

Ministry of Infrastructure
of the Republic of Slovenia
[Slovenia]

University of Rijeka,
Faculty of Maritime Studies
[Croatia]

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

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

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

Web

LinkedIn