EAP Workshop 9th February 2022

“CONCORDIA and the importance of information sharing for the future of the European Cybersecurity Ecosystem”

Mario Maawad Marcos, CAIXABANK
(mmawad@caixabank.com)
Threat Intelligence Information Sharing needs in the Financial Services sector

The digital transformation and technological development bring with them new **cyber-threats and risks** in the **financial sector** but...

*Are you seeing the whole elephant?*
Threat Intelligence Information Sharing needs in the Financial Services sector

• The scale and complexity of these cyber-threats require organizations to collaborate to help build resilience and leads to collective action.

What makes Cyber-Threat Intelligence in Financial Services special?

• Cyber-Threat Intelligence (CTI) sharing allows banks and CERTs react and properly respond to:
  • Potential cybersecurity attacks.
  • Financial fraud & crime information.
Threat Intelligence Information Sharing needs in the Financial Services sector

Is it a potential phishing?
Is it part of a ransomware?

Is this customer trustworthy?
Is this transaction fraudulent?

EAP Workshop:
“CONCORDIA and the importance of information sharing for the future of the European Cybersecurity Ecosystem”
Threat Intelligence Information Sharing needs in the Financial Services sector

*From Data to Intelligence*

High volume of data needs to be stored, processed, analysed and used to react.

*We need to automate it*

Heterogeneous data, formats and sources, even regulation.

EAP Workshop:
“CONCORDIA and the importance of information sharing for the future of the European Cybersecurity Ecosystem”
Threat Intelligence Information Sharing needs in the Financial Services sector

*Do you trust me?*

Financial institutions save very sensitive information and are especially reluctant to share data.

*How can we built something that those stakeholders trust and engage with?*

Even if we trust you...

*Should we trust your data?*

---

EAP Workshop:
“CONCORDIA and the importance of information sharing for the future of the European Cybersecurity Ecosystem”
Threat Intelligence Information Sharing needs in the Financial Services sector

**Threat Information Platforms (TIPs)** are proposed to enable CTI sharing among involved financial entities.

*Who will manage it?*

- Centralised or distributed control?
- Role-based control at entity level?
- Federated authentication?
- Specific and granular sharing groups?
Threat Intelligence Information Sharing needs in the Financial Services sector

- Build more secure financial institutions:
  - Secure our infrastructure.
  - Secure our clients.
  - Build on collaborative experience and knowledge:
    - More data → more secure.
    - Identify earlier and react faster.
- Be a player in the threat intelligence market:
  - Potential additional revenues.

- Trust
- Heterogeneity
- Data sensitivity
- Highly regulated sector
- Data volume

CONCORDIA Survey – Value and Benefits of CTI information sharing:
https://ec.europa.eu/eusurvey/runner/CONCORDIA_CTISurvey2021
Financial Threat Intelligence Platform

- Cyberthreat information sharing in finance sector
  - Infrastructure and financial fraud threats
- Define additional specific formats for banks
- Data sharing policies and GDPR is a critical aspect for financial entities
- Financial entities want to share data but have several constraints
Financial Threat Intelligence Platform

EAP Workshop:
“CONCORDIA and the importance of information sharing for the future of the European Cybersecurity Ecosystem”
Financial Threat Intelligence Platform

- Information Exchange Policies based on standards such as TLP, IEP 2.0 FIRST, etc.
- Encrypted information – access granted only to the shared person
- Shared information's access based on organisation, role, user and time, tailored constrains
Financial Threat Intelligence Platform

• Data-centric security approach
• Control with whom and how the CTI information is shared
  • Roles
  • Users
  • Organizations
  • Time
  • ...
• Information is protected and can only be accessed by allowed entities
Financial Threat Intelligence Platform

Share Threat Intelligence

- Incident Date: 03/02/2021
- Critical financial information
- File attachment: Financial Fraud Information.txt
- To whom: alejandro
- From Date: 03/02/2021
- Until Date: 06/02/2021
- Event UUID
- Share

EAP Workshop:
“CONCORDIA and the importance of information sharing for the future of the European Cybersecurity Ecosystem”