Financial Pilot: Assessing Cyber Risks and Threat Intelligence for the Finance Sector

Ramon Martín de Pozuelo, CAIXABANK
(rmartindepozuelo@caixabank.com)
Jose Francisco Ruiz, Esteban Armas, Atos
([josefrancisco.ruiz][esteban.armas.external]@atos.net)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Threat Intelligence Challenges and Opportunities in Financial 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 Challenges and Opportunities in Financial Sector

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

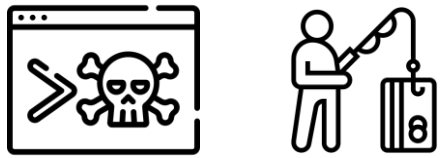
What makes Cyber-Threat Intelligence in Financial Services special?

- Cyber-Threat Intelligence (CTI) sharing allows banks and CERTs react and properly respond to:
  - Potential cybersecurity attacks.
  - Financial fraud & crime information.

Threat Intelligence Challenges and Opportunities in Financial Sector

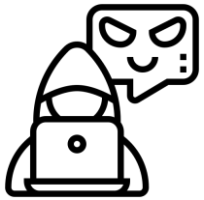
Is it a potential phishing?

Is it part of a ransomware?



Is this customer trustworthy?

Is this transaction fraudulent?

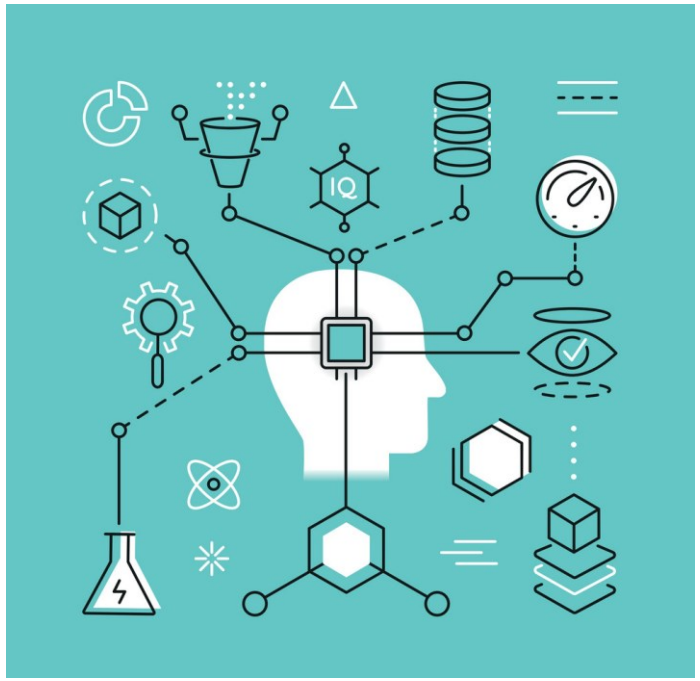


Threat Intelligence Challenges and Opportunities in Financial Sector

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.

Threat Intelligence Challenges and Opportunities in Financial 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?

Threat Intelligence Challenges and Opportunities in Financial Sector

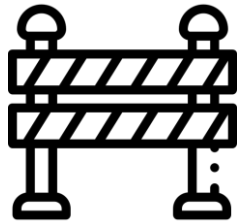
Threat Information Platforms (TIPs) are proposed to enable CTI sharing among involved financial entities.

Who will manage it?

- Centralised or distributed control?
- Role-based control at entity level?
- Federated authentication?
- Specific and granular sharing groups?

Threat Intelligence Challenges and Opportunities in Financial 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.



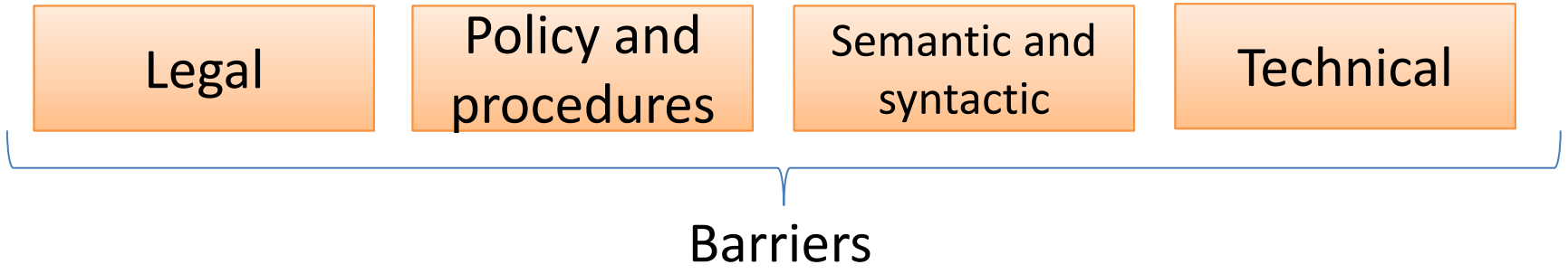
- Trust
- Heterogeneity
- Data sensitivity
- Highly regulated sector
- Data volume

Cyber-Threat Information Interoperability

- CTI can be defined as “any information that can help an organization to identify, assess, monitor and respond to cyber threats”
- The type of information that is shared includes, among others:
  - Log entries and alerts
  - Measurable actions
  - Identified vulnerabilities
- Number of CTI sources is increasingly yearly as do the number of tools that can consume the data
- Information sharing uses multiple actors, ranging from public institutions to industry-focused groups

Cyber-Threat Information Interoperability

- What is the final goal?
  - To share and process information automatically
- Why can't we share easily and open between us all?
  - What information is shared, how it is shared and legal issues (globalization)
- From the technical point of view there is not a single approach for sharing data due to multiple technical standards, policies, etc.



Cyber-Threat Information Interoperability

- One objective, several ways to achieve it
- We are moving from static and independent approaches to a distributed European one
- EC aims to have an European network for information sharing
- Benefits public and private organizations
- Protects against known and unknown attacks

Cyber-Threat Information Interoperability

- CTI allows for entities to react better to zero-day attacks, APT, etc.
- The more information is shared, the more prepared against cyberattacks
- Data of financial institutions is sensible, so a solution that can support data security and privacy needs is mandatory
- Support of policies at European, national and company level
- Need for tools for managing with whom and how information is shared

Cyber-Threat Information Interoperability

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

- The scale and complexity of these cyber-threats require financial organizations **to collaborate to helps build resilience and leads to collective action**

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

Cyber-Threat Intelligence (CTI) sharing allows banks and CERTs react and properly respond to potential cybersecurity attacks (e.g. phishing sites, malware campaigns, 0-day vulnerabilities or OSINT reports regarding the financial sector)

Demo