Collaborative Risk Assessment for Interconnected Critical Infrastructures of the Finance Sector

H2020 FINSEC Project

John Soldatos

The FINSEC project is co-funded from the European Union's Horizon 2020 programme under grant Agreement No 786727

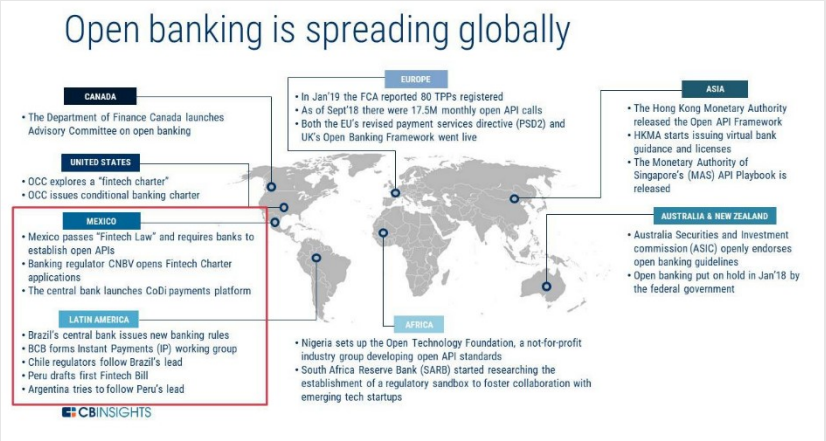
Background & Motivation

Stakeholders & Critical Infrastructures of the Finance Sector are densely Interconnected

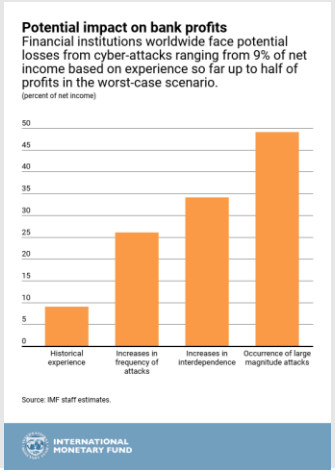
- Financial Supply Chain Services (e.g., SWIFT/SEPA Transactions, Trading)
- PSD2 & Open Banking increase the number of interconnected (supply chain) services
- Security Incidents on one organization can impact interconnected organizations (incl. possible cascading effects)

Critical Infrastructures in Finance are large scale Cyber-Physical Systems

- Cyber Assets (e.g., networks, computers, software systems)
- Physical Assets (e.g., buildings, data centres, ATM devices)
- Cyber-Physical Interconnection



9% of Profits at Risk due to Cyber-Attacks (source: IMF)



Challenges to Protecting Interconnected Cyber-Physical Systems in the Finance Sector

Integrating Information and Actions at Cyber & Physical Domains

- Cyber & Physical Security are still “siloed” – Organizational & Technical Silos
- Need for Integrated Modelling and Handling of Information
- Cyber-Physical Threat Intelligence i.e. the Core Topic of FINSEC Project

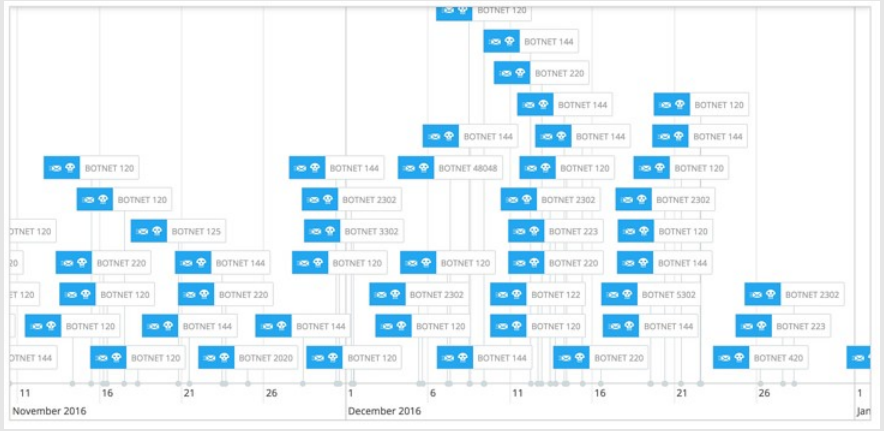
Poor Stakeholders’ Collaboration

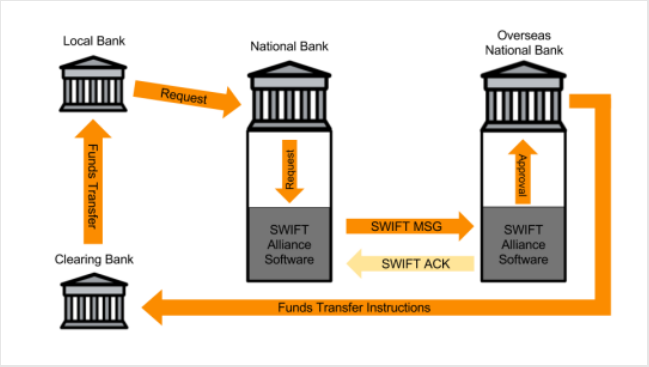
- Limited Sharing of Information across Stakeholders
- Limited Exploitation of Shared Information

Lack of Collaboration is a Source of Prominent Attacks

Dridex Malware Attacks end-up Establishing Botnets across different financial organizations (>=20 million GBP losses)

2016 attack against the SWIFT Network in Bangladesh Central Bank (>=$81 million losses)





Best Practices & Lessons Learnt for Stakeholders' Collaboration

Increase the frequency of information exchange between financial organizations

- Especially organizations participating in the joint delivery of financial services

Automate the process of information exchange based on software systems

- Including the exchange of cyber-physical information

Automate the processing and analysis of the exchanged information towards automatically extracting insights

- Suspicious behaviours, anomalies and other indicators of security incidents

Implement systems for the trusted and controlled exchange of information

- Financial organizations want to avoid sharing information that could compromise their reputation and create brand damage.

Information Sharing is a Key for Stakeholders Collaboration – Information Sharing in FINSEC

Information Sharing a Pre-Requisite for Collaboration

- ISAC Information Sharing & Analysis Centers
- Example: FS-ISAC for Financial Services

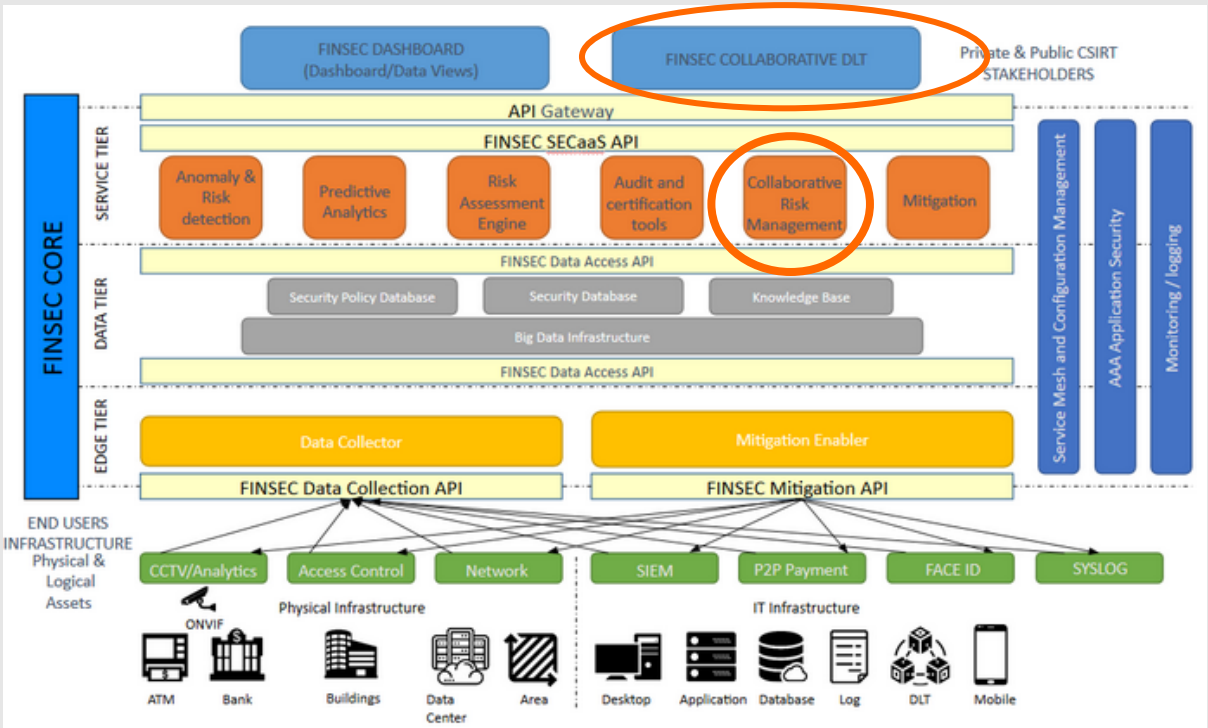
Limitations

- Limited to Cyber Security Information Sharing
- Centralized Approach

FINSEC Value Propositions

- Decentralized Approach
- Integrated Cyber-Physical Information Sharing

Information Sharing for Supply Chain Services in the FINSEC Reference Architecture



Advantages of a Decentralized approach (aka Blockchain-based implementation)

Decentralized Trust – Easier for Organizations to Share Incidents and Events

- Reputation Damage is always a major concern

No Single Point of Failure

- Lack of a Centralized Database that can be Compromised

Confidentiality, Integrity and Availability Properties

- Inherent in a Blockchain-Network

Anti-Tampering Properties

- Auditability & Transparency

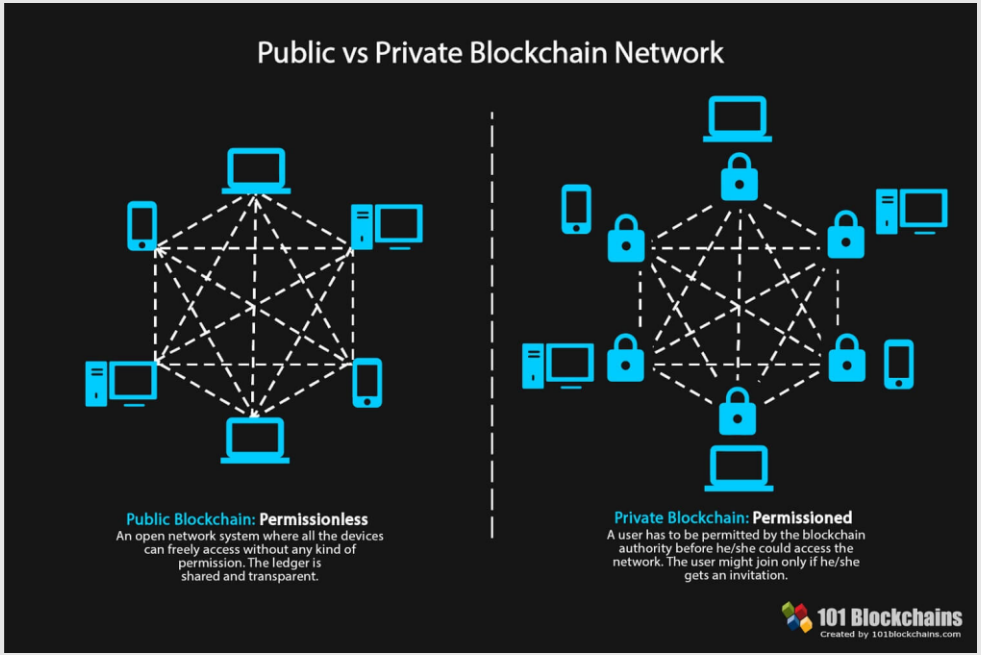
Alleviating the Drawbacks of a Blockchain Implementation

Alleviating the Performance Penalty

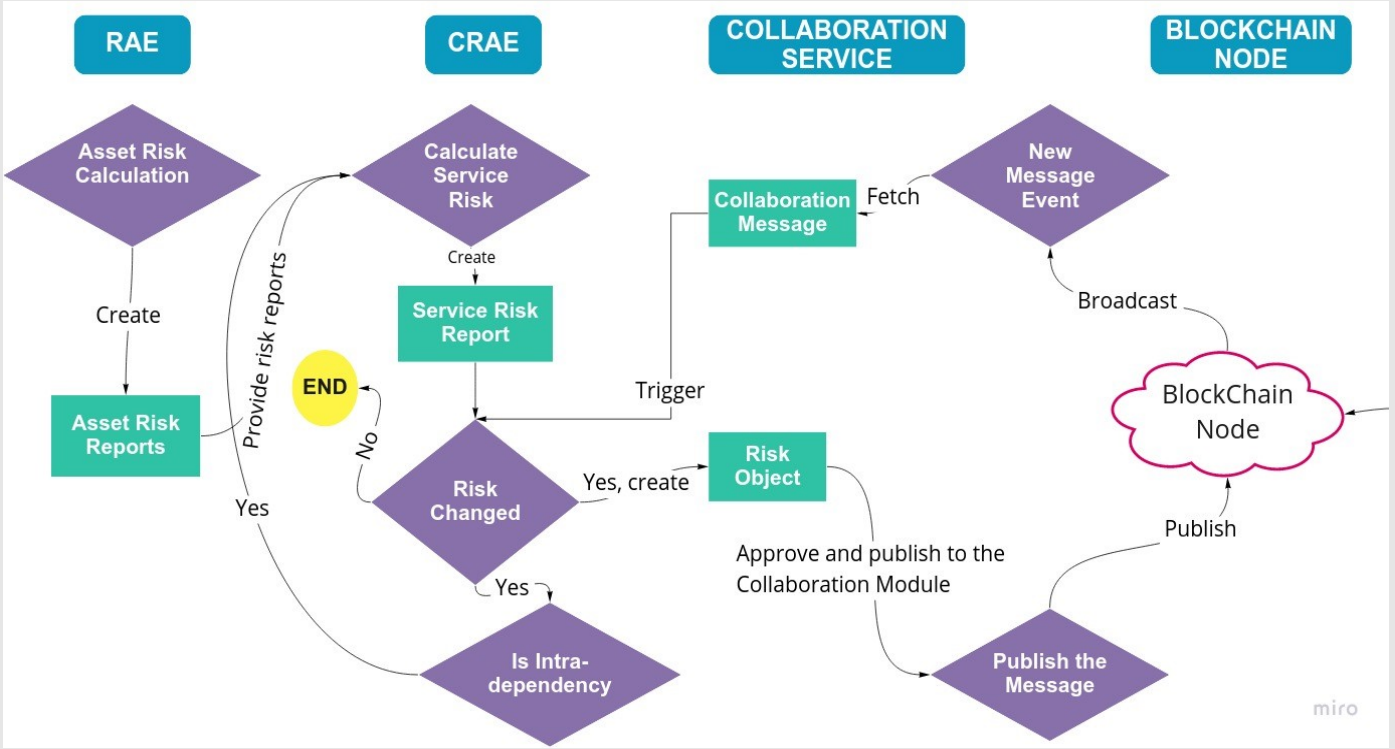
- Permissioned Blockchain
- No Computationally Demanding PoW (Proof-of-Work) Processes
- Some 1000s TPS (Transactions Per Second)

Privacy Control – User Authentication & Authorization

- Permissioned Network



Information Sharing and Collaborative Risk Assessment Engine (CRAE)



Collaborative Risk Assessment: Risk Calculation

Risk Metrics

- Provided at different levels
- Vulnerability level
- Impact level
- Threat level

Vulnerability and Impact levels

- CVSS (Common Vulnerability Scoring System)
- Assignment of severity scores to vulnerabilities
- Allow Responders to prioritize responses and resources according to threat
- Derived from the CVSS scores of the assets' vulnerabilities detected

Threat level

- Events occurring inside the organization
- Historical information

Risk Calculation Services

Initialization	Creation of a Service to initialize risk calculation suite
Storage	1) Services are stored in the FINSEC data-tier; 2) Data tier is protected using basic authentication
Asset selection and Vulnerability Definition	1) Performed for each asset 2) Takes places in conjunction with the Security Knowledge Base

Threats Specification

Threats that may target the service

List of events that should be defined

Events affect the level of the threat in real-time

Threats are associated with the Risk Service

Threat objects must be stored in the Security Knowledge Base

The Role of Events

Security officer needs to define event models and then map them to a predefined threat

- Example: “invalid login attempt” can be related to a “SWIFT compromise threat”

Instances of this model detected through Probes the platform detects it

If the trigger value is reached for this specific event the overall risk of the related threat is re-calculated

Risk calculations Service

Service to function properly, certain preconditions need to apply

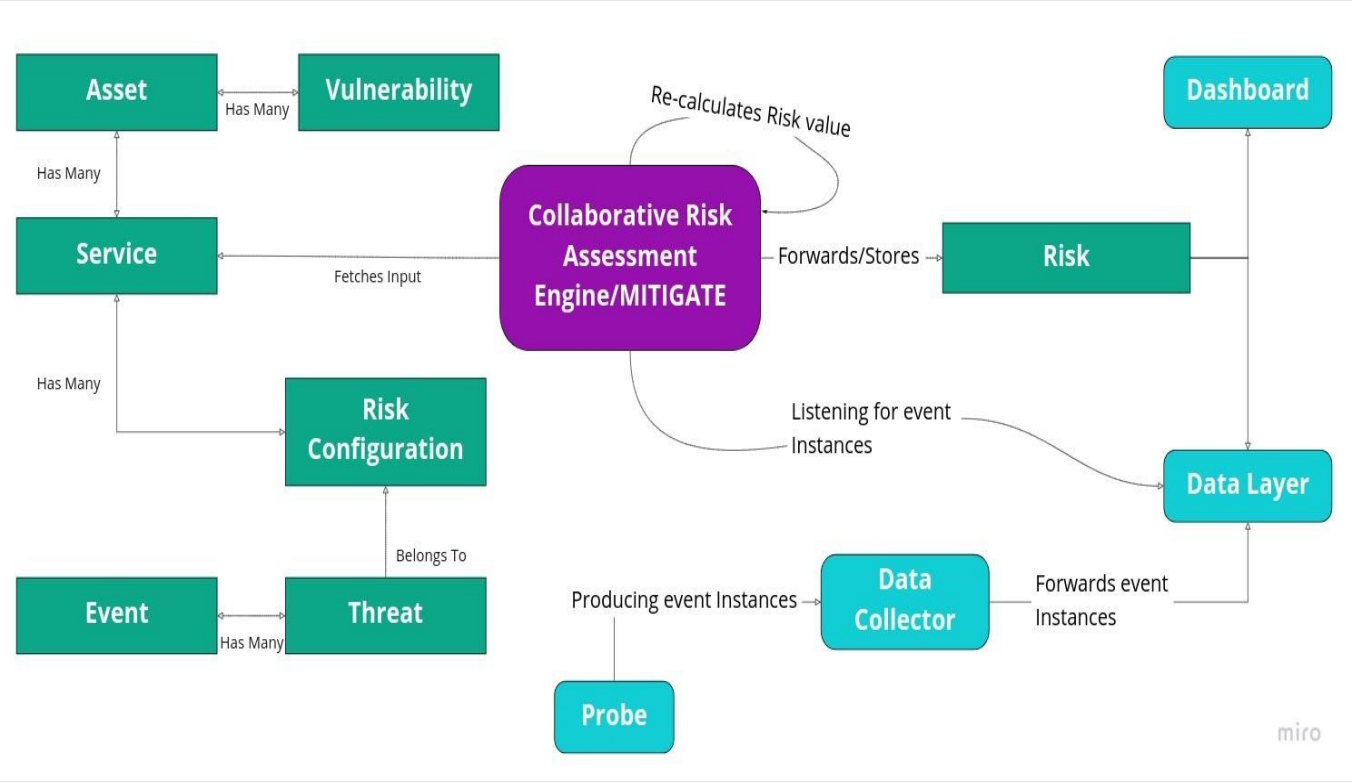
Service definition, the threat to event mapping and the probe to be up and running

Probe produces a new event which is forwarded through the data collector to the FINSEC data-layer

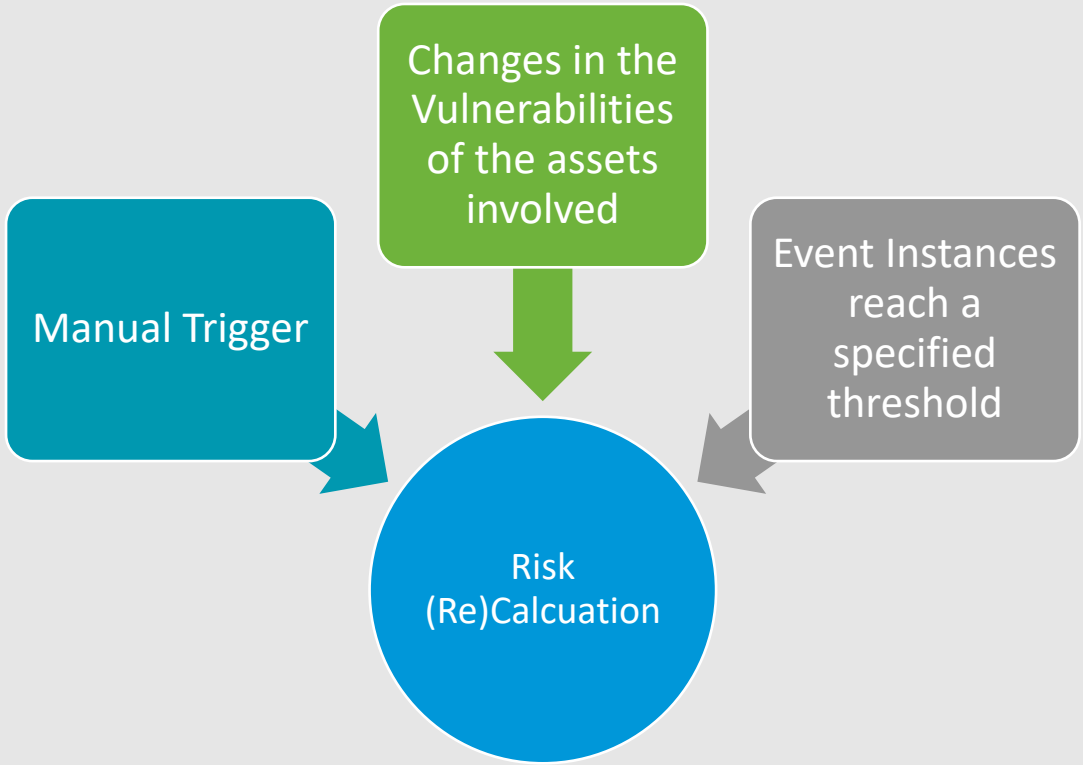
The Collaboration Service is connected to the data-layer and “listening” for event instances

Leverages the Collaborative Risk Assessment Engine of the H2020 MITIGATE Project

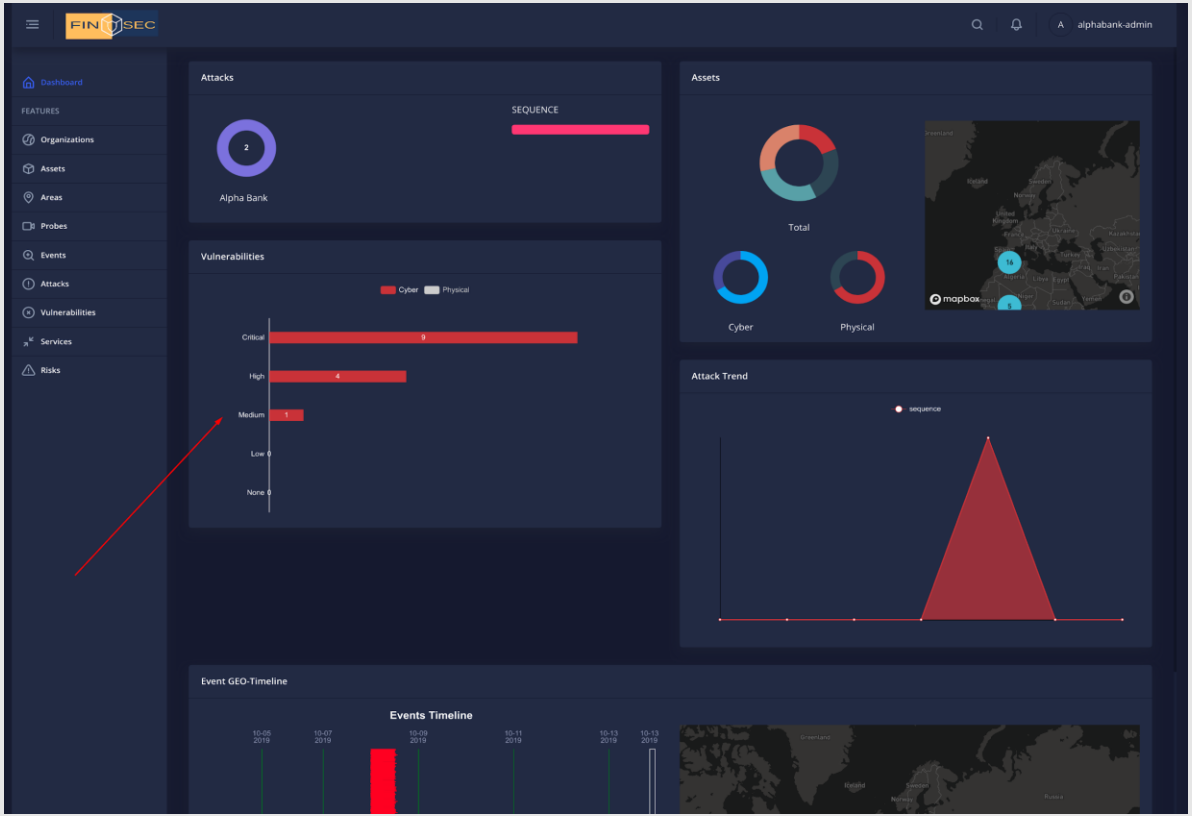
Collaborative Risk Assessment Inputs/Outputs



Triggers: What triggers risk (re)calculation?



Sample Risk Visualization in the FINSEC Dashboard



Vulnerabilities for the SWIFT service pilot, categorized by their domain (cyber/physical)

For More Information:

Please Register with: Finsecurity.eu

Thank you –Questions?