FINSEC

Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures

Overview and Status 2020

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

www.finsec-project.eu

The Project

H2020 FINSEC Project

Grant Agreement no. 786727

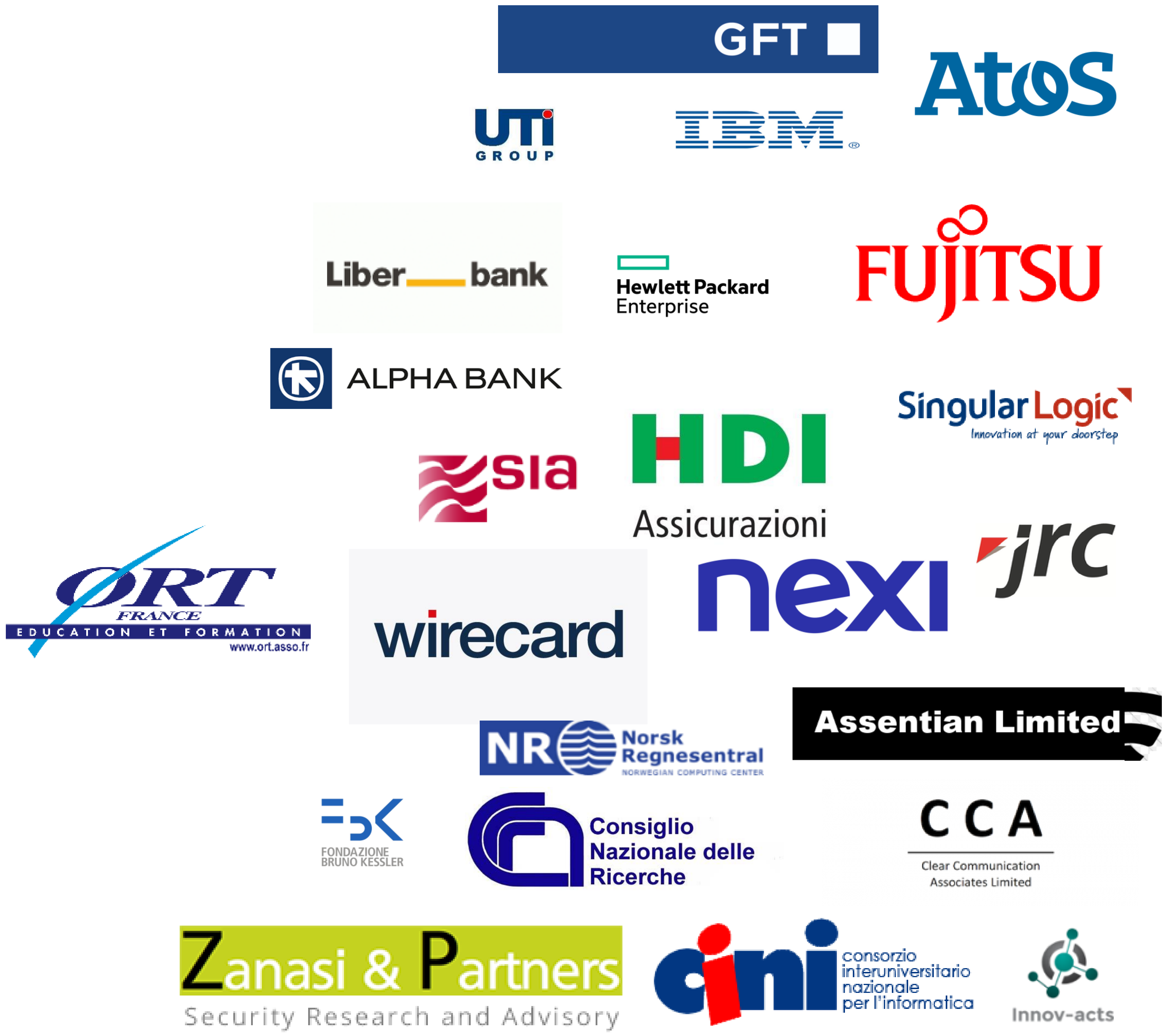
Integrated Framework
for Predictive and Collaborative
Security of Financial Infrastructures

- Prepared by **GFT Italia** – the coordinator - with 23 partners during summer 2017;
- Conceived for H2020 Programme in **Innovation Action** submitted to REA (Research Executive Agency) of EC;
- **CALL Reference CIP-01-2016-2017**: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe;
- Grant Agreement **FINSEC # 786727**;
- EC H2020 Project funding **7,817,631.35 €**;
- Duration **36 months**, from May 01, 2018 until April 30, 2021.

FINSEC Consortium

23 Partners from 10 European Countries

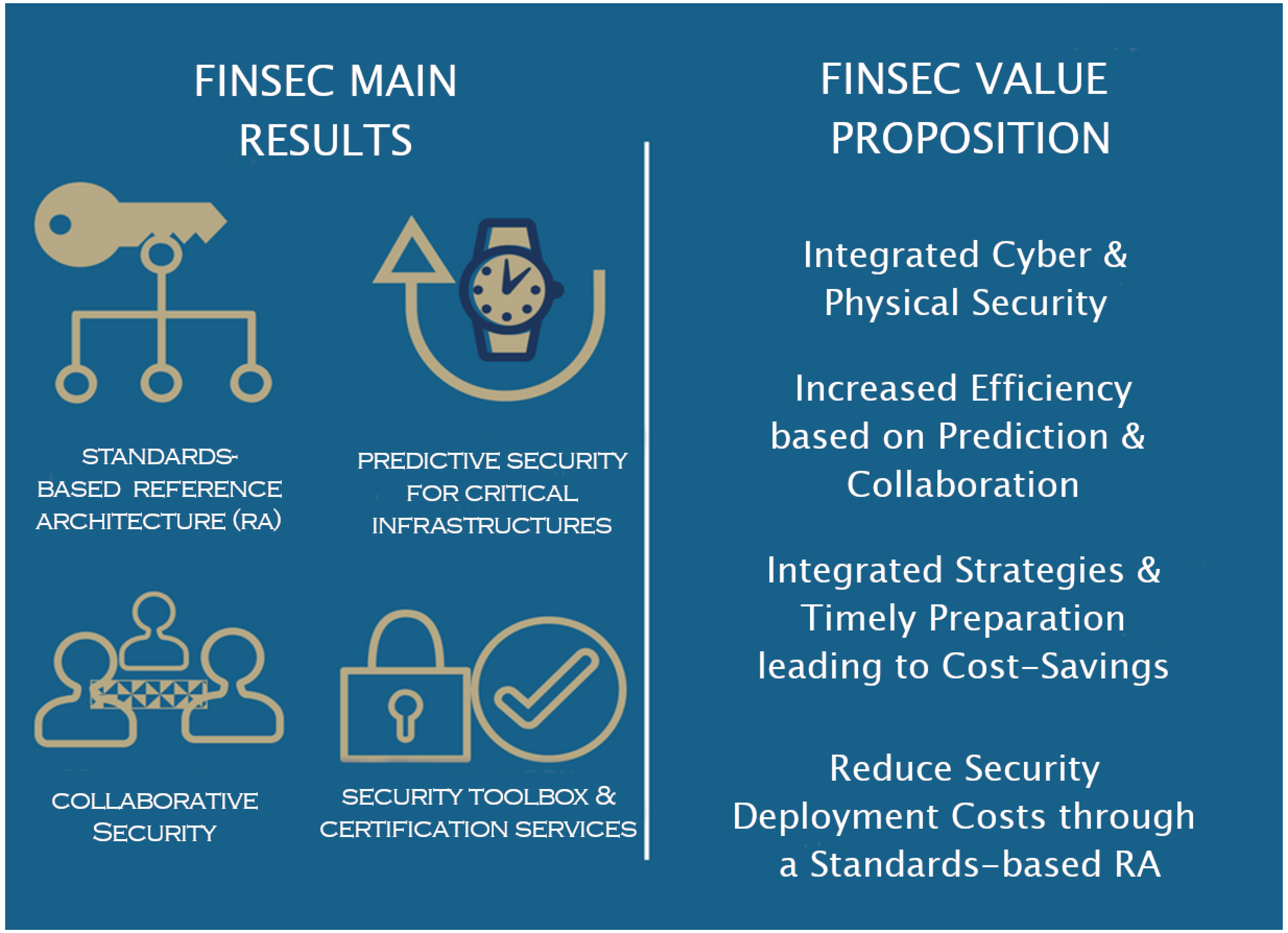
Joint effort of security experts, research centers, technology providers, academia and financial organizations.


GFT
Atos
UTi GROUP
IBM
Liber bank
Hewlett Packard Enterprise
FUJITSU
ALPHA BANK
SingularLogic
Innovation at your doorstep
sia
HDI Assicurazioni
ORT FRANCE
EDUCATION ET FORMATION
www.ort.asso.fr
wirecard
nexi
jrc
Assentian Limited
NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
FONDAZIONE BRUNO KESSLER
Consiglio Nazionale delle Ricerche
CCA
Clear Communication Associates Limited
Zanasi & Partners
Security Research and Advisory
cini
consorzio interuniversitario nazionale per l'informatica
Innov-acts

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Objectives

FINSEC develops and demonstrates an integrated (Physical + Cyber), intelligent, collaborative and predictive approach to the security of critical infrastructures in the financial sector



FINSEC MAIN RESULTS

STANDARDS-BASED REFERENCE ARCHITECTURE (RA)

PREDICTIVE SECURITY FOR CRITICAL INFRASTRUCTURES

COLLABORATIVE SECURITY

SECURITY TOOLBOX & CERTIFICATION SERVICES

FINSEC VALUE PROPOSITION

Integrated Cyber & Physical Security

Increased Efficiency based on Prediction & Collaboration

Integrated Strategies & Timely Preparation leading to Cost-Savings

Reduce Security Deployment Costs through a Standards-based RA

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSEC Tools

Tool	Main Functionalities	Enhancement as part of FINSEC	TRL	Owner
Security Information and Event Management (SIEM)	Security events collection, filtering, analysis and correlation	• Enhancement with more data sources and event types for the financial sector's infrastructures • Interoperability with other tools of the toolbox	>=7	ATOS
Risk Assessment Engine (RAE)	Real-time assessment of security risks, including business interpretation	• Support of business indicators for the financial sector • Assessment of economic impact • Support for Cyber & Physical Risks	>=6	ATOS
Collaborative Risk Assessment	Risk Analysis & Management; Document Sharing	• Adaptation to Cyber and Physical assets of the financial sector	>=7	SiLO
ATM Network Security Platform	ATM machines' network monitoring and security management	• Embedded ATM security device, integrating FUJITSU's CCTV Analytics & IBM' Anomaly detection (see below) • Secure, encrypted communications network	>=6	UTI
Pentesting service	Vulnerability Assessment associated with cyber assets	• Support for correlation with the vulnerabilities of physical assets	>=4	ATOS
Anomaly Detection	Detection of abnormal behaviours in ATM and PC networks	• Training of machine learning models for behaviours in the financial sector	>=7	IBM
CCTV Analysis	Identification & analysis of physical security incidents	• Adaptation to behavior patterns according ATM or building security • Development of threat model and threat evaluation	>=6	FUJITSU

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

The Problem

Security Incidents in the Finance Sector

2016

SWIFT Attack

The February 2016 Swift attack against the Bangladesh Bank robbery led to an illegally transfer of close to US $1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank.

2017

WannaCry

The WannaCry and Petya ransomware in 2017 had a significant adverse impact on Russian and Ukrainian banks.

2017

Equifax

The 2017 data breach at Equifax: Turmoil in the global markets affecting more than 140 million consumers.

2018

IMF Projection

According to IMF (International Monetary Fund), emerging cyber-attacks could put at risk a significant percentage (9%-50%) of the financial institutions' profits (June 2018).

2019

Metro Bank

The growing sophistication of attacks. The attack in early February 2019 by a Signaling Systems Number 7, SS7 (mobile networks connection).

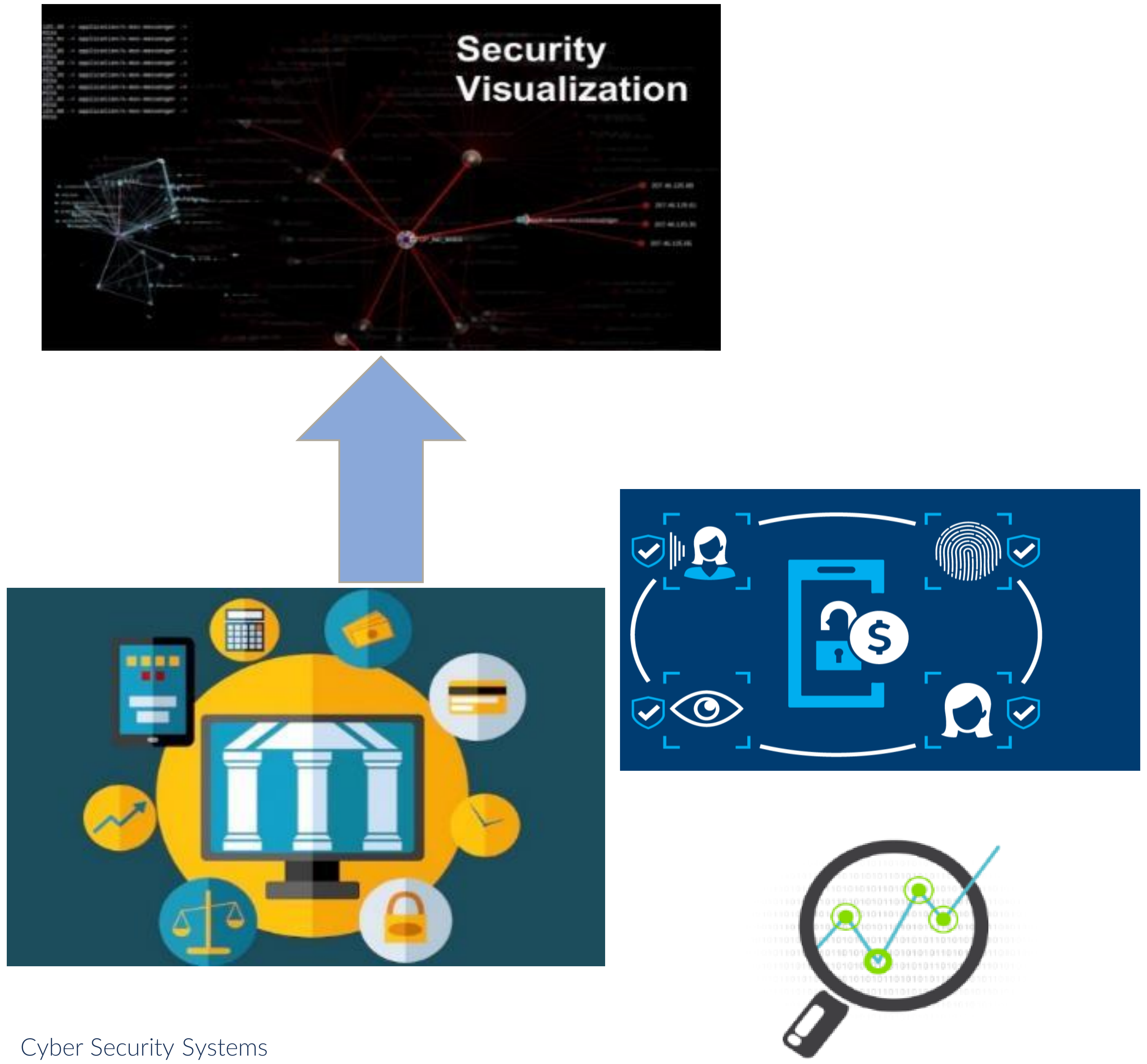
2019

Capital One

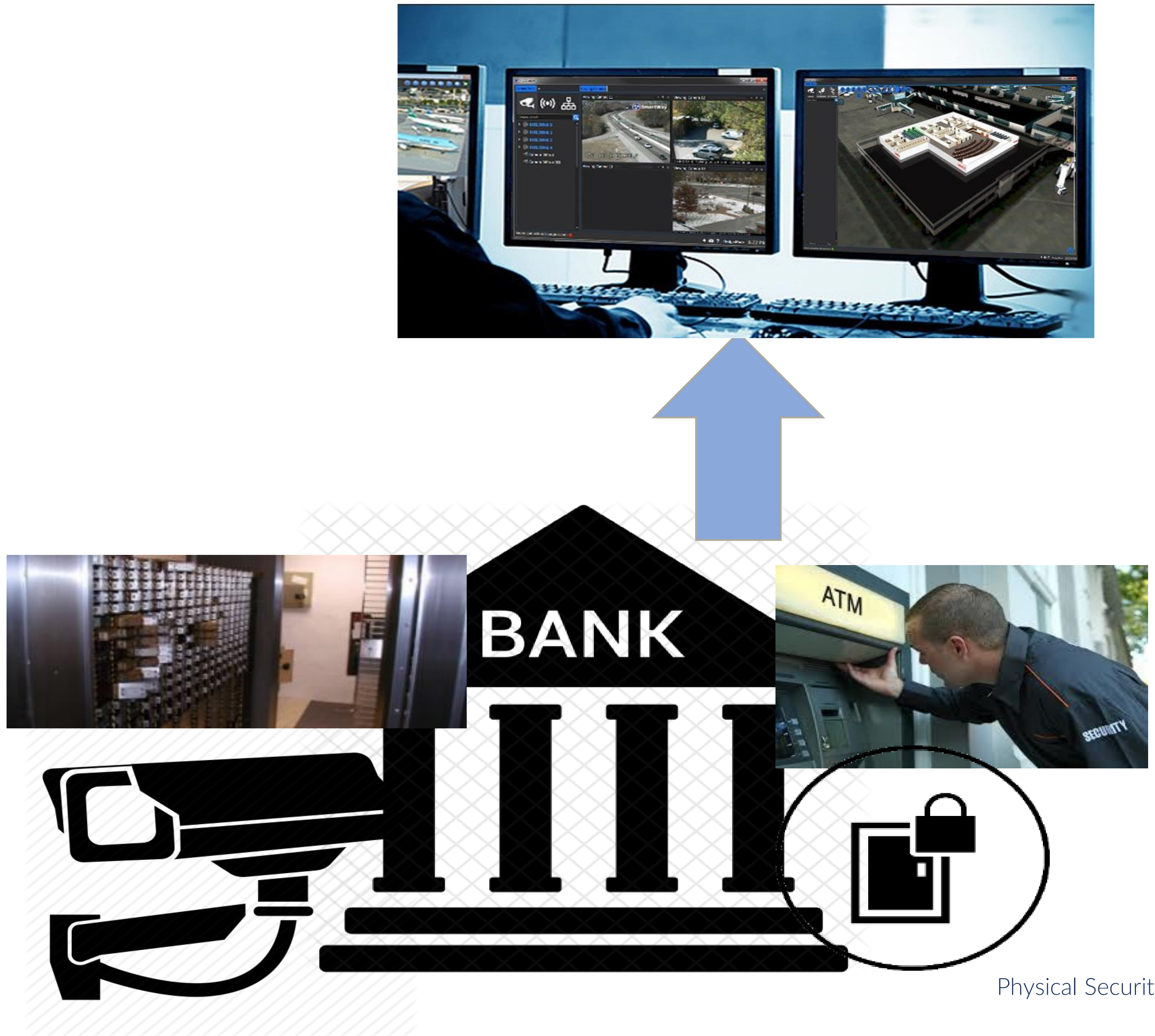
Announced in July 2019 a severe data breach of more than 100 million people, yielding private information such as credit scores and balances, ZIP codes, email addresses, dates of birth, etc.

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Physical & Cyber Security "Silos"



Cyber Security Systems



Physical Security Systems

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

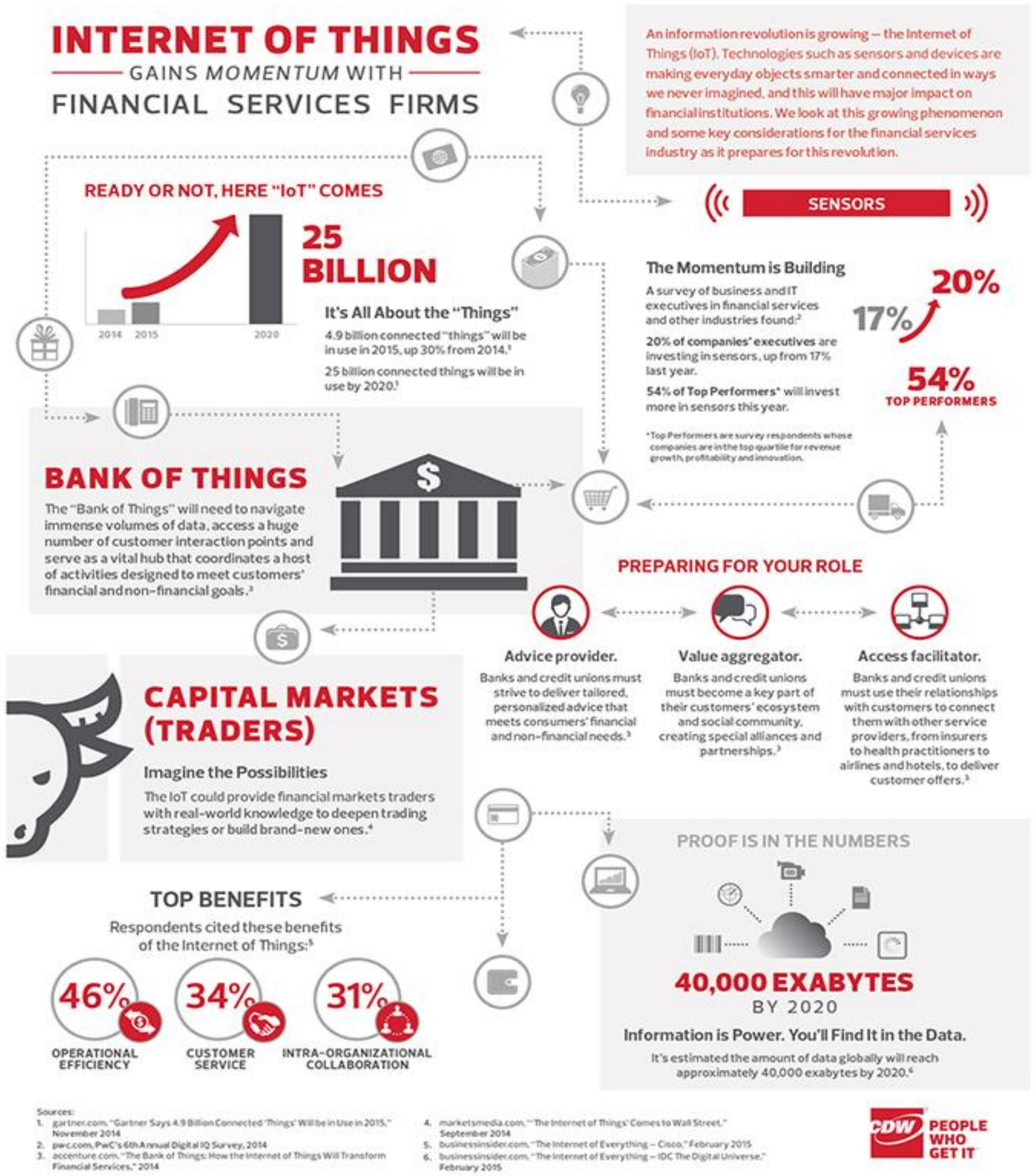
Motivation for Integrated Security

Rise of Internet connected devices (e.g., ATM)

- The “Bank of Things”
- Possibility for a wave of physical + cyber attacks

Physical & Cyber Security in financial institutions remain “siloed”

- Accuracy
- Resilience
- Cost-efficiency



INTERNET OF THINGS GAINS *MOMENTUM* WITH FINANCIAL SERVICES FIRMS

An information revolution is growing – the Internet of Things (IoT). Technologies such as sensors and devices are making everyday objects smarter and connected in ways we never imagined, and this will have major impact on financial institutions. We look at this growing phenomenon and some key considerations for the financial services industry as it prepares for this revolution.

READY OR NOT, HERE “IoT” COMES

25 BILLION

It's All About the “Things”

4.9 billion connected “things” will be in use in 2015, up 30% from 2014.[1]

25 billion connected things will be in use by 2020.[1]

SENSORS

The Momentum is Building

A survey of business and IT executives in financial services and other industries found:[2]

20% of companies' executives are investing in sensors, up from 17% last year.

54% of Top Performers* will invest more in sensors this year.

*Top Performers are survey respondents whose companies are in the top quartile for revenue growth, profitability and innovation.

BANK OF THINGS

The “Bank of Things” will need to navigate immense volumes of data, access a huge number of customer interaction points and serve as a vital hub that coordinates a host of activities designed to meet customers' financial and non-financial goals.[3]

PREPARING FOR YOUR ROLE

Advice provider. Banks and credit unions must strive to deliver tailored, personalized advice that meets consumers' financial and non-financial needs.[3]

Value aggregator. Banks and credit unions must become a key part of their customers' ecosystem and social community, creating special alliances and partnerships.[3]

Access facilitator. Banks and credit unions must use their relationships with customers to connect them with other service providers, from insurers to health practitioners to airlines and hotels, to deliver customer offers.[3]

CAPITAL MARKETS (TRADERS)

Imagine the Possibilities

The IoT could provide financial markets traders with real-world knowledge to deepen trading strategies or build brand-new ones.[4]

TOP BENEFITS

Respondents cited these benefits of the Internet of Things:[5]

46%	OPERATIONAL EFFICIENCY
34%	CUSTOMER SERVICE
31%	INTRA-ORGANIZATIONAL COLLABORATION

PROOF IS IN THE NUMBERS

40,000 EXABYTES BY 2020

Information is Power. You'll Find It in the Data.

It's estimated the amount of data globally will reach approximately 40,000 exabytes by 2020.[6]

Sources:

1. gartner.com, “Gartner Says 4.9 Billion Connected 'Things' Will be in Use in 2015,” November 2014
2. pwc.com, PwC's 6th Annual Digital IQ Survey, 2014
3. accenture.com, “The Bank of Things: How the Internet of Things Will Transform Financial Services,” 2014
4. marketsmedia.com, “The Internet of Things' Comes to Wall Street,” September 2014
5. businessinsider.com, “The Internet of Everything – Cisco,” February 2015
6. businessinsider.com, “The Internet of Everything – IDC The Digital Universe,” February 2015

CDW PEOPLE WHO GET IT

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Regulatory Requirements

NIS Directive: EU-wide legislation on cybersecurity:

- ❑ Adopted by the European Parliament on 6 July 2016 and entered into force in August 2016

NIS emphasizes on:

- ❑ Preparedness at national level e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority
- ❑ Cooperation among all the Member States, by setting up a cooperation group - CSIRT Network

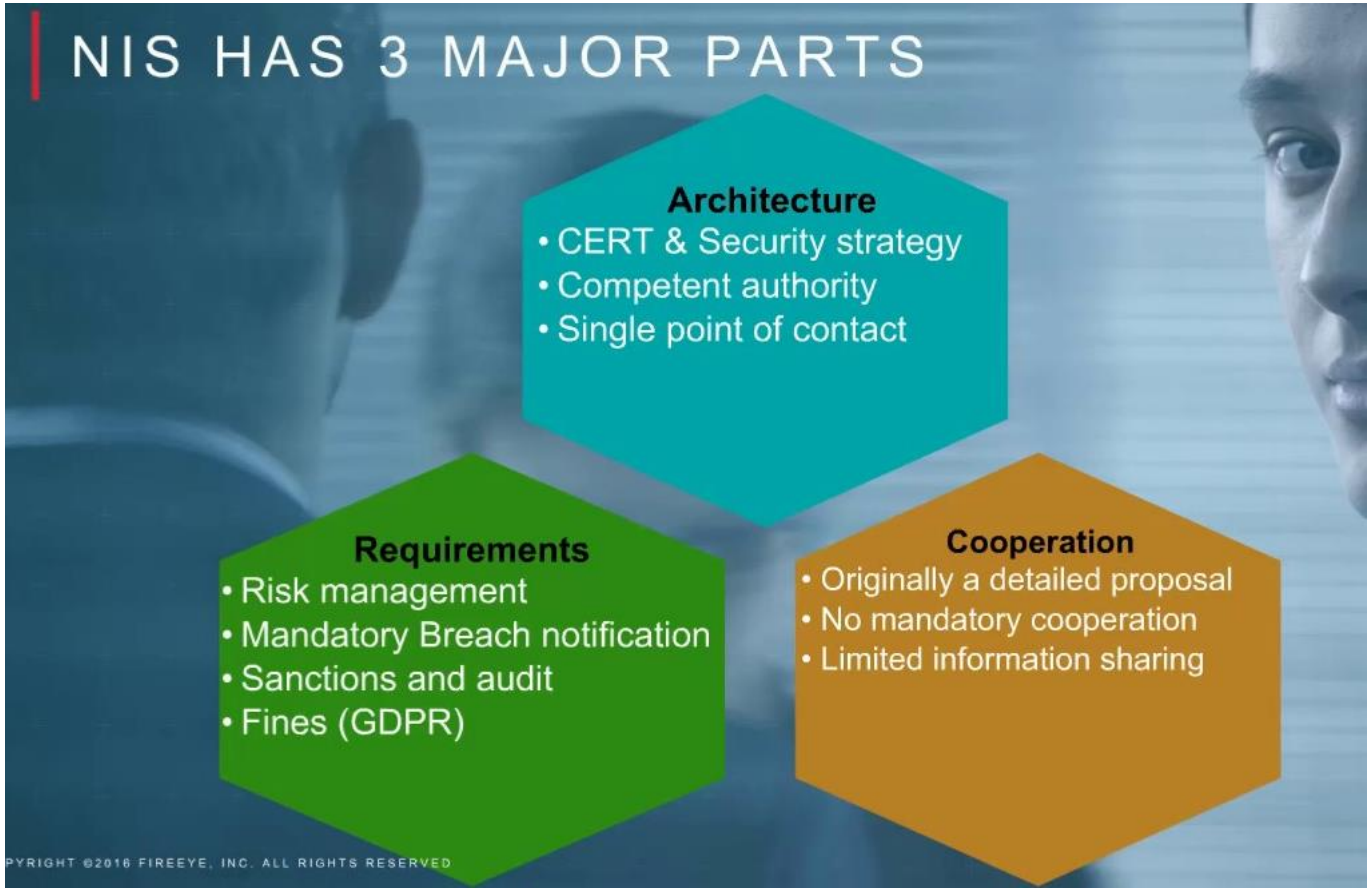
Sectors:

- ❑ Energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

General Data Privacy Regulation (GDPR), stricter and effective security measures for all assets where personal data are managed and exchanged.

The Second Payment Services Directive (PSD2): Compliance to the 2nd Payment Services Directive (PSD) demands for banks to be able to interact with multiple Payments Services Providers (PSPs) in the scope of an API based Open Banking approach. This raises more cybersecurity concerns and asks for strong security measures like pentesting and vulnerability assessment on the APIs

The EU legislative framework for electronic communications (EU Directive 2009/140/EC) reformed in 2009 and Article 13a introduced into the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). Article 13a concerns security and integrity of electronic communications networks and services



NIS HAS 3 MAJOR PARTS

Architecture
- CERT & Security strategy
- Competent authority
- Single point of contact

Requirements
- Risk management
- Mandatory Breach notification
- Sanctions and audit
- Fines (GDPR)

Cooperation
- Originally a detailed proposal
- No mandatory cooperation
- Limited information sharing

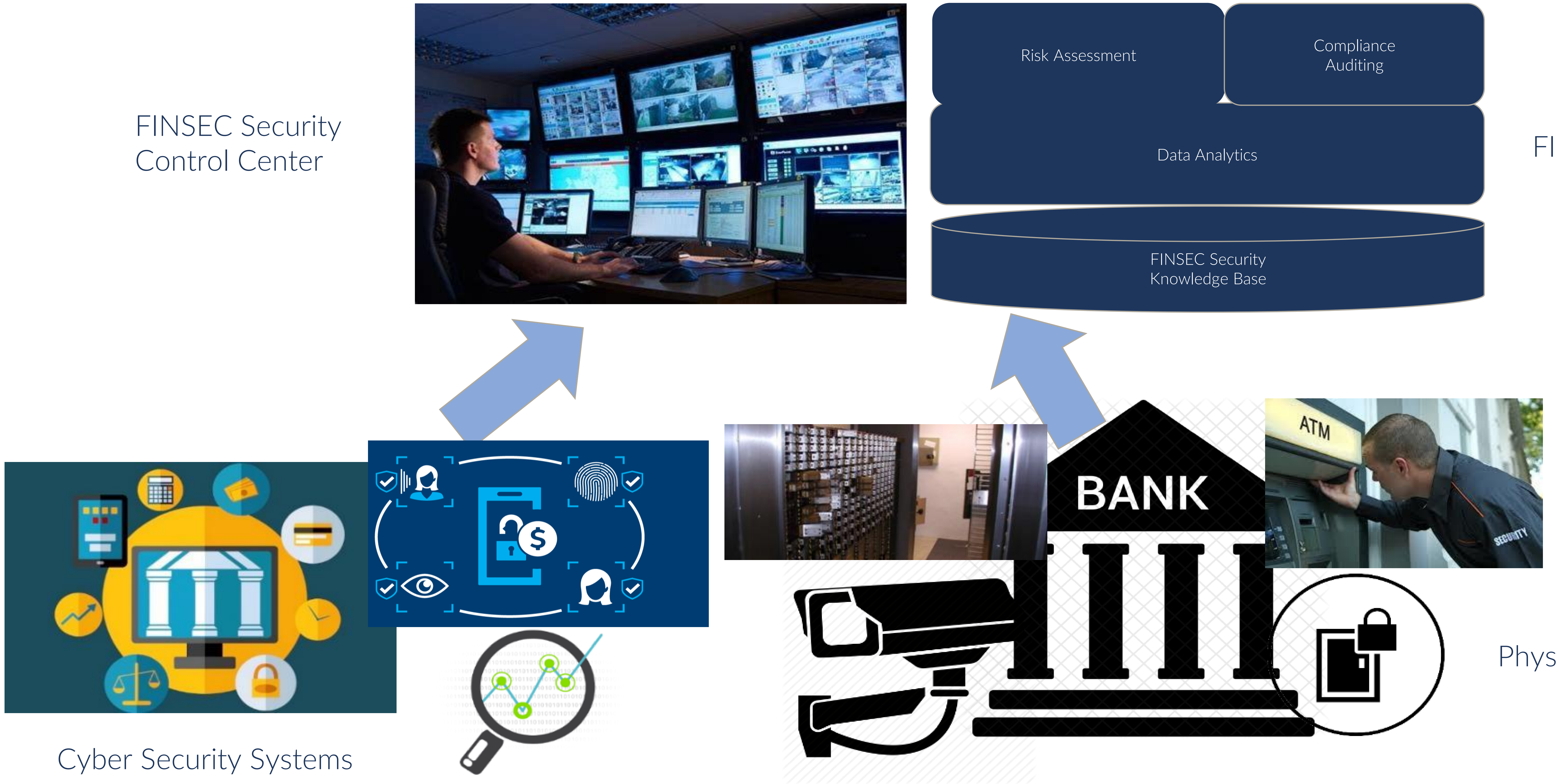
PYRIGHT ©2016 FIREEYE, INC. ALL RIGHTS RESERVED

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

The Concept

FINSEC Concept

Physical & Cyber Security Integration



FINSEC Security Control Center

FINSEC System

Risk Assessment

Compliance Auditing

Data Analytics

FINSEC Security Knowledge Base

Cyber Security Systems

Physical Security Systems

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Collaborative Risk Assessment in the Financial Supply Chain

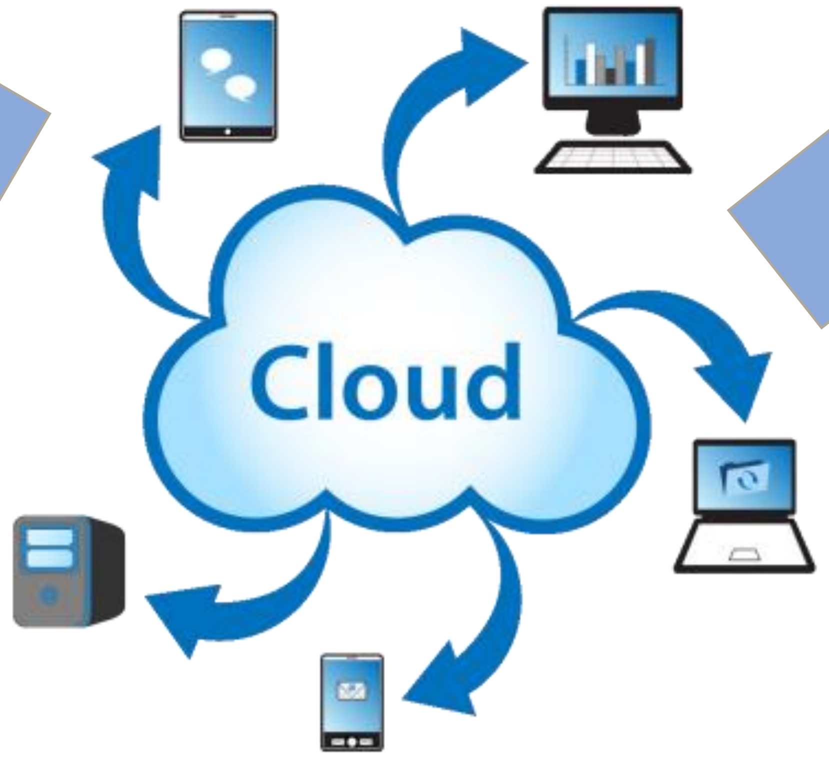
Supply Chain Processes

- SWIFT Transactions
- Trading
- OECD Info Exchange
- ……

FINSEC Enhanced Security Control Center

FINSEC Security Knowledge Base

FINSEC Security Data Sharing & Information Exchange



FINSEC Private Cloud

FINSEC Enhanced Security Control Center

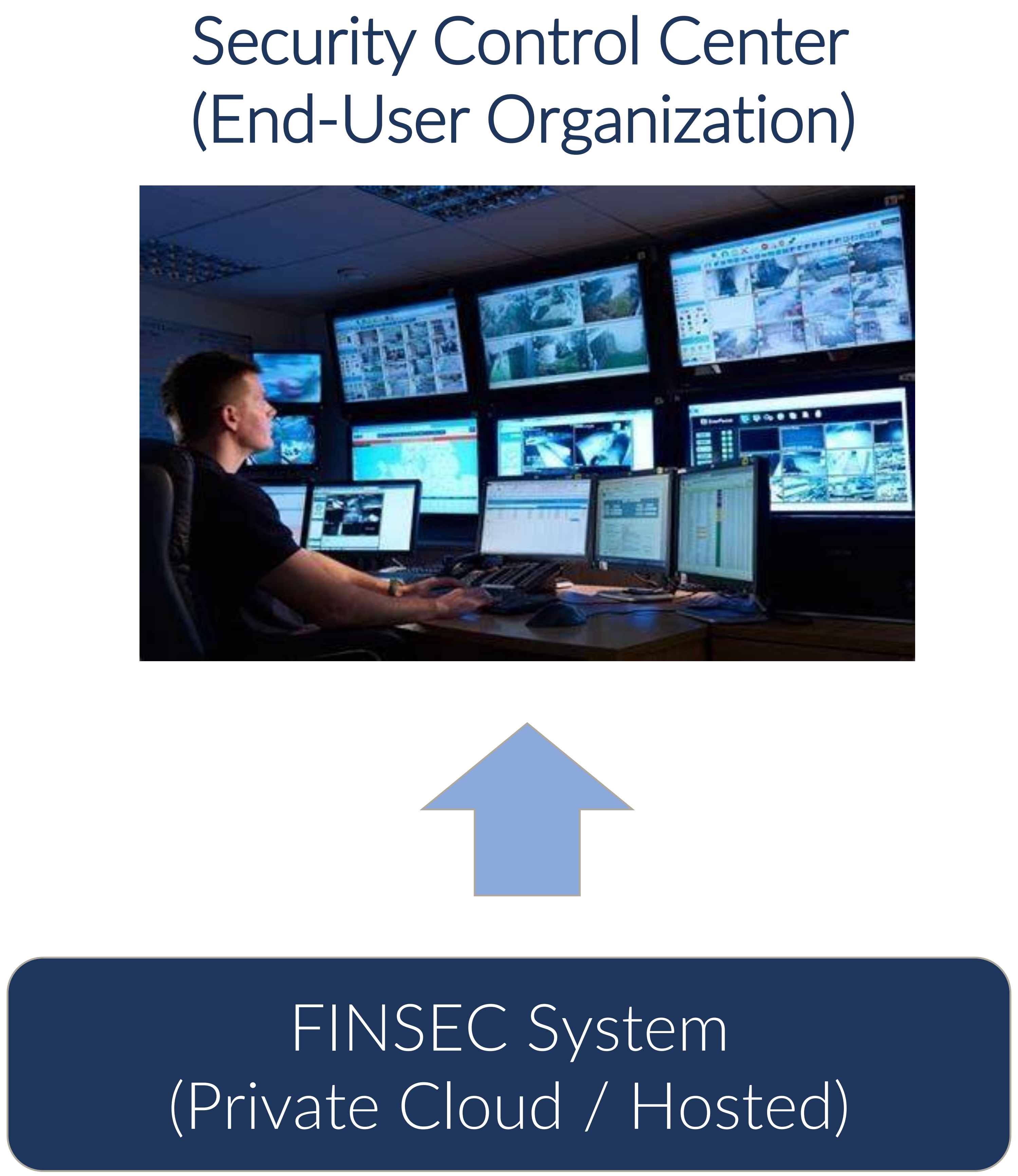
FINSEC Security Knowledge Base

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSEC Deployment Scenarios

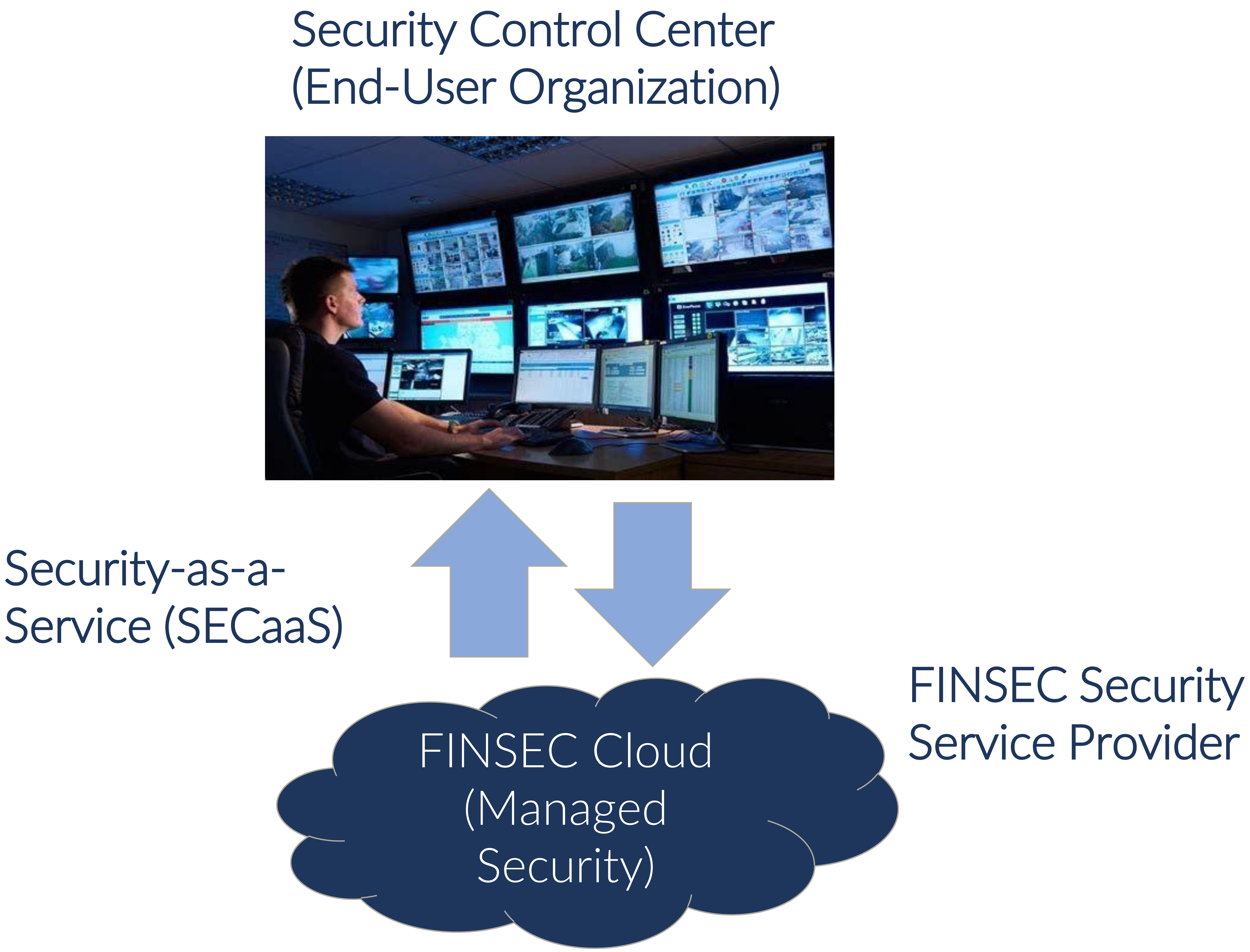
Private Hosting & Managed Security

Organizations may opt for the Deployment Scenario of their choice depending on their size, budget, internal organization etc…



Security Control Center
(End-User Organization)

FINSEC System
(Private Cloud / Hosted)



Security Control Center
(End-User Organization)

Security-as-a-Service (SECaaS)

FINSEC Cloud
(Managed Security)

FINSEC Security Service Provider

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

A Data Driven approach to Security

Concepts Lent & Learnt from Reference Security Frameworks

- ❑ E.g., Industrial Internet Reference Architecture and Industrial Internet Security Framework

Security is a Cross-Layer Function (Overlay)

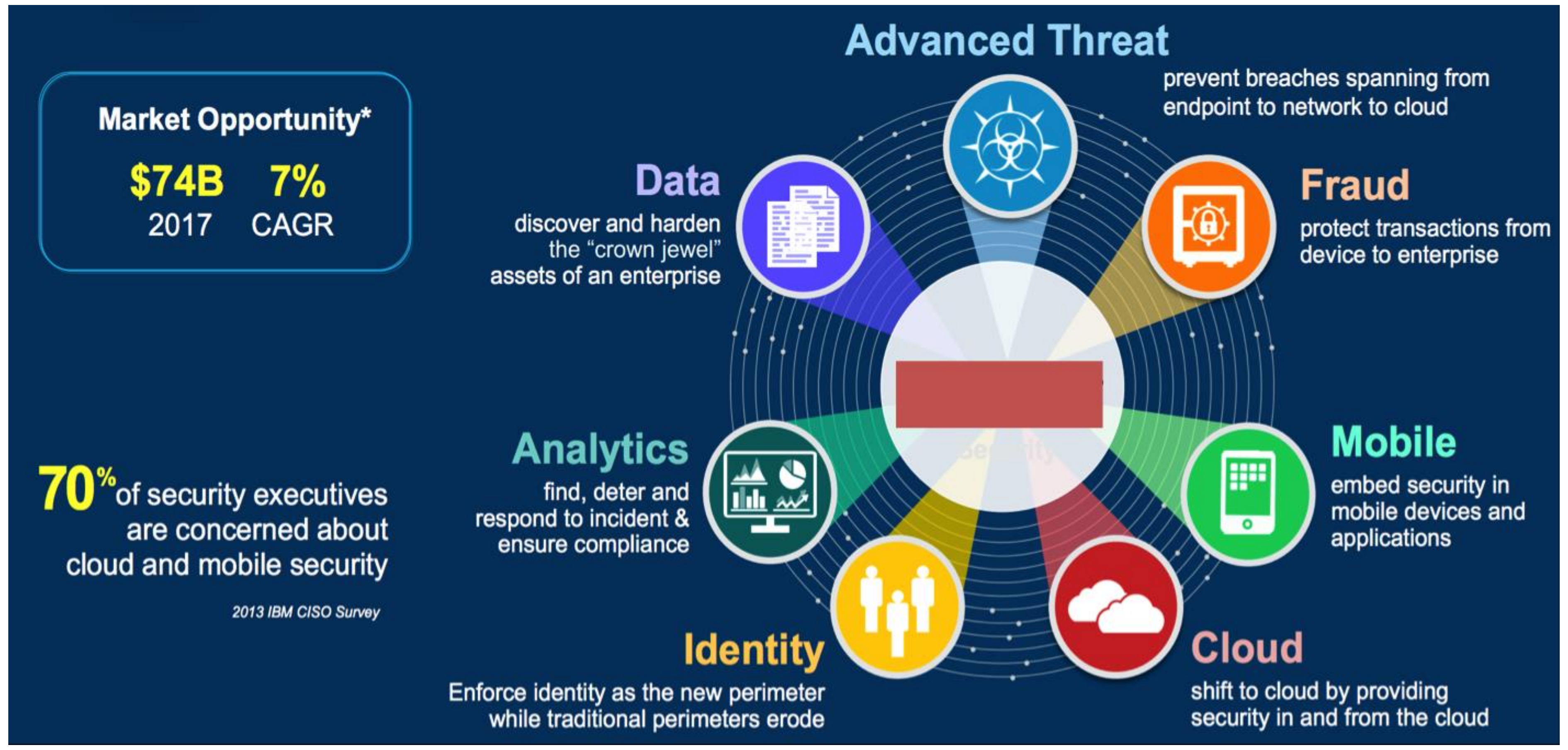
Security Monitoring & Analysis is relevant to FINSEC:

- ❑ Monitor -→ Analyze -→ Act Cycle
- ❑ BigData Analytics & AI are Trending

Three-Tier & Multi-Tier Architecture relevant for the IT Implementation

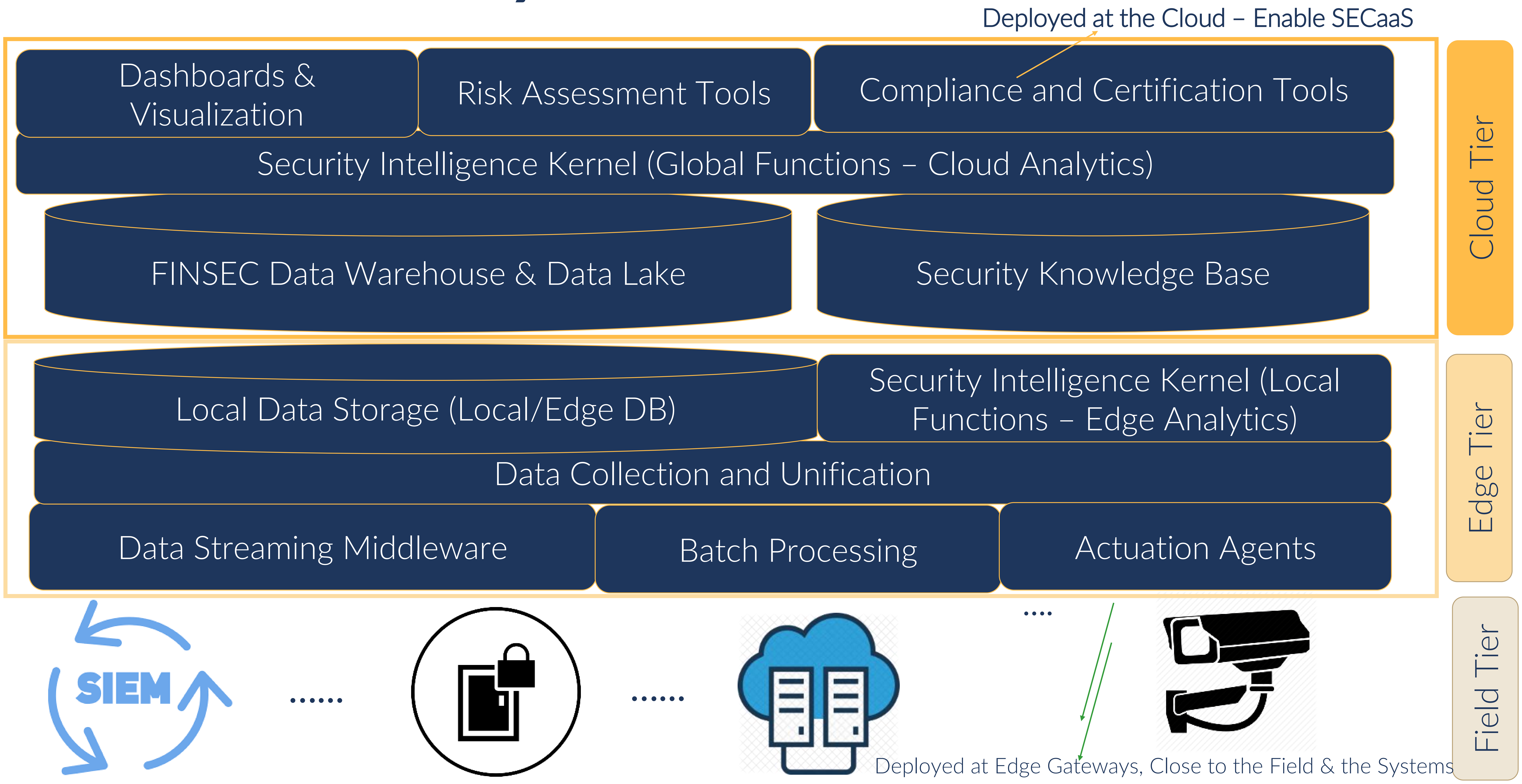
Cross-Cutting functions:

- ❑ Visualization/Dashboards
- ❑ Configuration/Management


Market Opportunity*
$74B 2017
7% CAGR
70% of security executives are concerned about cloud and mobile security
2013 IBM CISO Survey
Advanced Threat
prevent breaches spanning from endpoint to network to cloud
Data
discover and harden the "crown jewel" assets of an enterprise
Fraud
protect transactions from device to enterprise
[redacted]
Analytics
find, deter and respond to incident & ensure compliance
Mobile
embed security in mobile devices and applications
Identity
Enforce identity as the new perimeter while traditional perimeters erode
Cloud
shift to cloud by providing security in and from the cloud

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSEC Physical View Considerations



Deployed at the Cloud – Enable SECaaS

Dashboards & Visualization

Risk Assessment Tools

Compliance and Certification Tools

Security Intelligence Kernel (Global Functions – Cloud Analytics)

FINSEC Data Warehouse & Data Lake

Security Knowledge Base

Cloud Tier

Local Data Storage (Local/Edge DB)

Security Intelligence Kernel (Local Functions – Edge Analytics)

Data Collection and Unification

Data Streaming Middleware

Batch Processing

Actuation Agents

Edge Tier

Field Tier

Deployed at Edge Gateways, Close to the Field & the Systems

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 786727

"Composite" & Intelligent Probes

SIEM

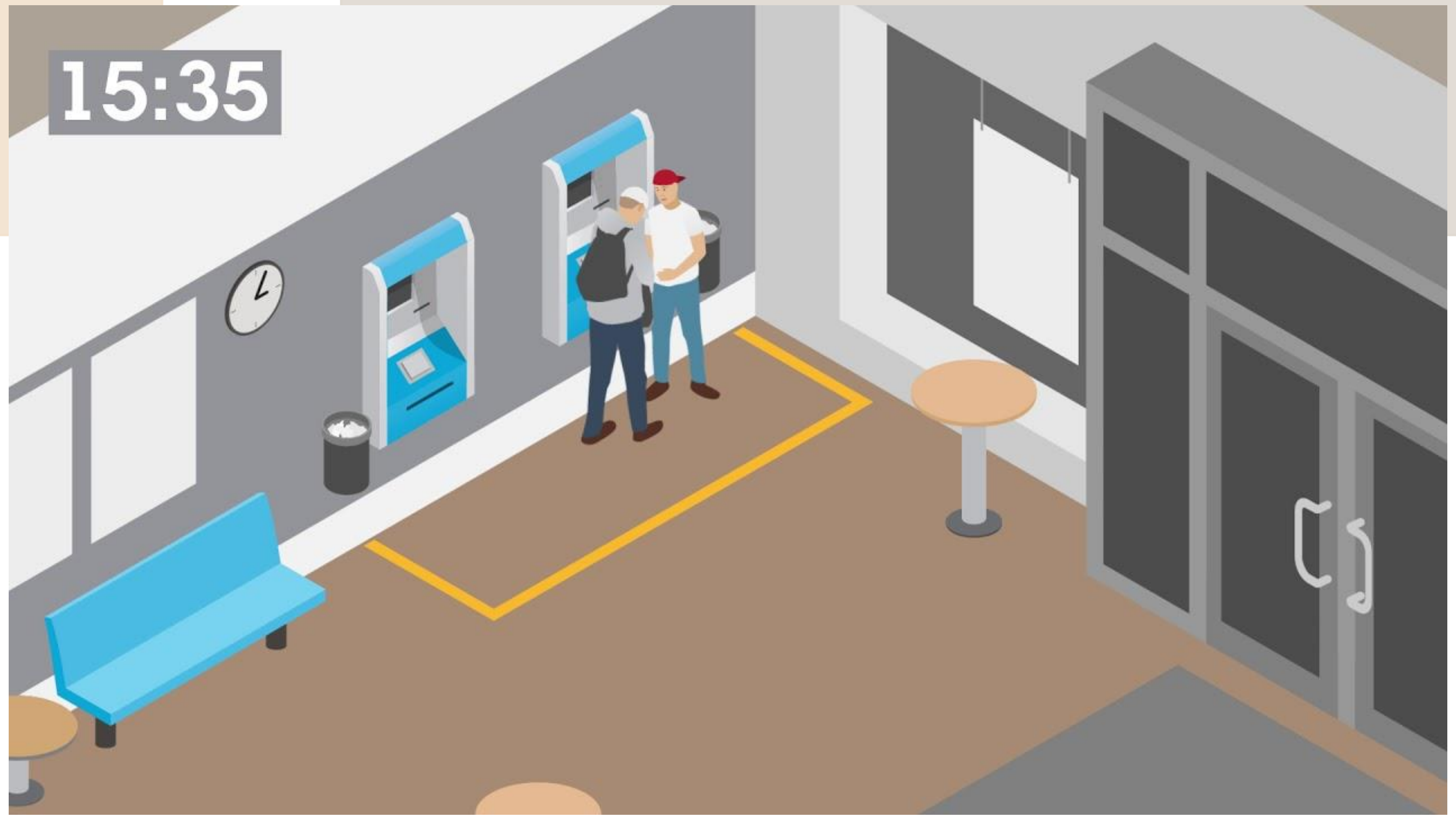
- Security Information and Event Management Platform
- Customized to Finance Sector
- Support for FINSTIX

CCTV Analytics

- Closed Circuit Television System
- AI-Based Visual Scene Analysis
- Trained on Finance Sector Scenarios (e.g., ATM Protection)

Anomaly Detection

- Analytics and Machine Learning over Raw Security Data
- Behavioral Analysis

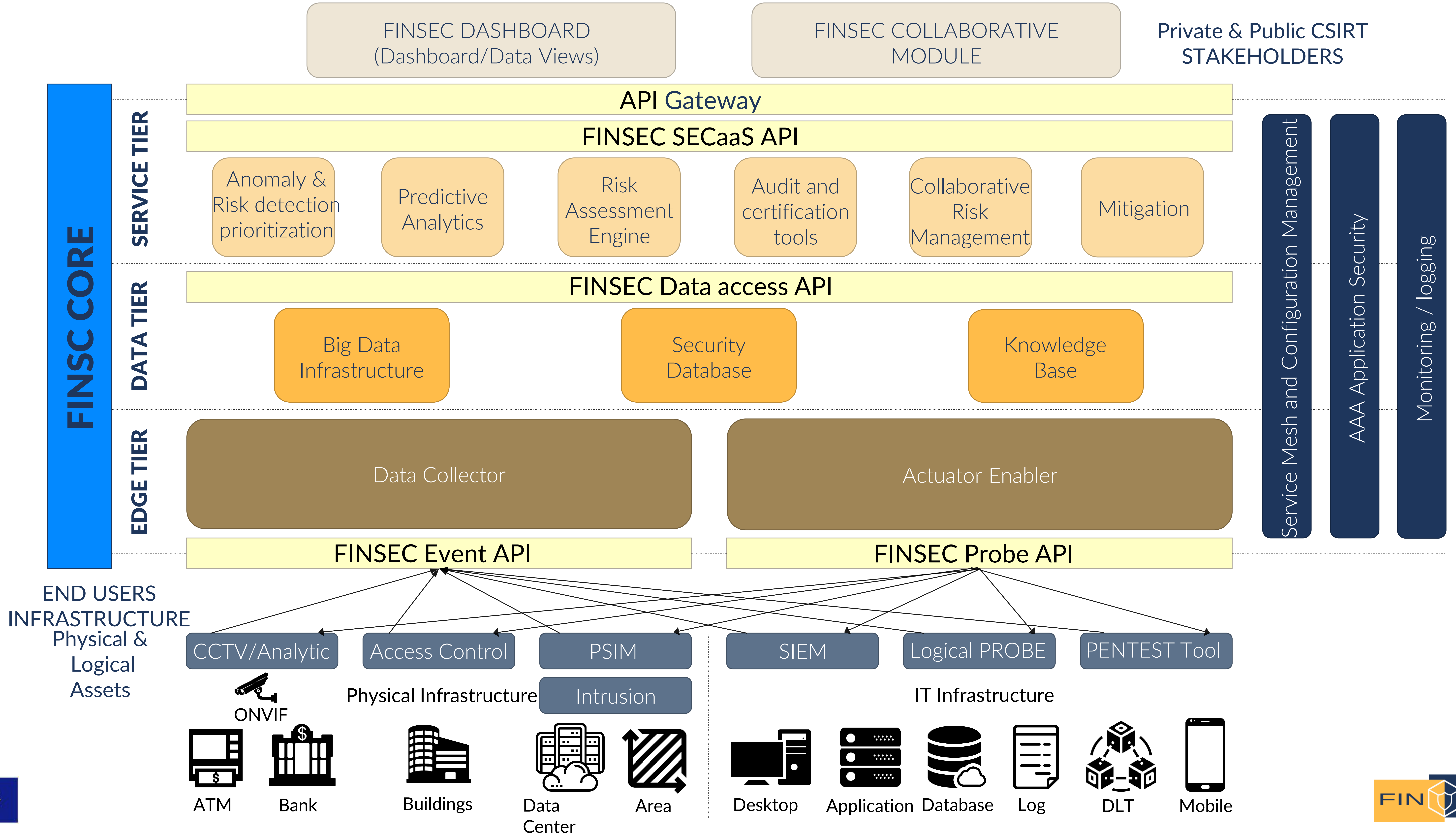


This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Main Results

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

The FINSEC Reference Architecture



FINSEC DASHBOARD (Dashboard/Data Views)

FINSEC COLLABORATIVE MODULE

Private & Public CSIRT STAKEHOLDERS

FINSC CORE

SERVICE TIER

API Gateway

FINSEC SECaaS API

Anomaly & Risk detection prioritization

Predictive Analytics

Risk Assessment Engine

Audit and certification tools

Collaborative Risk Management

Mitigation

DATA TIER

FINSEC Data access API

Big Data Infrastructure

Security Database

Knowledge Base

EDGE TIER

Data Collector

Actuator Enabler

FINSEC Event API

FINSEC Probe API

Service Mesh and Configuration Management

AAA Application Security

Monitoring / logging

END USERS INFRASTRUCTURE

Physical & Logical Assets

CCTV/Analytic

Access Control

PSIM

Intrusion

SIEM

Logical PROBE

PENTEST Tool

ONVIF

Physical Infrastructure

IT Infrastructure

ATM

Bank

Buildings

Data Center

Area

Desktop

Application

Database

Log

DLT

Mobile

Reference Architecture Highlights

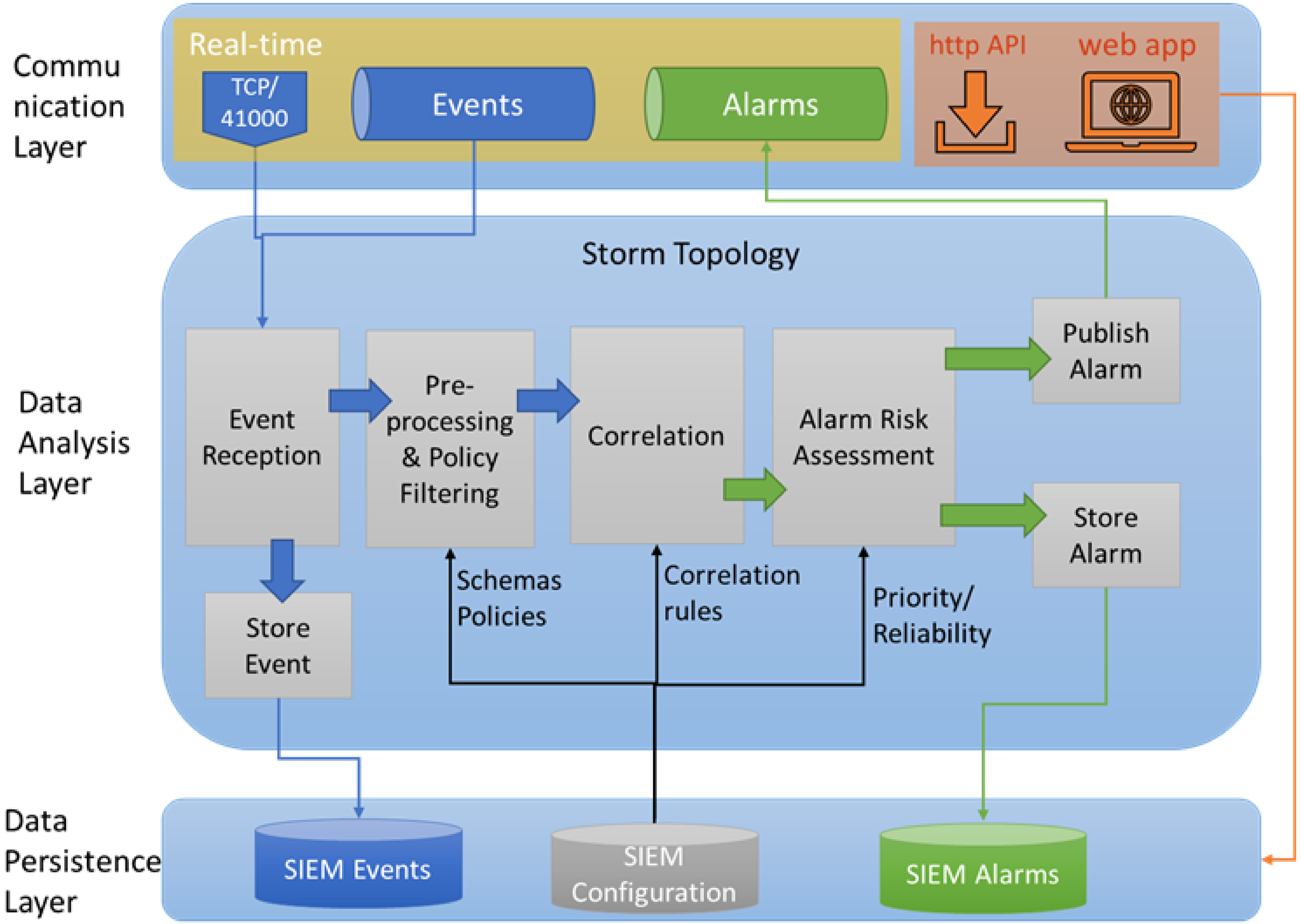
- State-of-the-art intelligent platform, edge type, for metadata and video images and based on “deep learning” algorithms
- Powerful fusion and artificial intelligence engines that support the decision-making process
- Advanced functions and versatile integration, compatible with new FINSTX proposed architecture and data-model

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 786727

The FINSEC SIEM Solution

Cross-Layer SIEM (XL-SIEM) for Finance

- SIEM solution with high-performance correlation engine
- Provides scalability and distribution in security events processing through a cluster of nodes, and capacity to raise security alerts from a business perspective
- Leverages events collected from different data sources at different layers.
- Supports security models and events for the finance sector
- ATOS technology built over the Alien Vault Open Source SIEM (OSSIM)

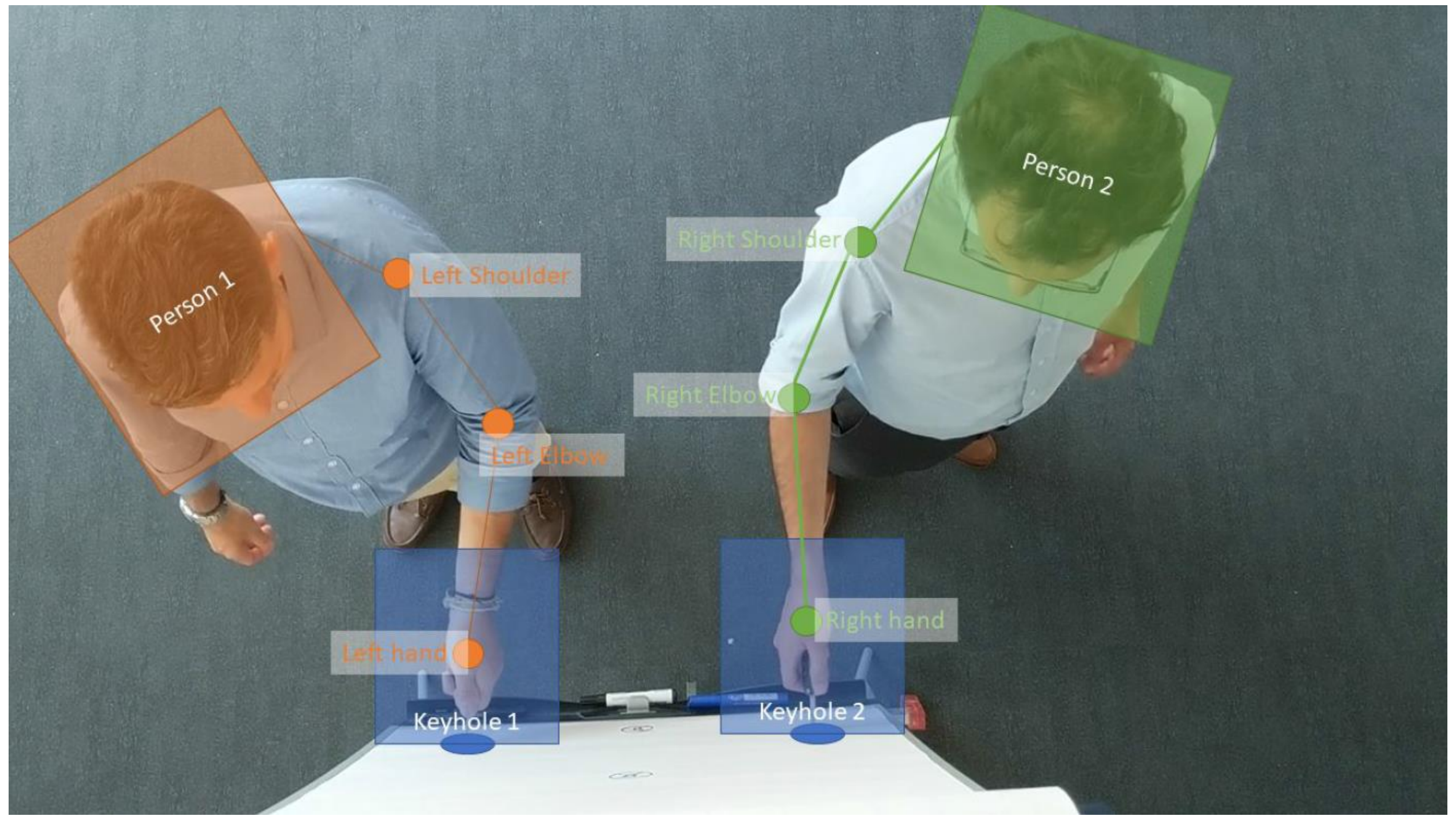


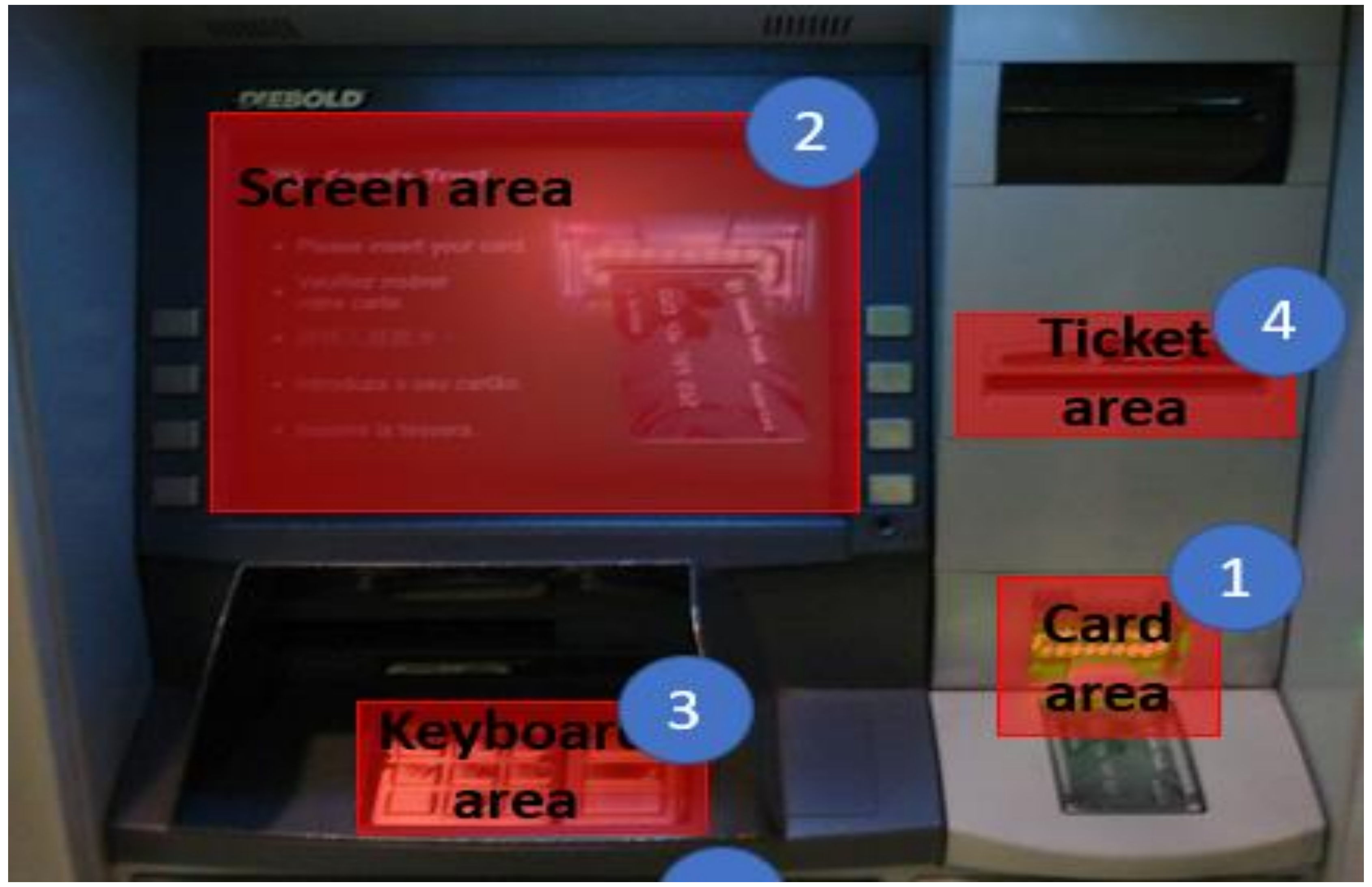
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

The FINSEC CCTV Solution

FINSEC CCTV Analytics Service (FCAS)

- Flexible framework to track events coming from physical interactions
- Detects objects (cars, bikes, people, heads, hands, etc.) and captures their interactions with each other and with physical motionless objects.
- Innovation: Ensuring complete respect of the privacy of the persons being filmed.
- Design agnostic of the security or business use cases
- Business Logic is implemented at upper layers of the FINSEC Architecture



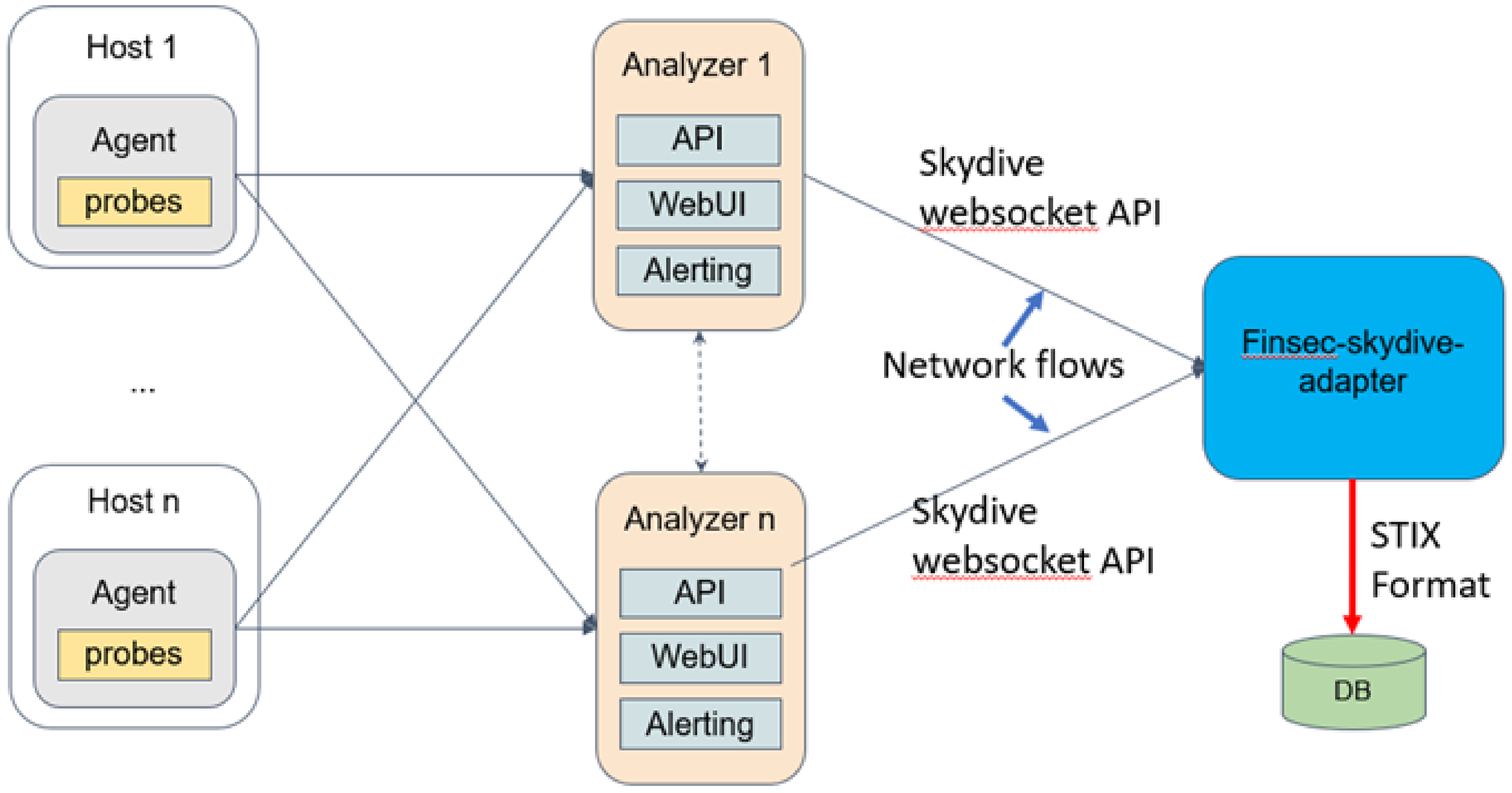


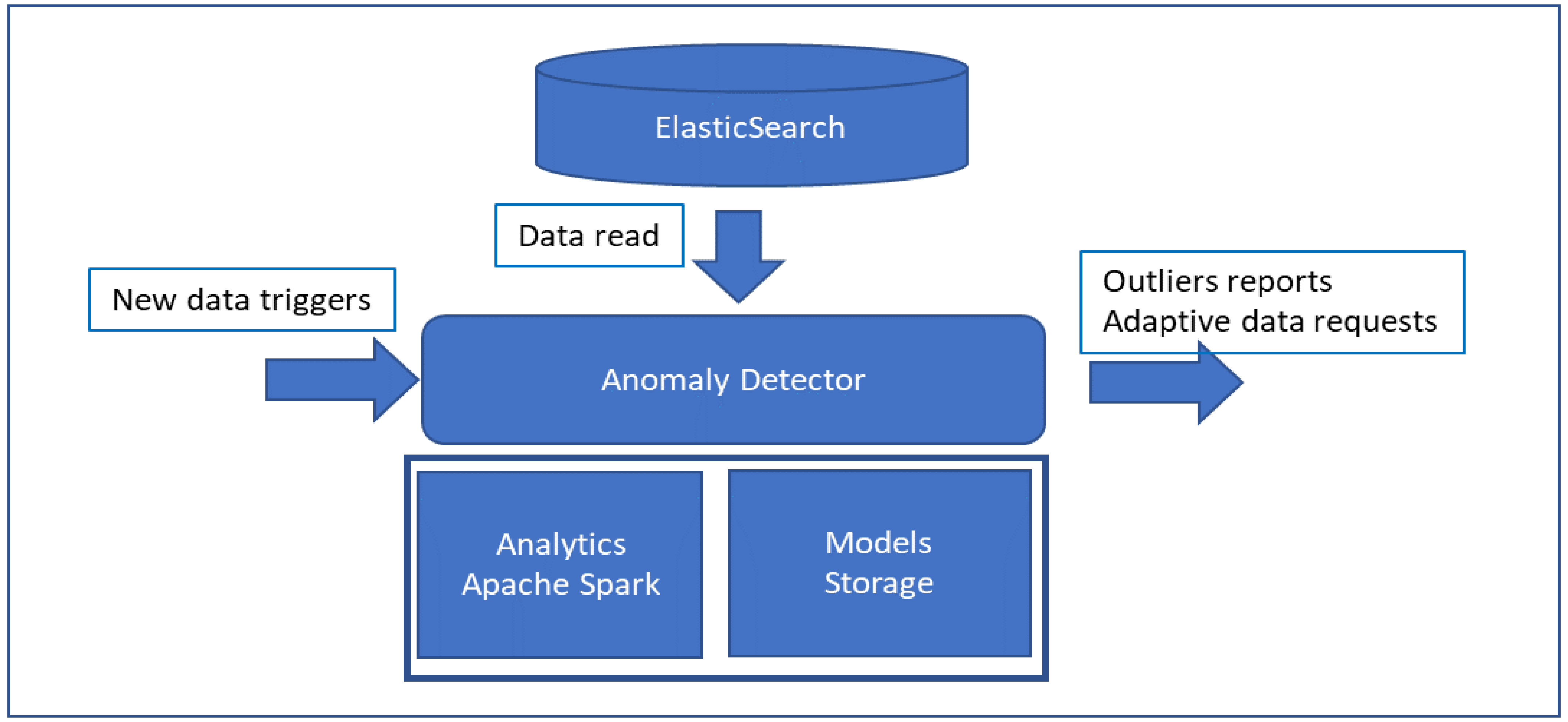
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

The FINSEC Anomaly Detection Service

FINSEC Anomaly Detection

- Family of analytics techniques that learn typical properties of the system and reports significant deviations from the typical system’s properties as outliers
- Used in the state-of-the-art Intrusion Detection Systems (IDSs)
- Samples use cases include Suspicious outbound access, Data leakage detection, Reconnaissance/port scan attack detection, Insider threat detection etc.



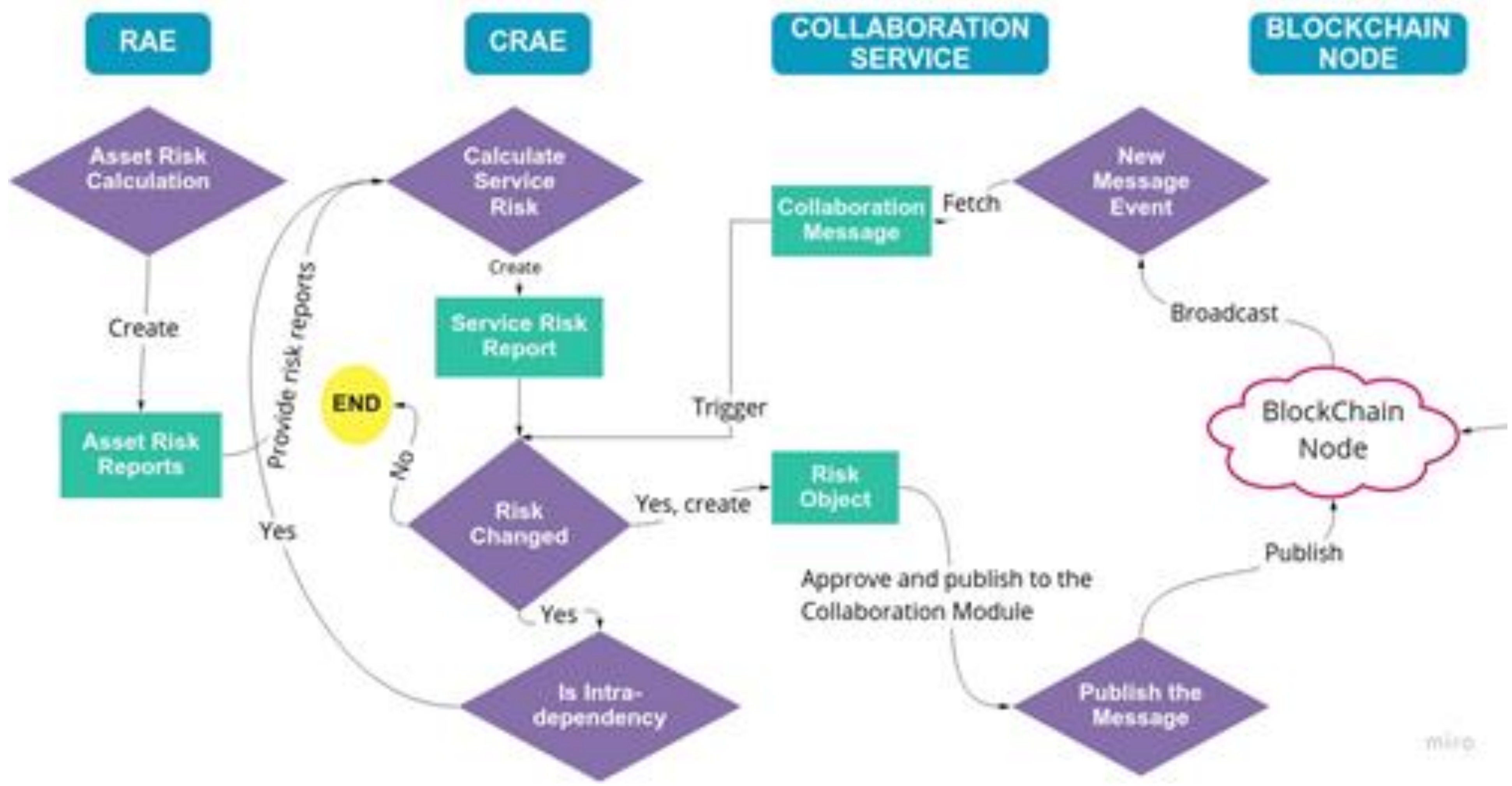


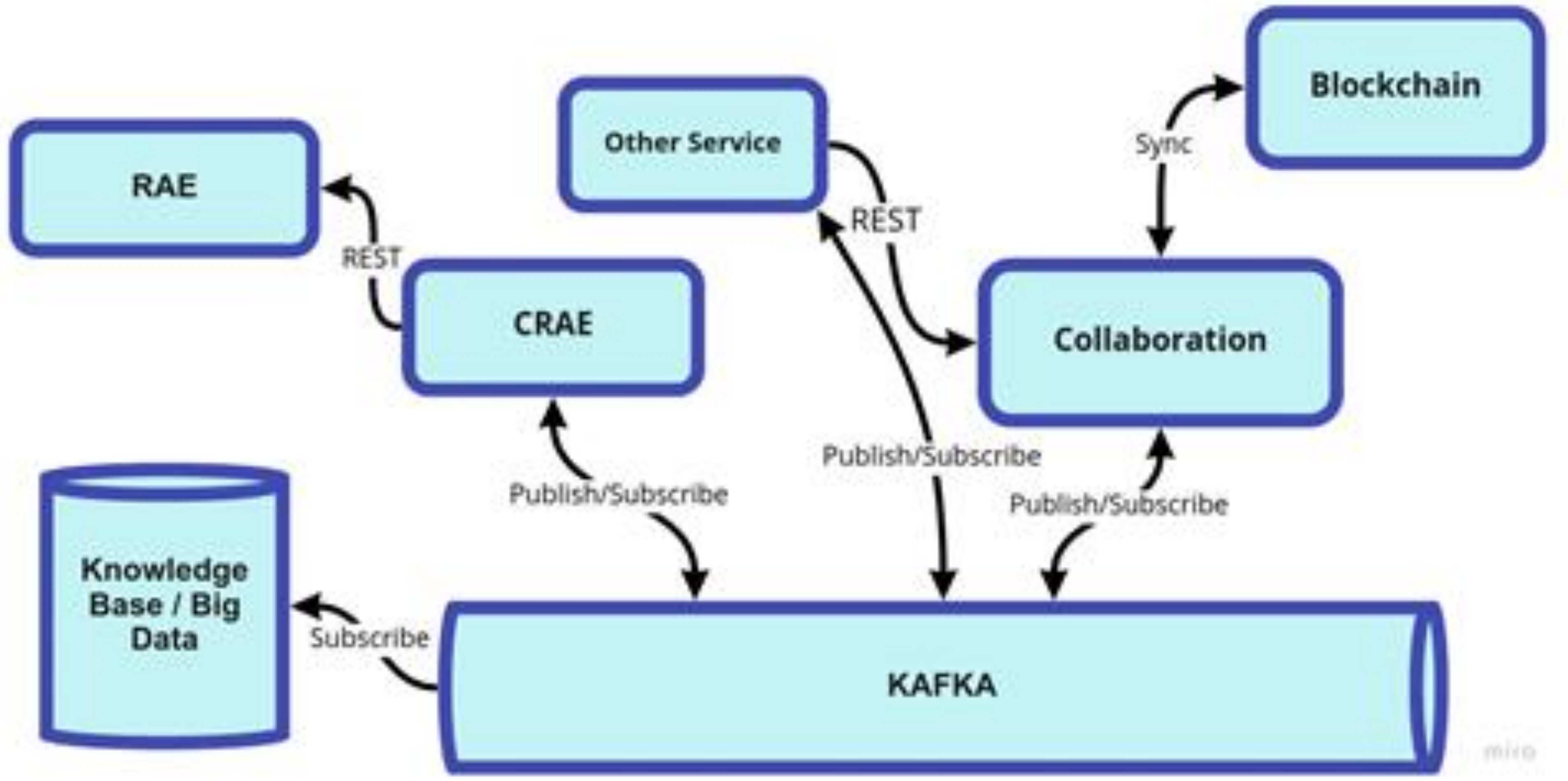
This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 786727

The FINSEC Collaborative Risk Assessment Service

FINSEC Collaborative Risk Assessment Service

- Sharing of Integrated (Cyber&Physical) Security Information through a permissioned blockchain
- Integrates the Risk Assessment Engine (RAE)
- Risk scoring triggered upon reception of security events from blockchain participants
- Key to implementing supply chain security (e.g., SEPA, SWIFT services)



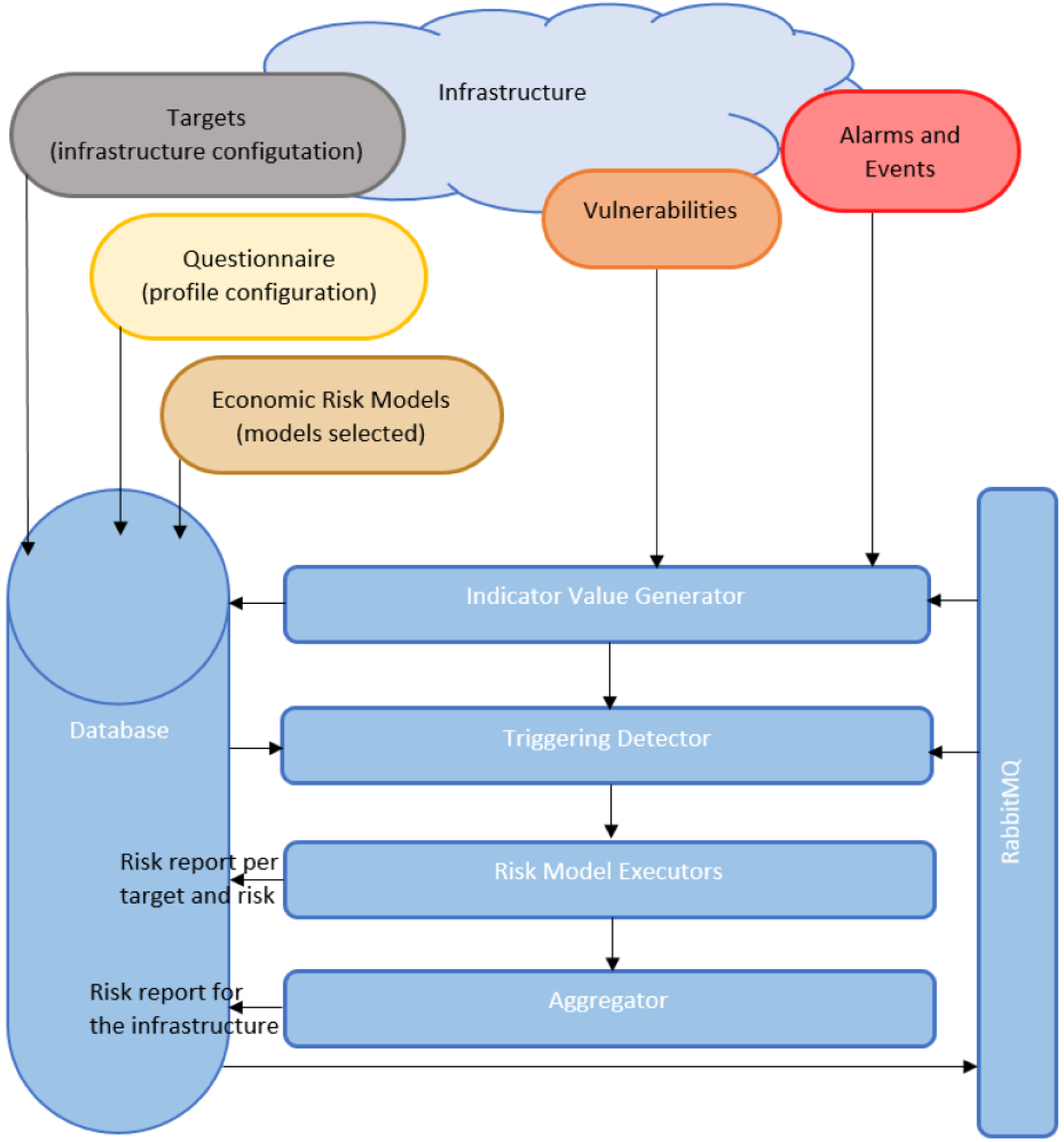


This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

The FINSEC Risk Assessment Engine

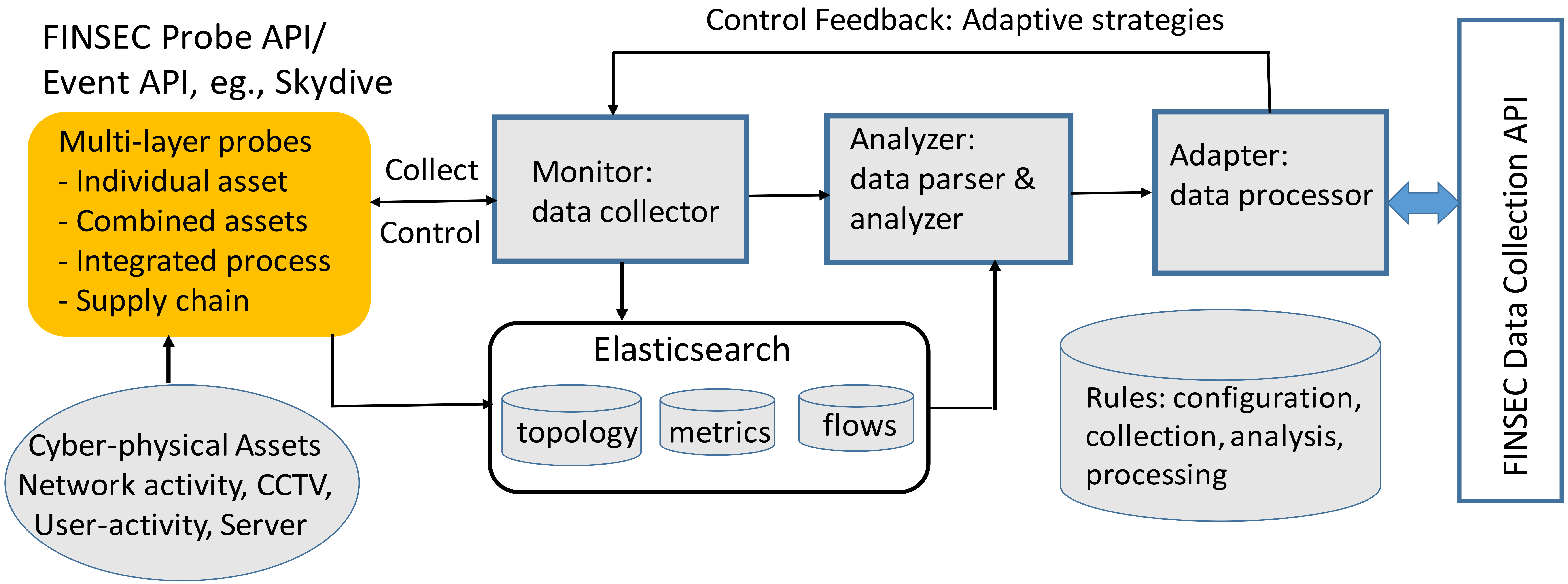
FINSEC Risk Assessment Engine

- Assess the risk level of a target financial infrastructure
- Evaluates security and economic aspects
- Security Impact assessed by CIA triad (Confidentiality, Integrity, Availability)
- Economic impact assessed through computes economic loss estimations also related with the CIA triad.



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

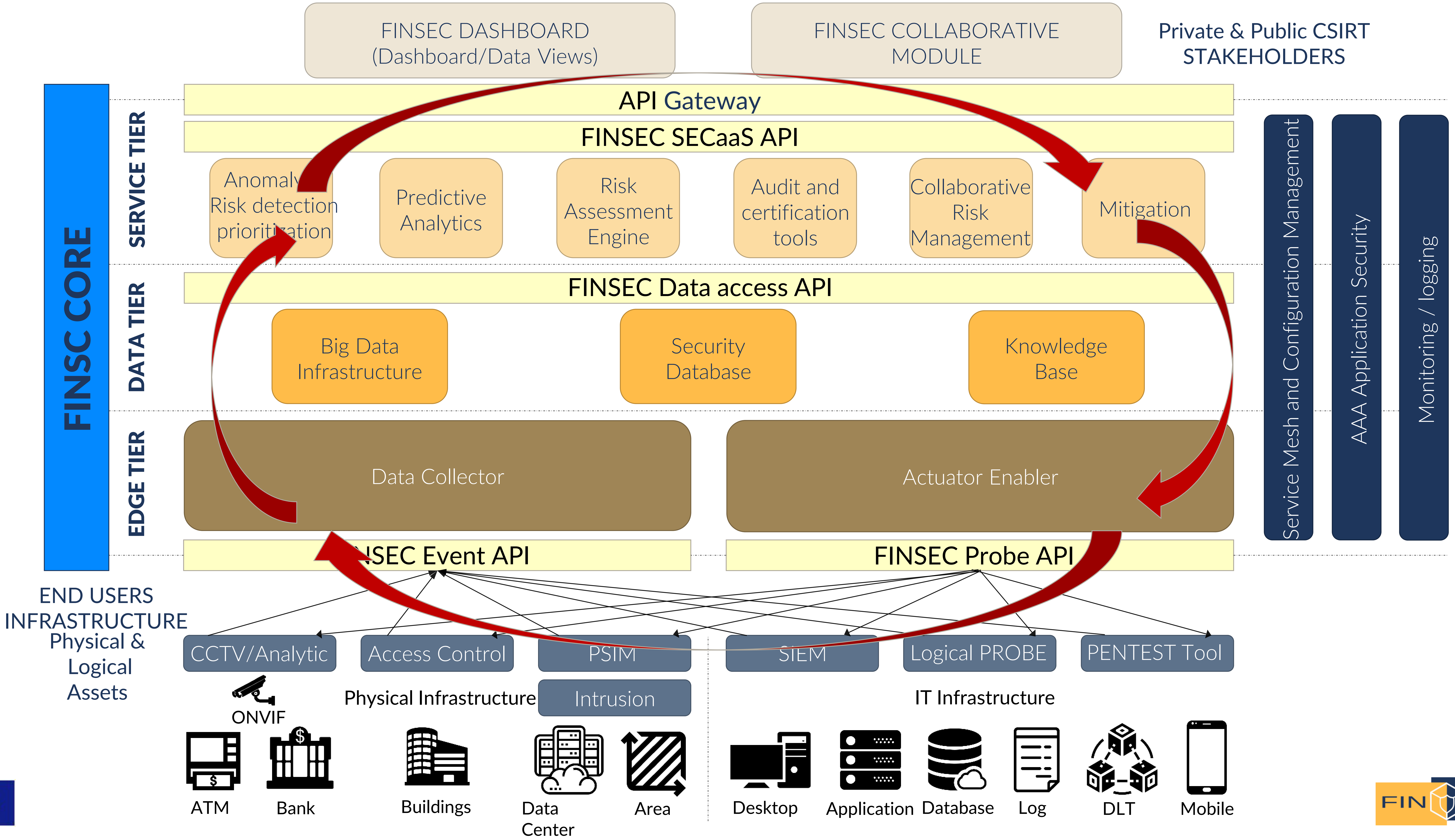
FINSEC Adaptive & Intelligent Data Collection (AIDC)



- Make Data Collection Intelligent as a means of economizing of resources and accessing the right information at the right time
- Configurable Probes and Adaptive Strategies

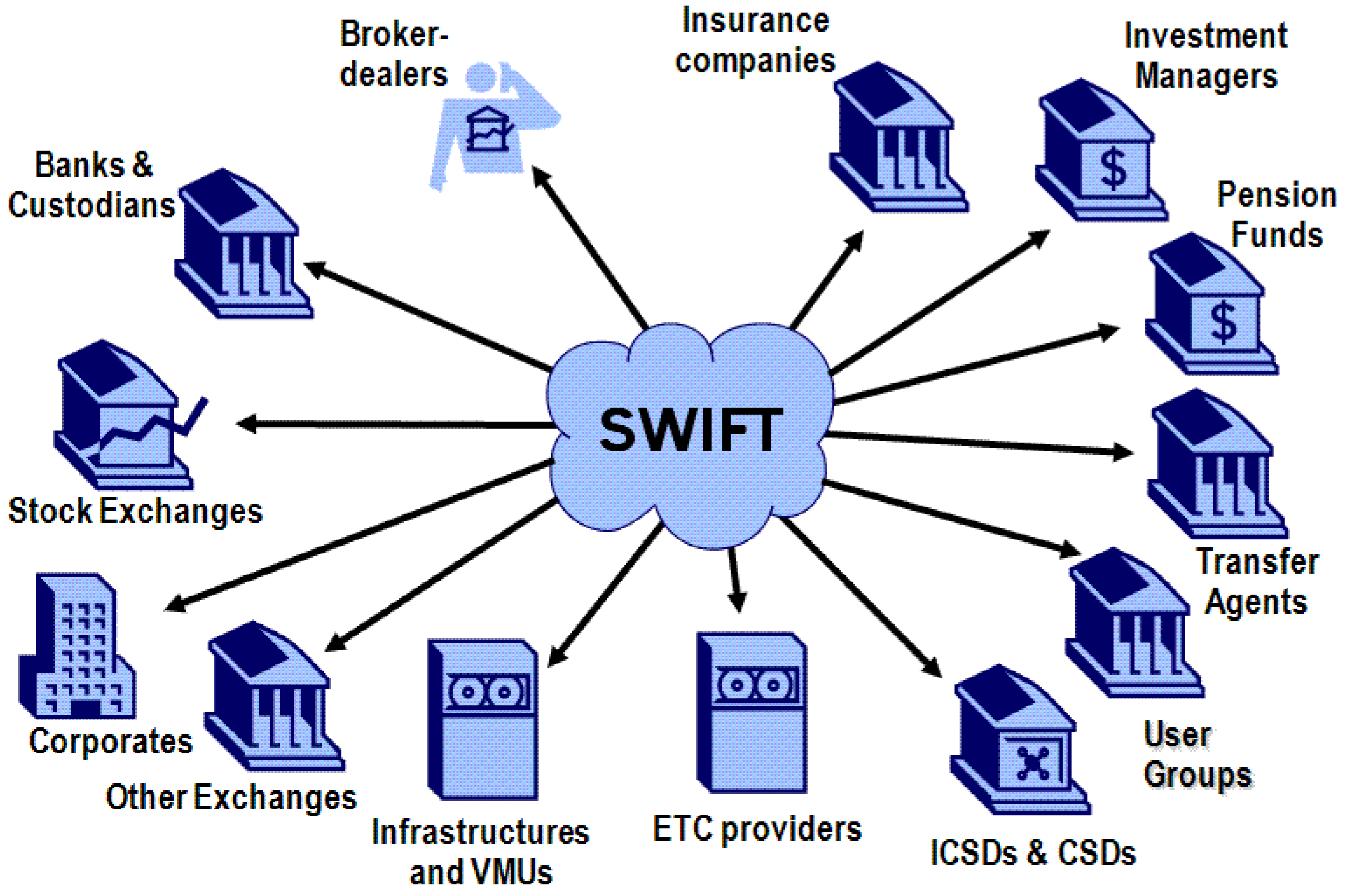
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

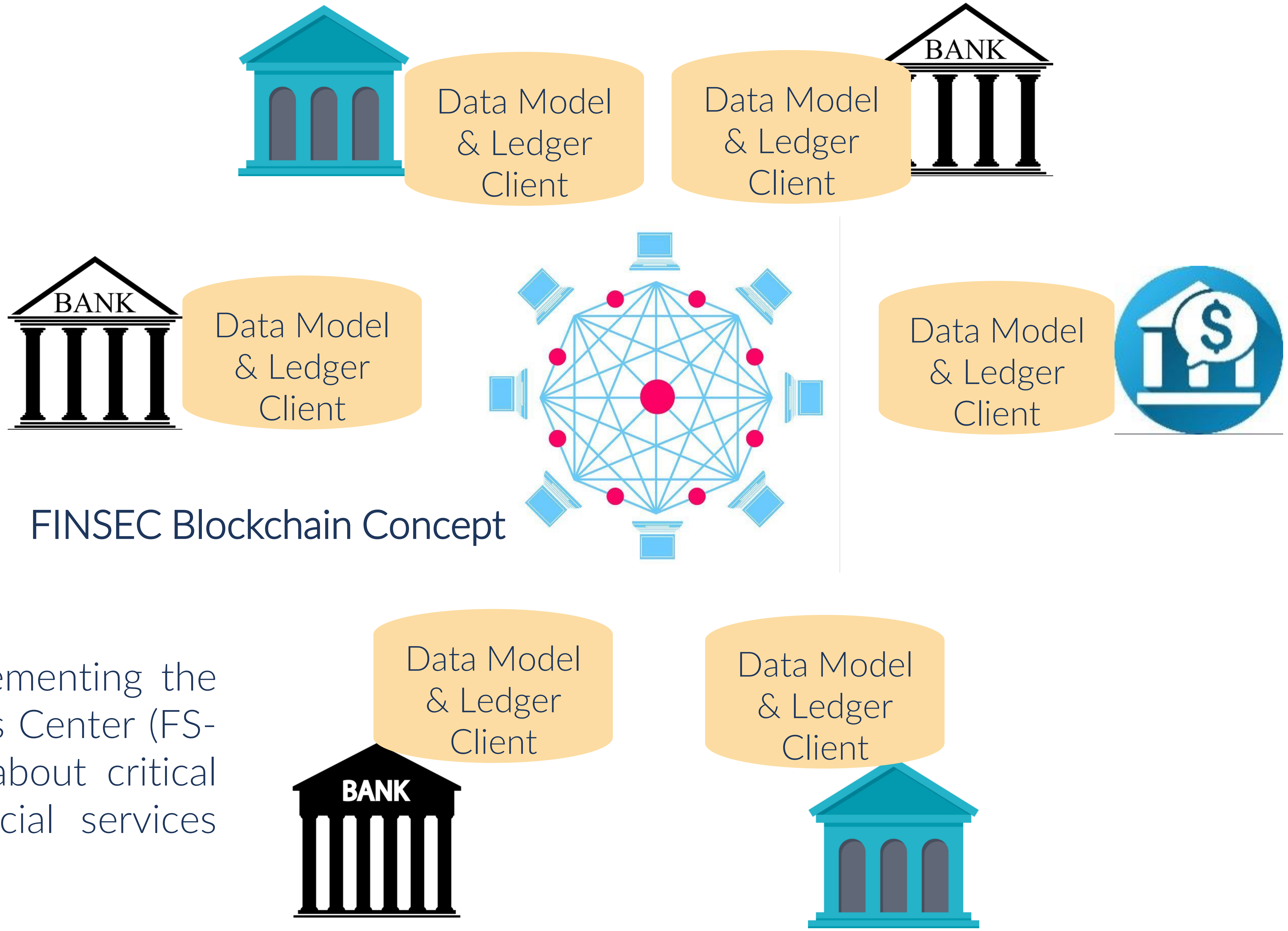
AIDC Mapping to the FINSEC Reference Architecture



FINSEC Details of Supply Chain Collaboration

Overall Blockchain Concept




BANK
Data Model & Ledger Client
Data Model & Ledger Client
BANK
Data Model & Ledger Client
Data Model & Ledger Client
Data Model & Ledger Client
BANK
Data Model & Ledger Client

FINSEC Blockchain Concept

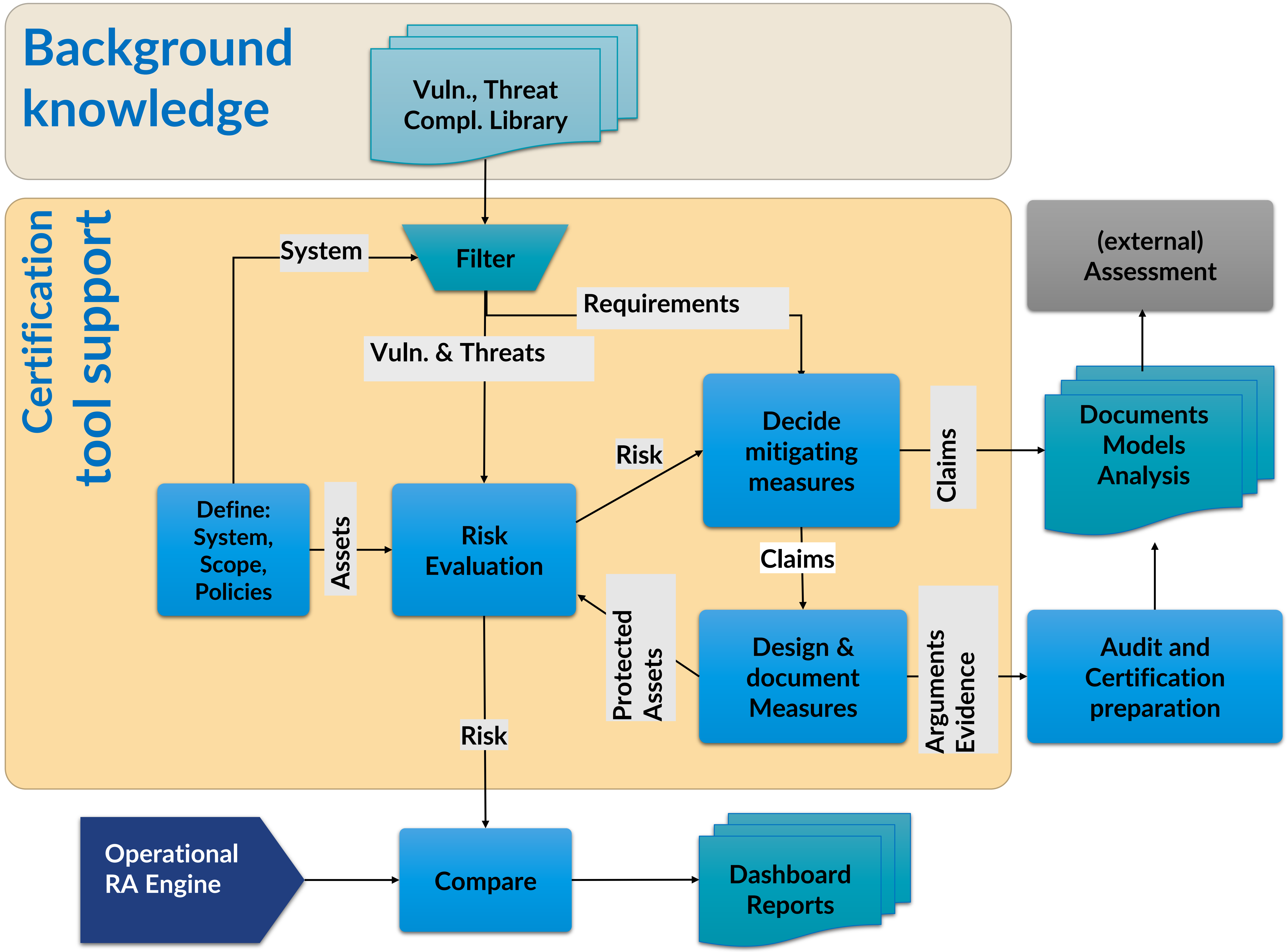
Blockchain based sharing of security data complementing the Financial Services Information Sharing and Analysis Center (FS-ISAC) i.e. the industry forum for sharing data about critical physical and cybersecurity threats in the financial services industry.

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

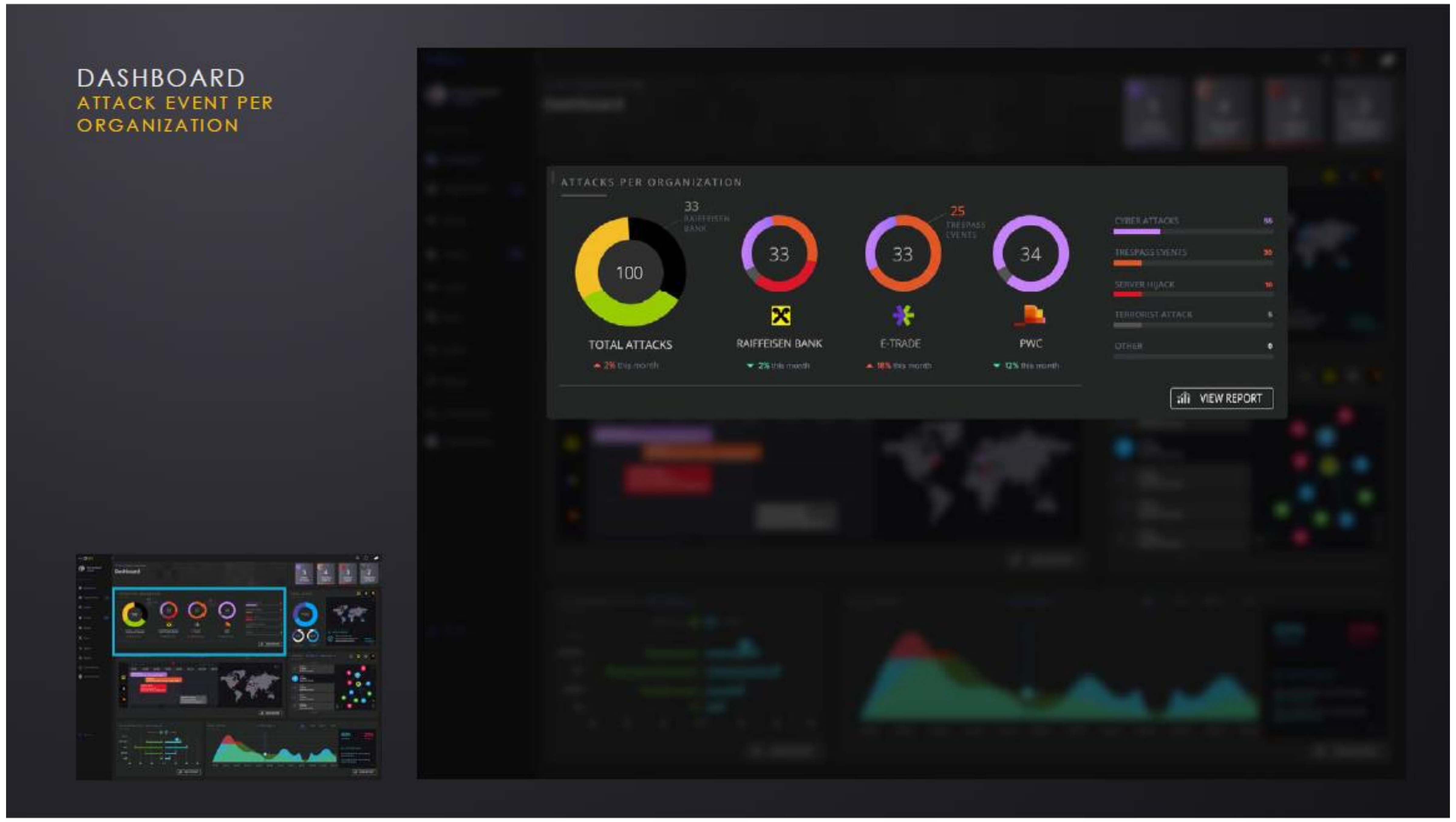
FINSEC Audit and Certification Service

FINSEC Assurance Approach

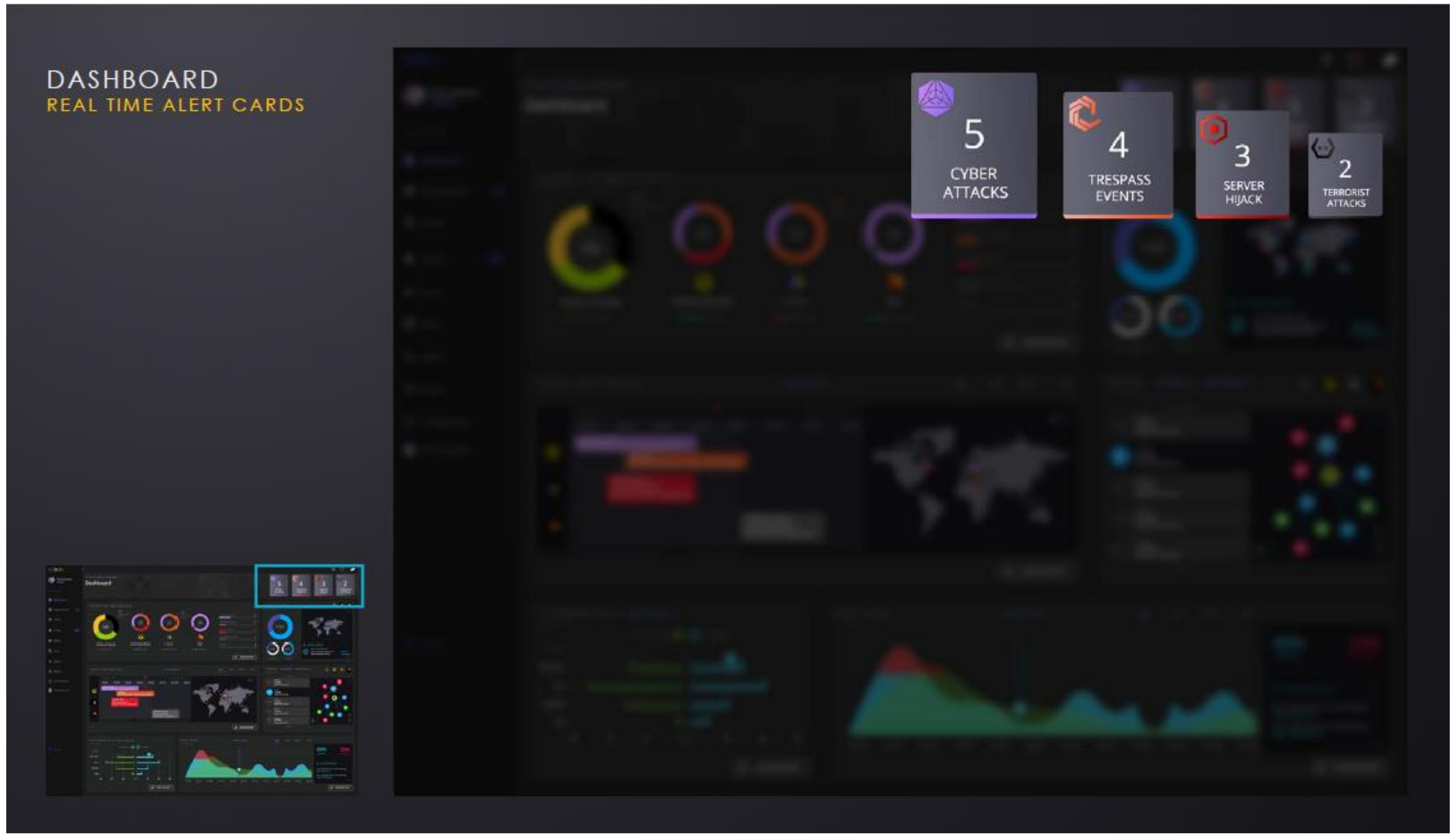
- Security activities are often uncoordinated and disconnected (e.g. cyber vs physical)
- Different knowledge and backgrounds introduces ambiguities and inconsistencies
- Integrate multiple tools; cover all key components of the security assurance value chain
- Provide interfaces to operational services (e.g. SIEM and risk engine)
- Provide arguments and evidence for technical audit & certification purposes



Snapshot of the FINSEC Dashboard



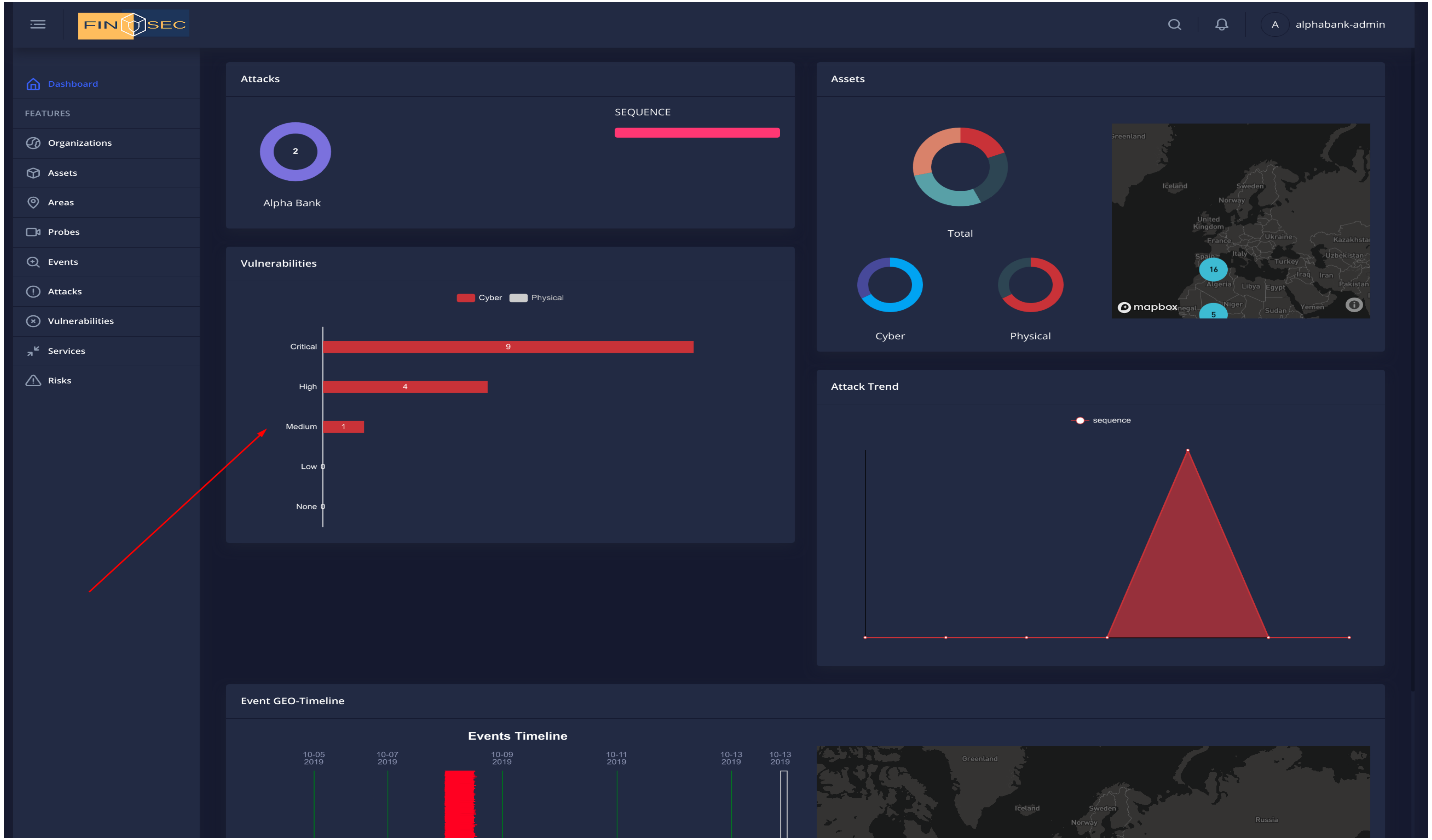
DASHBOARD
ATTACK EVENT PER ORGANIZATION



DASHBOARD
REAL TIME ALERT CARDS

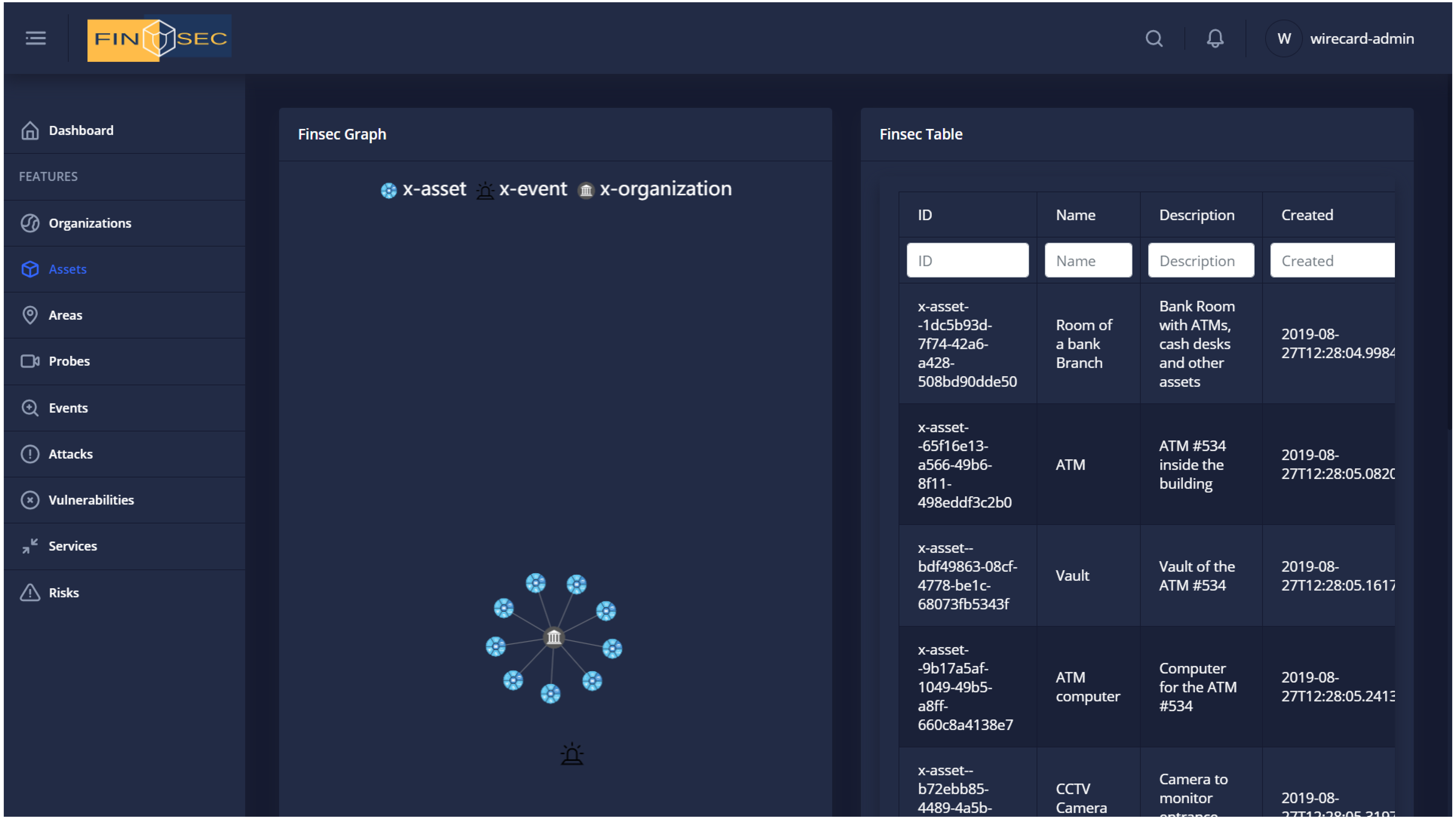
This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 786727

FINSEC Dashboard



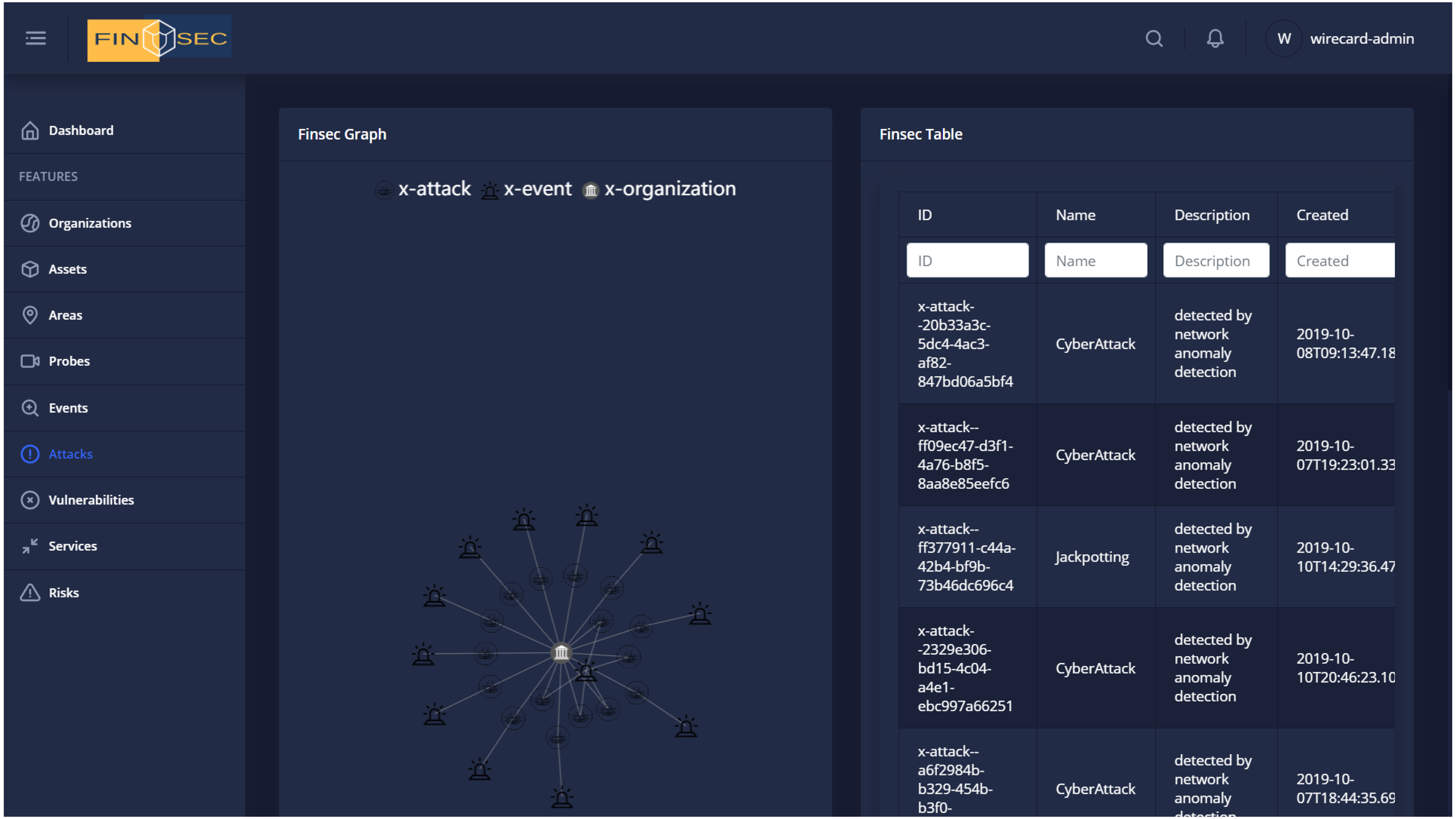
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSEC Dashboard Assets



ID	Name	Description	Created
ID	Name	Description	Created
x-asset--1dc5b93d-7f74-42a6-a428-508bd90dde50	Room of a bank Branch	Bank Room with ATMs, cash desks and other assets	2019-08-27T12:28:04.9984
x-asset--65f16e13-a566-49b6-8f11-498eddf3c2b0	ATM	ATM #534 inside the building	2019-08-27T12:28:05.0820
x-asset--bdf49863-08cf-4778-be1c-68073fb5343f	Vault	Vault of the ATM #534	2019-08-27T12:28:05.1617
x-asset--9b17a5af-1049-49b5-a8ff-660c8a4138e7	ATM computer	Computer for the ATM #534	2019-08-27T12:28:05.2413
x-asset--b72ebb85-4489-4a5b-	CCTV Camera	Camera to monitor entrance	2019-08-27T12:28:05.3197

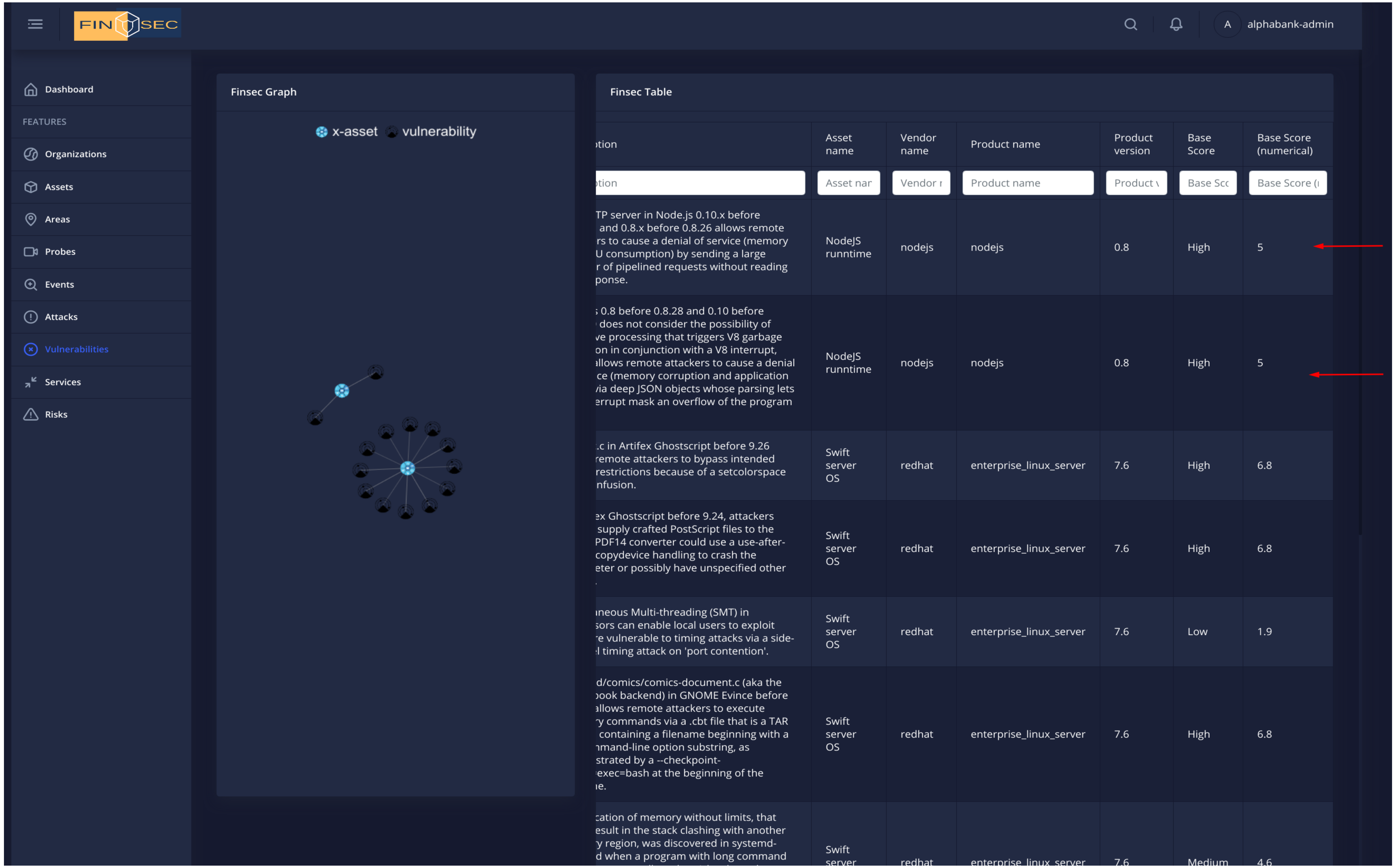
FINSEC Dashboard Attack view



ID	Name	Description	Created
ID	Name	Description	Created
x-attack--20b33a3c-5dc4-4ac3-af82-847bd06a5bf4	CyberAttack	detected by network anomaly detection	2019-10-08T09:13:47.18
x-attack--ff09ec47-d3f1-4a76-b8f5-8aa8e85eefc6	CyberAttack	detected by network anomaly detection	2019-10-07T19:23:01.33
x-attack--ff377911-c44a-42b4-bf9b-73b46dc696c4	Jackpotting	detected by network anomaly detection	2019-10-10T14:29:36.47
x-attack--2329e306-bd15-4c04-a4e1-ebc997a66251	CyberAttack	detected by network anomaly detection	2019-10-10T20:46:23.10
x-attack--a6f2984b-b329-454b-b3f0-	CyberAttack	detected by network anomaly detection	2019-10-07T18:44:35.69

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Snapshot of the FINSEC Dashboard

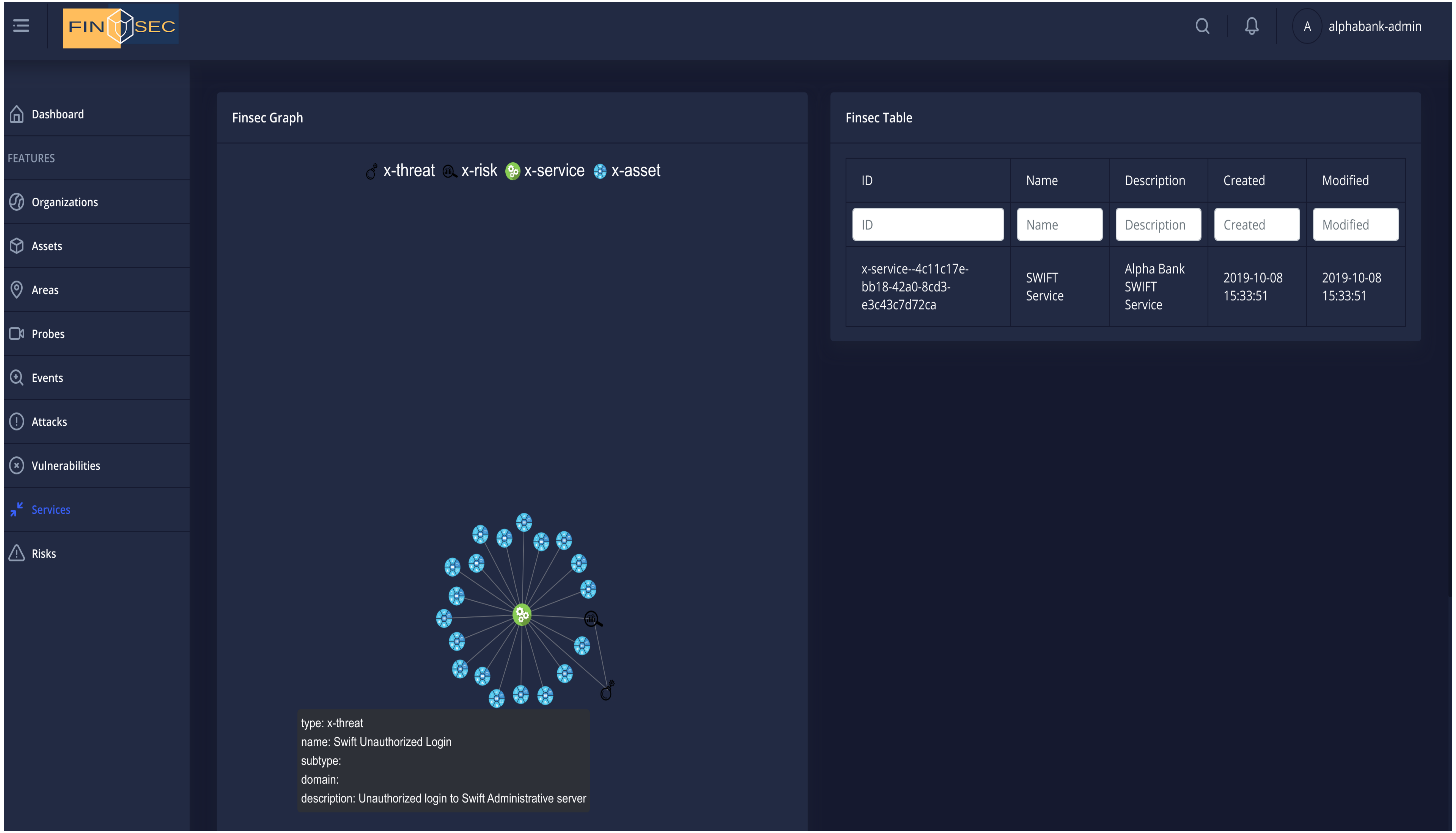


Finsec Table

›tion	Asset name	Vendor name	Product name	Product version	Base Score	Base Score (numerical)
›tion	Asset nar	Vendor ı	Product name	Product \	Base Scc	Base Score (ı
TP server in Node.js 0.10.x before and 0.8.x before 0.8.26 allows remote rs to cause a denial of service (memory U consumption) by sending a large r of pipelined requests without reading ponse.	NodeJS runntime	nodejs	nodejs	0.8	High	5
; 0.8 before 0.8.28 and 0.10 before does not consider the possibility of ve processing that triggers V8 garbage on in conjunction with a V8 interrupt, ıllows remote attackers to cause a denial ce (memory corruption and application via deep JSON objects whose parsing lets errupt mask an overflow of the program	NodeJS runntime	nodejs	nodejs	0.8	High	5
.c in Artifex Ghostscript before 9.26 remote attackers to bypass intended restrictions because of a setcolorspace nfusion.	Swift server OS	redhat	enterprise_linux_server	7.6	High	6.8
ex Ghostscript before 9.24, attackers supply crafted PostScript files to the PDF14 converter could use a use-after- copydevice handling to crash the eter or possibly have unspecified other .	Swift server OS	redhat	enterprise_linux_server	7.6	High	6.8
ıneous Multi-threading (SMT) in sors can enable local users to exploit re vulnerable to timing attacks via a side- l timing attack on 'port contention'.	Swift server OS	redhat	enterprise_linux_server	7.6	Low	1.9
d/comics/comics-document.c (aka the book backend) in GNOME Evince before ıllows remote attackers to execute y commands via a .cbt file that is a TAR containing a filename beginning with a nmand-line option substring, as strated by a --checkpoint- exec=bash at the beginning of the ıe.	Swift server OS	redhat	enterprise_linux_server	7.6	High	6.8
cation of memory without limits, that esult in the stack clashing with another y region, was discovered in systemd- d when a program with long command	Swift server	redhat	enterprise_linux_server	7.6	Medium	4.6

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Vulnerabilities filtered by product name



type: x-threat
name: Swift Unauthorized Login
subtype:
domain:
description: Unauthorized login to Swift Administrative server

Finsec Table

ID	Name	Description	Created	Modified
ID	Name	Description	Created	Modified
x-service--4c11c17e-bb18-42a0-8cd3-e3c43c7d72ca	SWIFT Service	Alpha Bank SWIFT Service	2019-10-08 15:33:51	2019-10-08 15:33:51

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Scientific Background

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Scientific Contribution

- Physical and Cyber security integration and modeling
- Adaptive and intelligent monitoring and data collection
- Predictive analytics for the identification of complex attack patterns
- Adaptive anomaly detection for a multivariate analysis of dynamic data patterns
- Increased automation for detection, prevention and mitigation measures for attacks
- Collaboration in vulnerability assessment, risk analysis, threat identification, threat mitigation, and compliance
- Data Model and FINSTIX enhancement to STIX standard

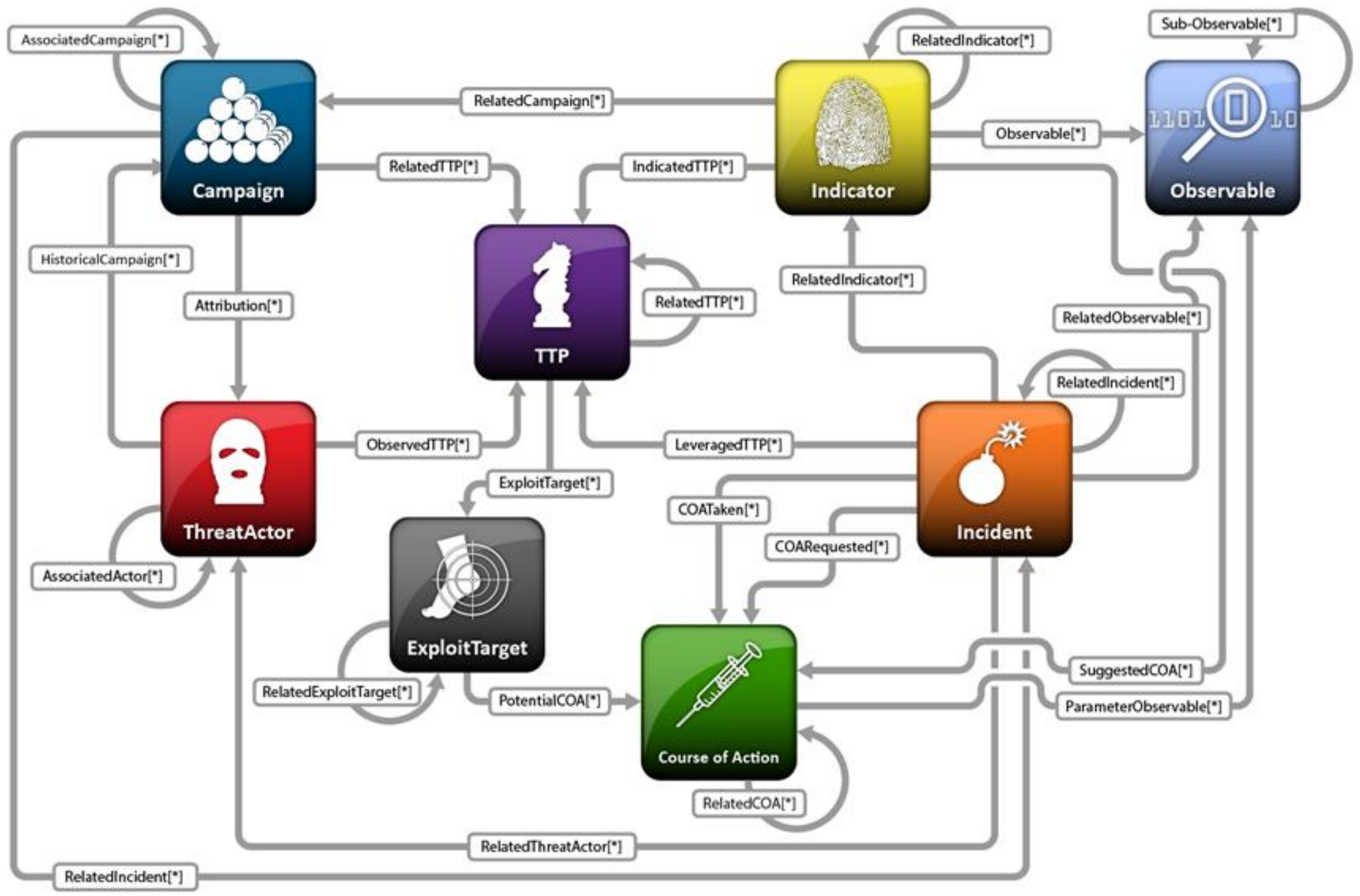
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

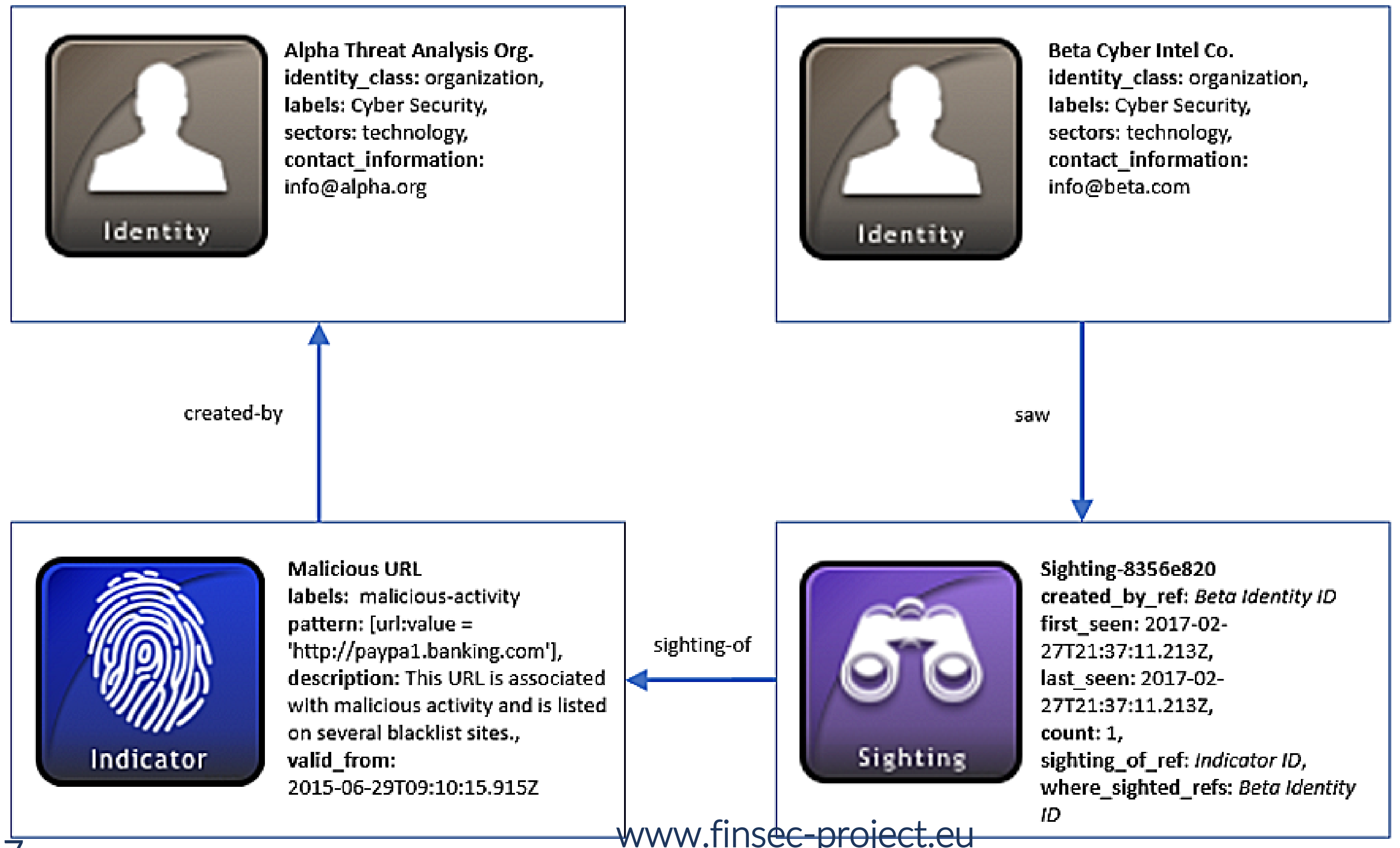
Data Model

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Integrated Security Information Modelling: From STIX to FINSTIX

- STIX (Structured Threat Information eXpression):
  - Standardized XML programming language for conveying data about cybersecurity threats
  - Easily understood by humans and security technologies
  - Main Entities: Observable, Incident, Threat Actor…
- FINSTIX
  - STIX Instantiation in FINSEC
  - Enhancement of new objects
  - Copes with Logical and Physical incidents





Alpha Threat Analysis Org.
identity_class: organization,
labels: Cyber Security,
sectors: technology,
contact_information:
info@alpha.org

Beta Cyber Intel Co.
identity_class: organization,
labels: Cyber Security,
sectors: technology,
contact_information:
info@beta.com

Malicious URL
labels: malicious-activity
pattern: [url:value =
'http://paypa1.banking.com'],
description: This URL is associated with malicious activity and is listed on several blacklist sites.,
valid_from:
2015-06-29T09:10:15.915Z

Sighting-8356e820
created_by_ref: *Beta Identity ID*
first_seen: 2017-02-27T21:37:11.213Z,
last_seen: 2017-02-27T21:37:11.213Z,
count: 1,
sighting_of_ref: *Indicator ID*,
where_sighted_refs: *Beta Identity ID*

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSTIX Principles (1)

FINSTIX	Variant of STIX2 - Extends STIX2 into the physical and logical domain
Basic object	Sequence of key-values that can be passed as JSON
General object	Aggregate of more objects and relations still expressed in JSON
Extensions	Shall include information relevant to the financial sector
Integrated Security	Defines other objects and relations to STIX2 to cope with the correlation of physical and logical data

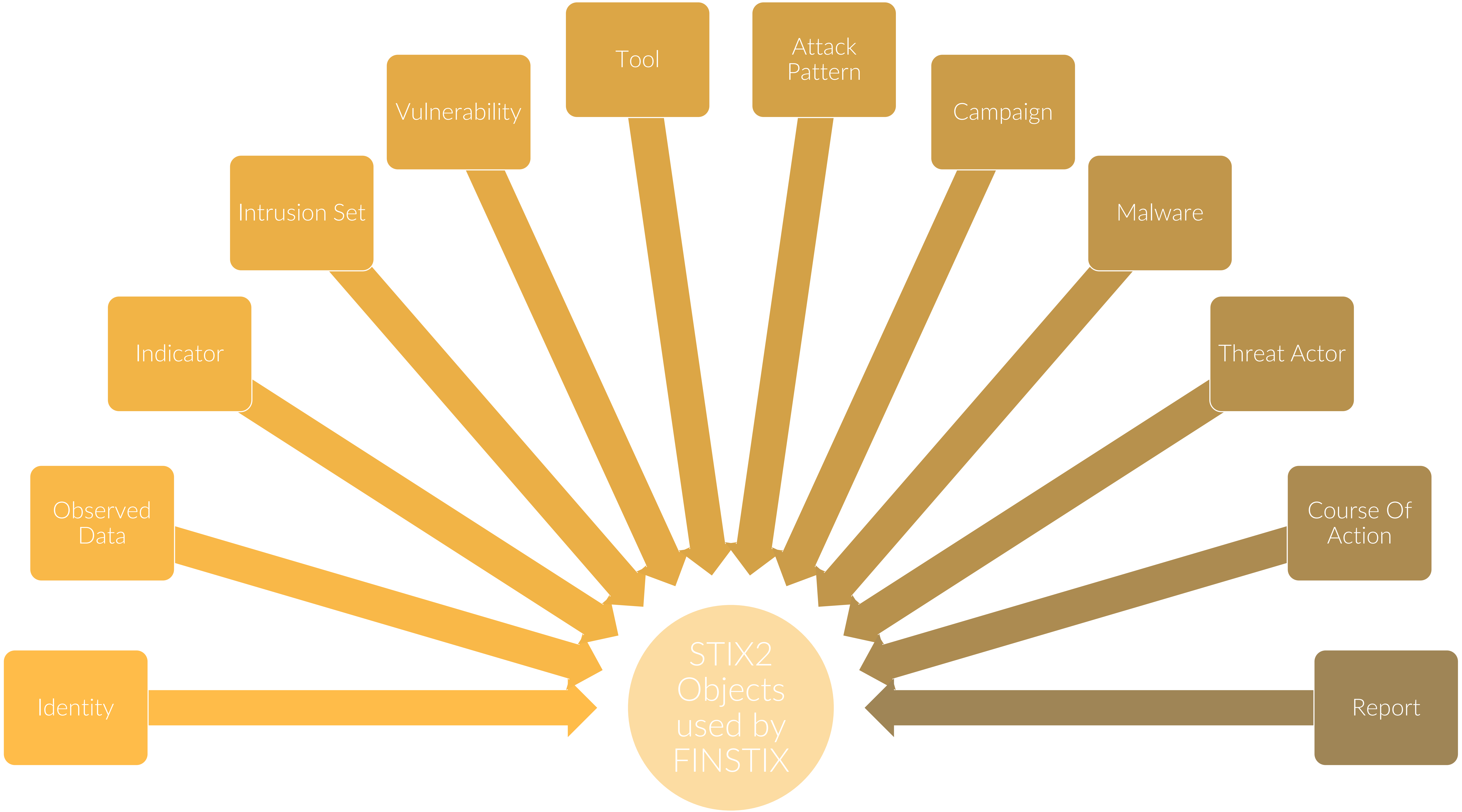
This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSTIX Principles (2)

Probes	Generate Observed Data, Events, Incidents, Logs (observed data) according to the FINSTIX Data Model
Data Collectors (DC)	Gather data from probes normalizing, sanitizing, prioritizing and storing CPTI into the Data Layer.
Asset Model (AM) and Knowledge Base (KB)	Represented with FINSTIX objects as well.
Analytics/Predictive algorithms	Use events, observed data, the Knowledge base and Asset Models to produce Cyber Physical Threat Intelligence (CPTI vs CTI).

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

STIX2 objects in FINSTIX



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSTIX Extensions and Custom Objects (1)

Organization

Asset

- Organization’s valuable infrastructure. PCs, server rooms, ATMs, applications etc.

Area of Interest

- Logical/physical area inside an asset

Service

- Collection of assets forming a publicly exposed service

Probe

- Monitoring infrastructure

Probe Configuration

- Data sent to a probe in order to configure details of the monitoring process

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 786727

FINSTIX Extensions and Custom Objects (2)

Event

- Information of something happened/happening;

Person

- Extension to the STIX Identity used to describe people involved in the events

Risk

- Calculated risk for a specific asset or service

Risk Configuration

- Optimizes the risk assessment

Regulation

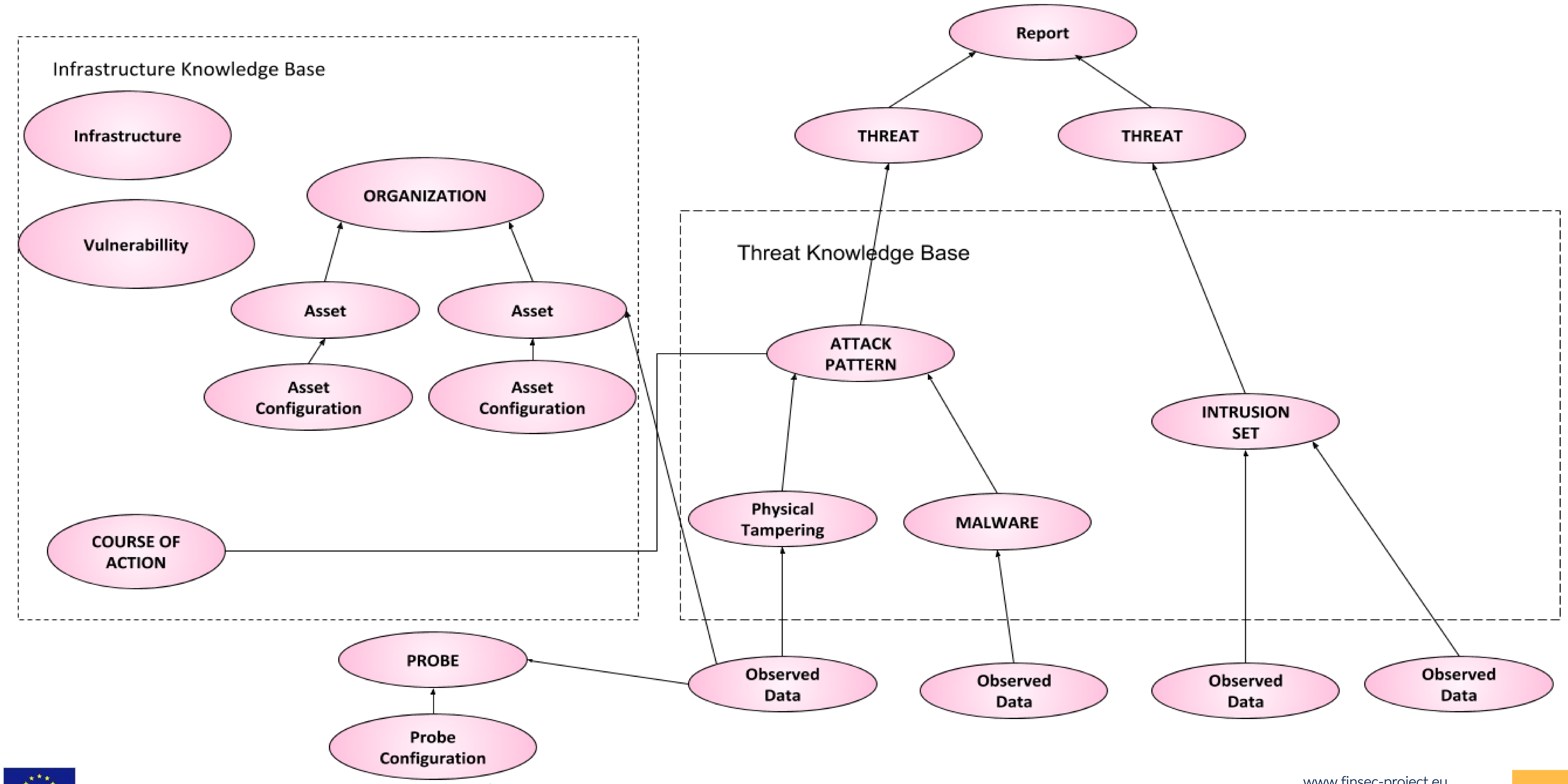
- An object used to depict a regulation violation

CPTI

- Enriched by threat information as soon as they are gathered from the probes and processed by the Predictive Analytics module

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSTIX Entities Snapshot



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

The Pilots

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSEC Pilots

#	Pilot & Critical Infrastructure (CI)	FINSEC Toolbox Services Used	FINSEC Added-Value	Partners Involved
1	Attacking the SWIFT Network	SIEM, Anomaly Detection, RAE, Collaborative Analysis & Management (RAS, RMS, SCCS)	Handling of Integrated Attacks; Early Preparation; Stakeholder's Collaboration in Risk Assessment	ALPHA, AS, GFT, NRS
2	Correlating Physical and Cyber Attacks in Buildings	Predictive Security, SIEM, RAE, Collaborative Assessment (RAS, RMS, DMS, SCCS), Anomaly Detection, CCTV, ATM Network Security Platform	Automation in the identification and correlation of events associated with the buildings of financial institutions; Increased accuracy due to stakeholders' collaboration	NEXI, GFT, FUJITSU WIRE, UTI, CNR, NRS
3	Predictive Protection of Peer-to-Peer Payments Infrastructure	Predictive Security, SIEM, RAE, Vulnerability Scanning, Anomaly Detection	Early identification of vulnerabilities of blockchain; Identification, assessment and mitigation of internal threats	SIA, GFT, AS, HPE
4	Protecting the infrastructures of small financial institutes through Security-as-a-Service (SECaaS)	Predictive Security, SIEM, RAE, Collaborative Assessment (RAS, REM, DMS, SCCS), Anomaly Detection	Cost-reduction based on the deployment of the SECaaS model; Timely prevention of attacks against connected infrastructure (using the SMEs infrastructures as entry point)	JRC, AS, CNR
5	Insurance & Risk Management in Public Infrastructures	Predictive Security, SIEM, RAE, Collaborative Assessment (RAS, RMS, SCCS)	Accurate risk assessment for complex infrastructures with interlinked assets; Improved insurance contracts	HDI, GFT, FBK

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

ATM Pilot Overview

Use Case Overview

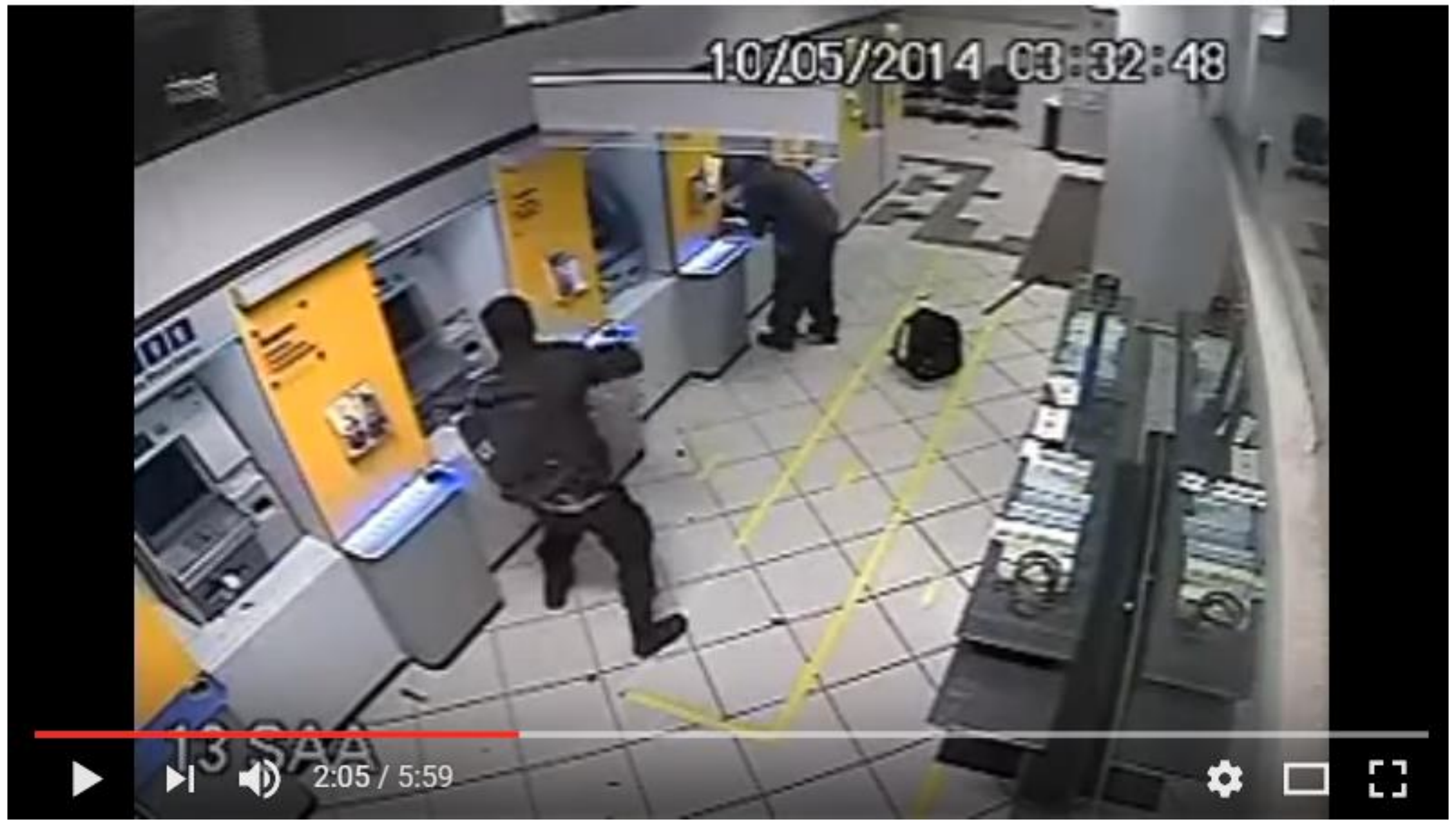
- ATM Supervised by two (2) cameras (inside the ATM & one more environmental camera)
- ATM has a vault and a PC in two different areas that are accessible to authorized personnel
- Physical attack sensors will be used (e.g., vibration sensors and magnetic contacts for the doors of the ATM) to check whether maintenance actions from authorized people take place

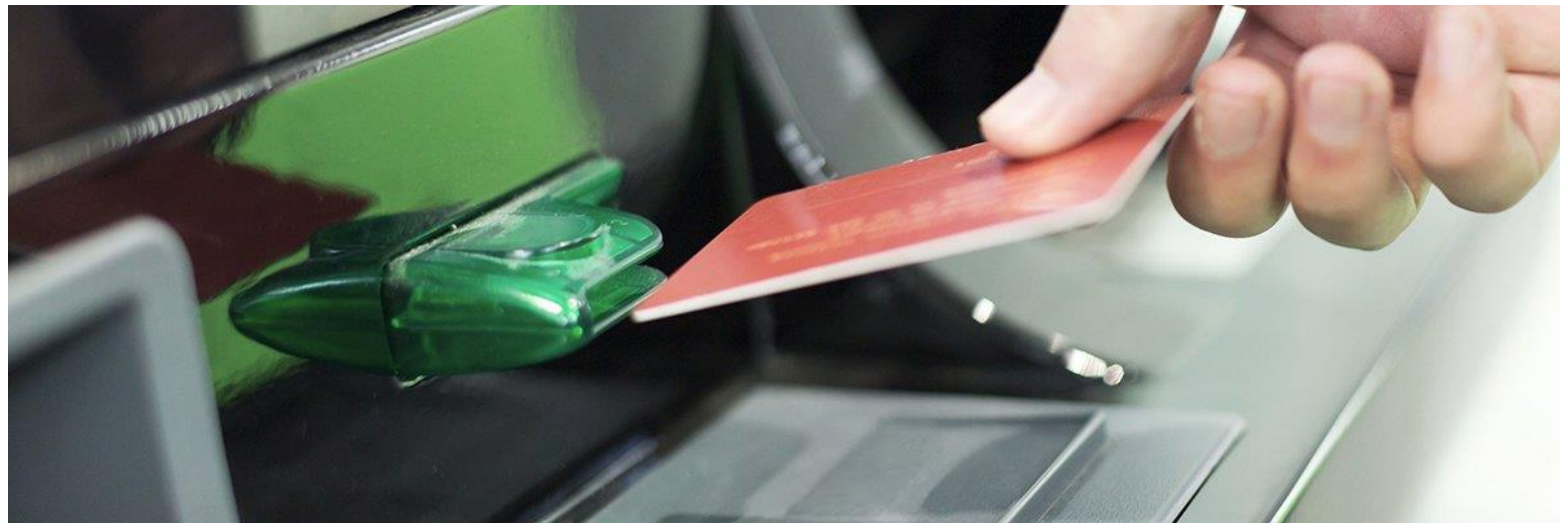
Physical Assets

- PC and Vault
- Connection between PC and Vault
- Printer
- Sensors provide information on the physical status of the object

Attack Scenarios / Possibilities:

- Scenario 1: Client is the Physical Adversary
- Scenario 2: Somebody else is the Adversary that wants to attack through the Client
- Scenario 3: Cyberattack such as malware to PC or the network
- Scenario 4: Attach the PC to get remote control (Jackpot attack) - Order to Dispense the Cash Challenge: The Malicious software gets on the ATM and it's not possible to detect it from remote (e.g., remote management events)





This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Events Captured

Most based on AI over CCTV:

- Person Entering the ATM area
- In front of ATM
- Description Accessories (No Mask, Large/Big Luggage)
- No Card Event - No Keyboard Events
- Person Reappearing
- Vibration Sensor to Check Open Case
- Interaction between People (Very Short Distance between two persons)
- People Fighting
- Waiting in line or not
- Person Leaving

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 786727

Typical Script

Flow of Security Events

- Someone is entering the ATM area
- The person is carrying luggage
- The person is approaching the ATM and uses a card
- The person performs activity in the vicinity of the ATM
- Loitering
- Attack a person already present in front of the ATM
- Attack the ATM
- The probe is sensing vibrations
- The person is vandalizing the camera
- Unauthorized extraction of money (several times)
- Loss of communication
- Attacking the system (connecting to the local IT system of the ATM)

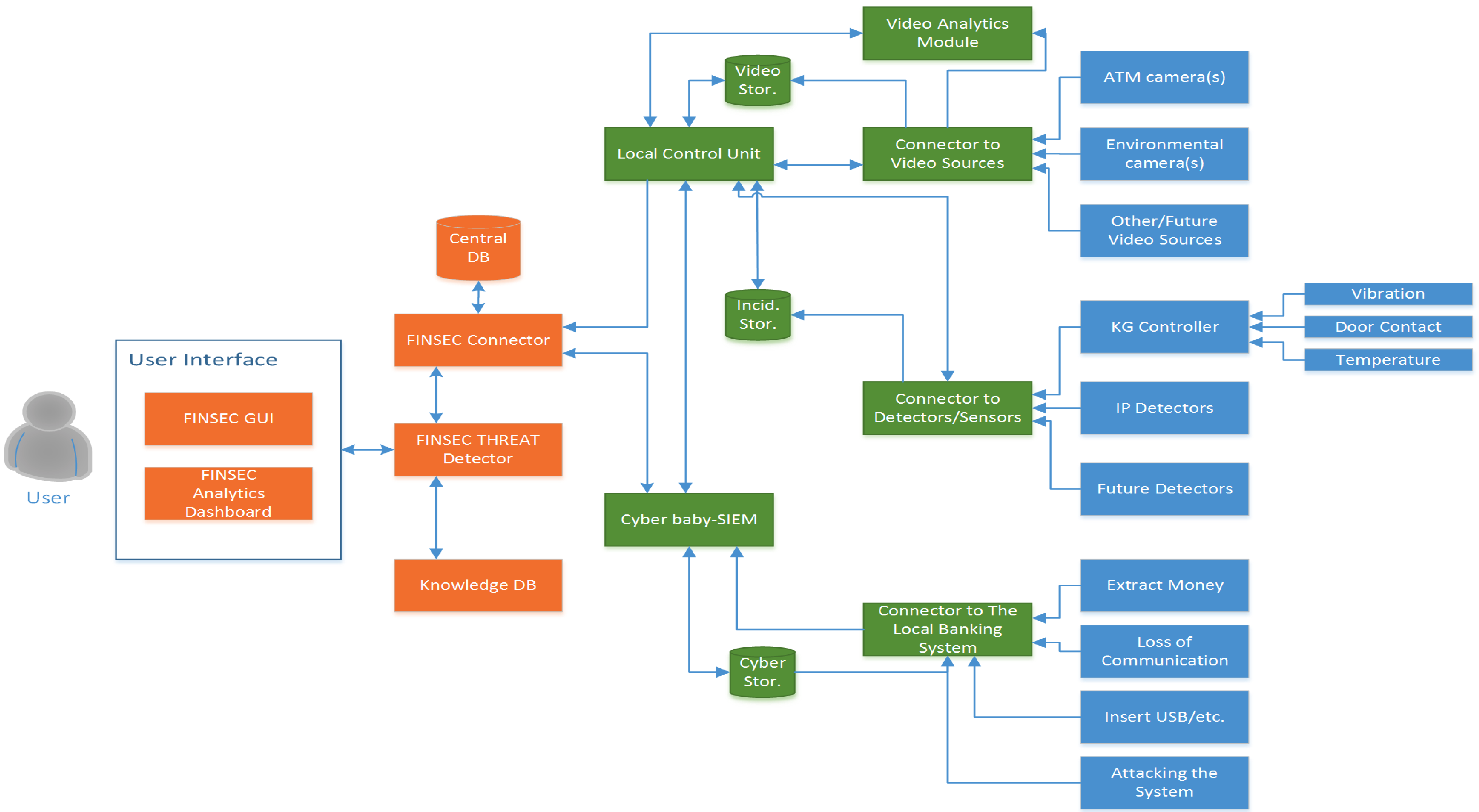
Security Measures & Functionalities

- Risk assessment levels are computed & tuned automatically
- Alerts are produced and disseminated to security personnel
- Information is visualized and analyzed

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Architecture of ATM Pilot Scenario

Functional Blocks Diagram



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Other FINSEC Pilots (1)

NEXI (Banking)

- Unauthorized physical access to Data Center
- Check Dual Control mechanism for physical access to secured area/secure elements (safe, rack...)

HDI (Insurance)

- Reliability and anti-tampering of data in the scope of the insurance contract underwriting process.

SIA (Payments/Blockchain)

- Protect DCASH in terms of the SIAchain (blockchain), the GB Cash Collateral Accounts (CCAs) and digital wallets;
- Detect accesses and intrusions to relevant data centers rooms.
- Protect the nodes from cyber attacks

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

Other FINSEC Pilots (2)

JRC (Trading/Investments)

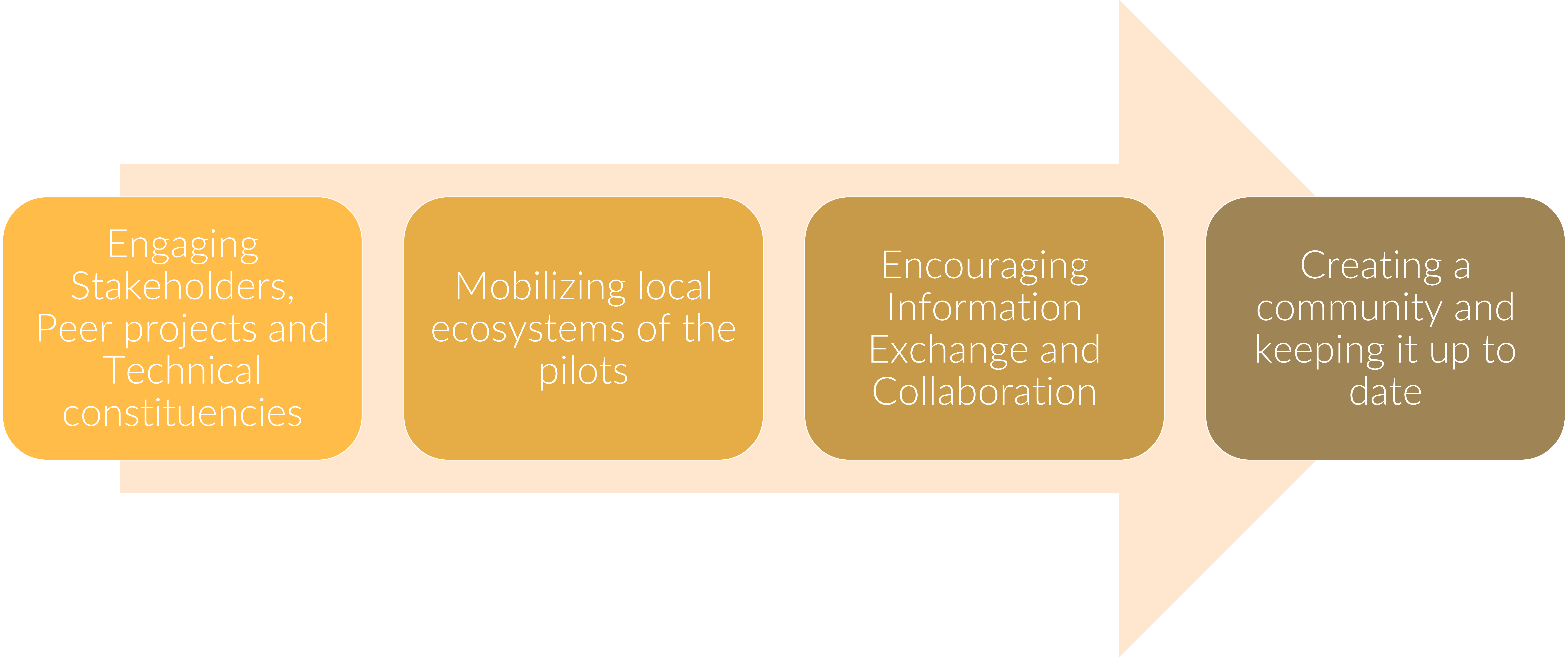
- Protection form property theft, with a specific interest on intellectual property (e.g. algorithmic trading strategies)
- Detect any other fraudulent behavior

APLHA (SWIFT System)

- Correlate of physical intrusion to the SWIFT room/data center (e.g., unauthorized access) with cyber-security attacks (e.g., log-in attempts)
- Stakeholders: SWIFT Administrators, Cyber Security & Physical Security Departments

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727

FINSEC Stakeholders Alliance



Engaging Stakeholders, Peer projects and Technical constituencies

Mobilizing local ecosystems of the pilots

Encouraging Information Exchange and Collaboration

Creating a community and keeping it up to date

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement no 786727

EU Project Roadmap

- Project is completing its 18th Month out of 36 (50%)
- Minimum Viable Platform completed
- First wave of Pilots will be completed end of October
- Second wave mid 2020
- Full Platform end of 2020
- Marketplace launch end of 2020
- Final Pilots March 2021

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement no 786727