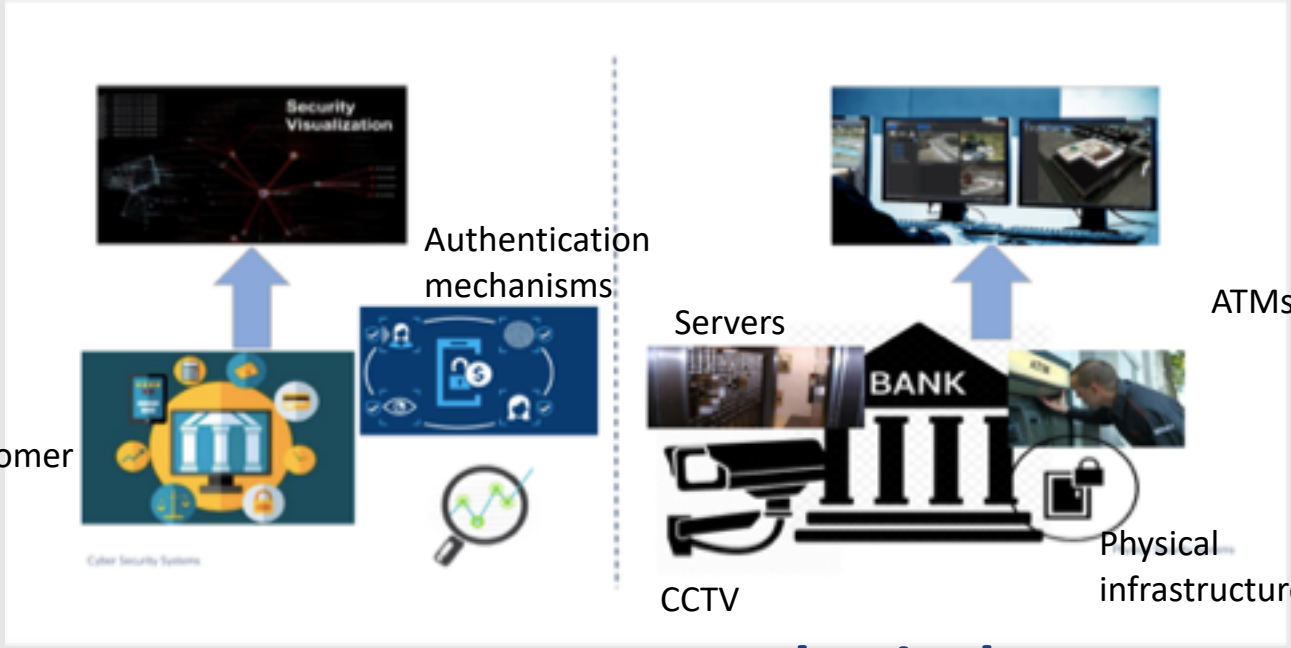
Securing Critical Infrastructures In The Financial Sector

Integrated Security

Understanding the need for collaborative security

Examples of physical and cyber assets



Business motivation for integrated security

Cyber and physical security “SILOs”

Four models of attacks:

- Attacks with only physical aspects
- Attacks with only cyber aspects
- Physical-enabled cyberattacks
- Cyber-enabled physical attacks

Integrated solutions:

- Augmented vulnerability assessment methodology for physical security in the cyber domain, Vulnerability Assessment (VA), proven based on simulation and cost-benefit analysis
- Integrated modelling approach for cyber-physical systems for power grids and critical infrastructures for energy

Business motivation for integrated security (cont.)

- Integrated security methodologies based on various disciplines and techniques e.g., control theory, optimization, game theory
- do not take a holistic data-driven approach

- Data driven systems do not provide the non-functional properties (e.g., scalability, performance) needed for their deployment at scale

- Rarely address the special requirements of the financial sector: asset modelling, event correlation and regulatory compliance (e.g., MiFID, GDPR, PSD2)

Existing reference architectures

- **Industrial Internet Reference Architecture (IIR):** focus on the implementation of systems with both cyber and physical parts [typical examples of OT (Operational Technology) and IT (Information Technology) convergence
- **Internet Security Framework (IISF):** specifies security functions for IIoT systems which comprise cyber and physical assets

Influence the development of platforms for integrated security:

Design of Horizontal Security Functionalities
Specification of Data-Driven Security Functionalities

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

1.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

2.Poor Stakeholders’ Collaboration

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

How is FINSEC addressing Integrated Security?

- Integrated Architecture
- Integrated Threat Modelling: FINSTIX, Security Knowledge base (introduced later in this course) → transforming observed data from the physical and digital world into Threat Intelligence information
- Correlation of Cyber-Physical Information (introduced later in this course) → Integrated Cyber-Physical Information Sharing

The FINSEC Reference Architecture

FINSEC RA: Driving Principles

Data driven principle	• enables the development, deployment and integration of data driven security systems • emphasis on the collection & processing of security data, flow across the financial services supply chain
Separation of Aspects and Concerns	• Reference Architecture Logical Design defined in term of (services) modules • every single module of the architecture should do one thing well
Modules are Individually Manageable	• implemented as manageable & independently deployable service component

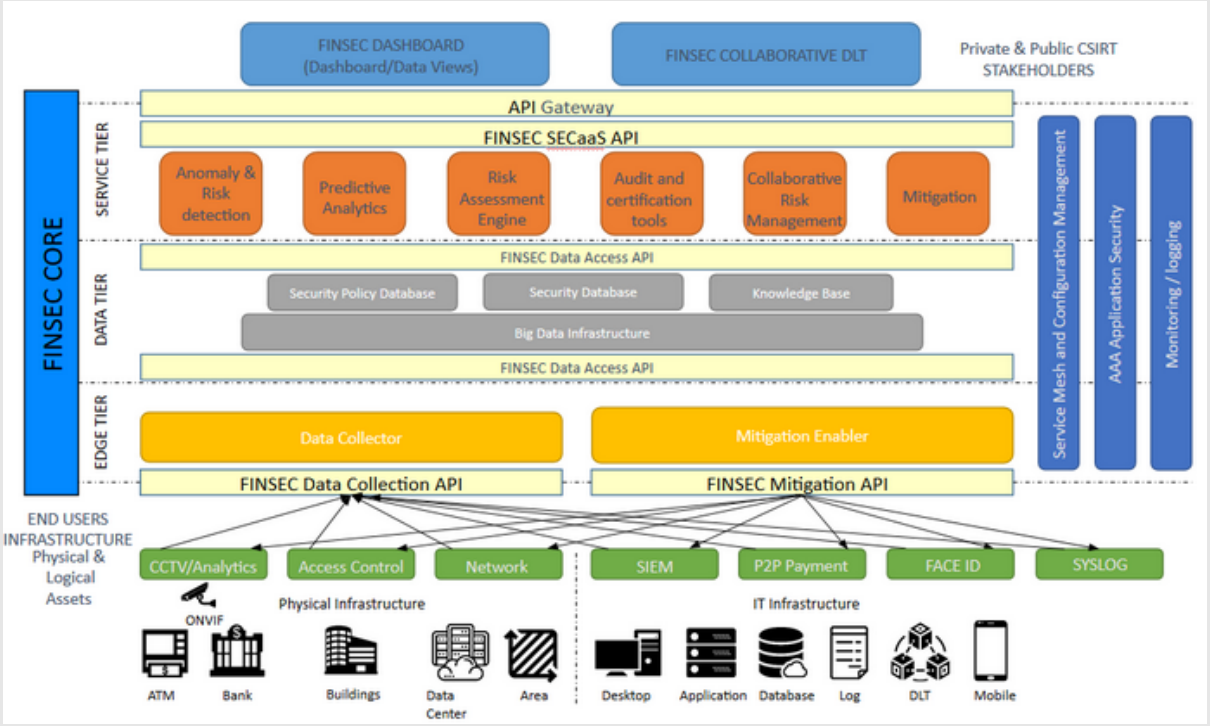
FINSEC RA: Driving Principles (cont.)

Clearly Defined Interfaces between the Modules	• clearly defined Interface to other modules • any module in the RA shall communicate with other modules via a well-defined API
Synthesis Principle	• FINSEC Reference Architecture can have multiple instance, being agnostic from implementation, the basic design principles suggest that it could be easily designed to be implemented using a Micro Service Architecture
Inter-Domain Collaboration Support	• RA covers systems that span multiple administrative domains, supporting stakeholders' collaboration
Managed Security Paradigm	• enables the provision of security services as managed security services i.e. according to a utility driven, pay-as-you-go paradigm

Microservices Architecture's Tiers

Field Tier	lower level and includes the probes and their APIs, whose role is extracting raw data from the physical and logical assets to be protected against threats
Edge Tier	contains the Actuation Enabler and a Data Collection module, which is needed to filter the needed information during their flow
Data Tier	logical layer where information is stored, organized into three different storage infrastructures, providing consisting data access APIs to all other modules
Service Tier	kernel applications and the security toolbox
Business Client Applications Tier	where end-users and business applications may actually get benefits from the platform capabilities

FINSEC Reference Architecture



Security Platform Architecture – Building Blocks

Monitoring Probes	In order to collect security information, the platform makes provisions for monitoring probes on both cyber and physical security elements
Legacy Security Systems	The platform supports the integration of legacy security systems that collect, analyze and persist security information & events. Typical examples of such systems, include SIEM (Security Information and Event Management) and CCTV (Closed Circuit TeleVision) systems.
Data Collection & Unification	The platform is a data intensive system that collects and consolidates security data from many different and heterogeneous sources

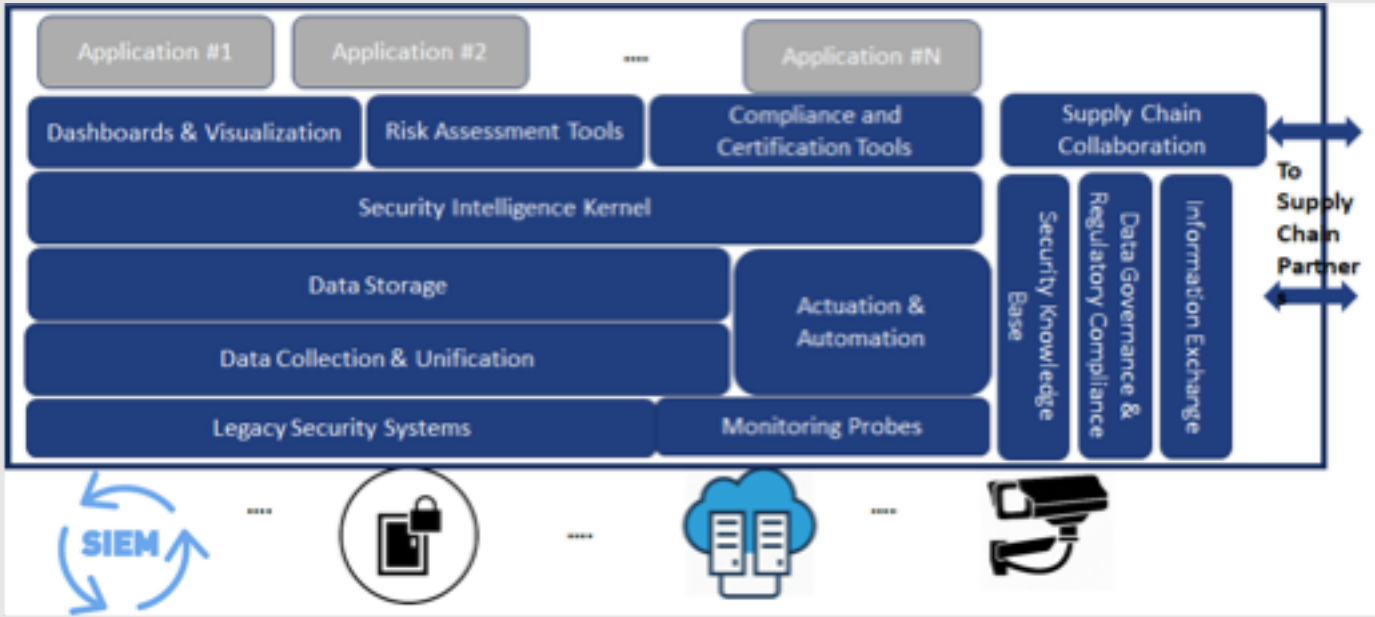
Security Platform Architecture – Building Blocks (cont.)

Data Storage and Persistence	This module comprises data lakes ensuring that very large datasets of security information can be effectively persisted and managed
Actuation and Automation	The platform provides the means for interacting with the field and the systems of the critical infrastructure towards automating security actions (e.g., as part of the implementation of a security policy), as well as towards (re)configuring the operation of the probes
Security Intelligence Kernel	The security intelligence kernel is the building block that extracts security insights based on processing of the collected information using advanced analytics. The kernel interacts with the Security Knowledge Base

Security Platform Architecture – Building Blocks (cont.)

Security Knowledge Base	The knowledge base comprises readily available security knowledge, such as information about known threats, attacks, malware and more. It helps to resolve attack and threat patterns against known information
Dashboards & Visualization	The platform provides visualization of security information
Risk Assessment & Compliance Auditing	These are two building blocks that are delivered as a service i.e. based on a Security as a Service (SECaaS) modality
Supply Chain Collaboration	This module leverages information exchange/sharing capabilities of the platform towards enabling collaborative risk assessment and compliance auditing for the assets of the critical infrastructures

Security platform architecture



Microservices Architecture