A Blueprint Architecture for Integrated Security of Critical Infrastructures in the Finance Sector

H2020 FINSEC Project White Paper

www.finsecurity.eu

GFT Italia Srl

Hewlett Packard Enterprise

INNOV-ACTS LIMITED

Assentian Ltd.

November 28, 2019

Version 1

This project has received funding from the European Union's Horizon 2020 research and innovation programme 2014-2020 under grant agreement No 786727

1. Securing Finance Sector Infrastructures: The Challenges

1.1. Recent Security Incidents in the Finance Sector

In the era of globalization, the finance sector comprises some of the most critical infrastructures that underpin our societies and the global economy. In recent years, the critical infrastructures of the financial sector have become more digitalized and interconnected than ever before. Indeed, recent advances in leading edge ICT technologies like BigData, Internet of Things (IoT), Artificial Intelligence (AI) and blockchains, coupled with a wave of financial technology (FinTech) innovations has resulted in an explosion of the number of financial transactions. As a result, the critical assets of financial institutions are no longer only physical (e.g., bank branches, buildings, ATM machines), but comprise many different cyber assets (e.g., computers, networks, IoT devices) as well.

However, the increased digitization and sophistication of the critical infrastructures of the finance sector has also raised the importance of cybersecurity in the finance sector. Nevertheless, despite significant investments in cybersecurity, recent incidents demonstrate that financial organizations remain vulnerable against cyberattacks. As a prominent example, the fraudulent SWIFT (Society for Worldwide Interbank Financial Telecommunication) transactions cyberattack back in February 2016 resulted in $81 million being stolen from the Bangladesh Central Bank. Likewise, the famous "Wannacry" ransomware attacked financial institutions and had a significant adverse impact on Russian and Ukrainian banks. As another example, in 2017 a data breach at Equifax created a turmoil in the global markets and affected more than 140 million consumers. In general, the finance sector suffers from security attacks more than other sectors, especially from cyber security attacks. In 2016 financial services customers suffered over 60% more cyberattacks than customers in any other sector, while cyberattacks against financial services firms increased by over 70% in 2017. Moreover, a June 2018 analysis from the IMF (International Monetary Fund) estimates that emerging cyber-attacks could put at risk a significant percentage of the financial institutions' profits, which ranges from 9% to even 50% in worst case scenarios.

In response to these notorious attacks against financial institutions and their cyber assets, finance sector organizations are allocating more money and effort in increasing their cyber-resilience. According to Netscribes, the global cybersecurity market for in financial services is expected to expand at a CAGR (Compound Annual Growth Rate) of 9.81%, leading to a global revenue of USD 42.66 billion by 2023. Other studies reflect a similar estimation e.g., a Compound Annual Growth Rate (CAGR) of 10.2% during 2018–2023 and a cybersecurity market growth from USD 152.71 billion in 2018 to USD 248.26 billion by 2023.

1.2. Security Challenges and Emerging Solutions

Through their security investments, financial organizations will be striving to confront the following challenges.

1.2.1. Limited integration between Physical Security and Cybersecurity

Even though the critical infrastructures of the finance sector comprise both physical and cyber assets, physical security and cyber security are in most cases handled in isolation from one another. In particular, cyber and physical security processes in financial organizations remain "siloed" and fragmented. The latter fragmentation concerns both the technical and the organizational levels i.e. physical and cyber security are handled by different security technologies and different security teams. For instance, physical security systems such as CCTV (Closed Circuit Television) systems, intelligent visual surveillance, security lighting, alarms, access control systems and biometric authentication, are not integrated with cybersecurity platforms like SIEM (Security Information and

Event Management) and IDS (Intrusion Detection Systems). Likewise, processes like vulnerability assessment, threat analysis, risk mitigation and response activities are carried out separately by physical security officers and cybersecurity teams.

This "siloed" nature of systems and process leads to several inefficiencies, including:

- **Inefficient security measures**, that consider the state of the cyber or the physical assets alone, instead of considering the global security context. There are specific types of security attacks (e.g., ATM Network attacks), where security processes like risk assessment and mitigation should consider the status of both types of assets.
- **Inability to cope with the proliferating number of combined cyber/physical attacks**. For example, a physical security attack (e.g., unauthorized access to a device or data centre) is nowadays one of the best ways to gain access to internal resources and launch a cybersecurity attack as an insider. Indeed, the recent cyberattack against the Bangladesh Central Bank exploited access to physical assets of the bank like SWIFT computing devices.
- **Increased costs** as several processes are duplicated and overlapping. In this context, an integrated approach to security could help financial organizations streamline their cyber and physical security resources and processes, towards achieving greater efficiencies at a lower cost.

1.2.2. Poor Stakeholders' Collaboration in Securing Financial Services

In an era where financial infrastructures are more connected than ever before, their vulnerabilities are likely to impact other infrastructures and systems in the financial chain, having cascading effects. In this context, stakeholders' collaboration can be a key towards identifying and alleviating issues in a timely manner. However, collaboration is currently limited to exchanging data as required by relevant security regulations and do not extend to join security processes like (collaborative) risk assessment and mitigation.

Information sharing between stakeholders of the financial supply chain is a first and prerequisite step to their collaboration in security issues. In the finance sector, the Financial Services Information Sharing and Analysis Center (FS-ISAC) has been established, as an industry forum for sharing data about critical cybersecurity threats in the financial services industry. FS-ISAC provides its members with access to threat reports with tactical, operational and strategic levels of analysis for a greater understanding of the tools, methods and actors targeting the sector. This allows them to better mitigate risk.

Information sharing (e.g., as implemented by FS-ISAC) is a foundation for collaboration in security processes like joint risk scoring for assets and services that are part of the financial services supply chain. Such IT-supported collaborative workflows have been demonstrated in many sectors, including the financial sector. Nevertheless, there are still trust barriers to information sharing and collaboration, especially when data must be shared across private enterprises. Recent advances in IT technologies like blockchain and cloud computing facilitate the sharing of information and the implementation of collaborative security functionalities.

1.2.3. Compliance to Stringent Regulatory Requirements and Directives

Financial institutions are nowadays faced with a need of complying with a host of regulations, which has a severe impact on their security strategies. For example:

- **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 General Data Privacy Regulation (GDPR):** As of May 2018 financial organizations have to comply with the General Data Privacy Regulation (GDPR), which asks for stricter and effective

security measures for all assets where personal data are managed and exchanged. Note that GDPR foresees significant penalties for cases of non-compliance, which is the reason why financial organizations are heavily investing in security systems and measures that boost their compliance.

- **The Network Information Systems (NIS) Directive:** The NIS Directive prescribes security measures for the resilience of the IT systems and networks that support Europe's critical infrastructures, including infrastructures in the financial sector. The prescribed measures include the establishment of risk-driven security polices, as well as the collaboration between security teams (including CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) at national and international level. Financial organizations are therefore investing in the implementation of the NIS Directive's mandates.
- **The EU legislative framework for electronic communications** (EU Directive 2009/140/EC) was 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. The first part of Article 13a requires that providers of networks and services manage security risks and take appropriate security measures to guarantee the security (paragraph 1) and integrity (paragraph 2) of these networks and services. The second part of Article 13a (paragraph 3) requires providers to report significant security breaches and losses of integrity to competent national authorities, who should report about these security incidents to ENISA and the European Commission annually.

1.2.4. Limited Automation

Financial organizations are nowadays required to secure their infrastructures in a fast moving and volatile environment, which is characterized by a proliferating number of threats and vulnerabilities that are likely to emerge and affect critical infrastructures. Hackers and adversaries are continually taking advantage of leading-edge technologies in order to exploit the rising number of vulnerabilities of the physical and cyber assets of the critical infrastructures. Therefore, it is not practical and, in several cases, not possible to manually carry out all security and protection tasks such as detection, monitoring, patching, reporting and security policy enforcement activities.

In this context, one of the main challenges faced by the security officers of financial organizations is the poor automation of security functions. To confront this challenge there is a need for solutions that offer immediate mitigation actions, as well as (semi)automated enforcement of security policies. To this end, financial organizations can take advantage of recent advances in technologies like Artificial Intelligence, Machine Learning and automated orchestration of security functions.

1.2.5. Lack of Flexibility in Coping with a Proliferating Number of Threats

In addition to automation, security officers of financial organizations are very keen on being flexible when dealing with the proliferating number of threats, including the emergence of several new cyber threats every year. Hence, security departments must be able to deploy new security functions (such as patches or protection policies) very frequently e.g., daily or even several times per day. In this direction financial organizations could benefit from latest developments in software engineering practices and methodologies such as the DevOps (Development and Operations) paradigm. Recent research initiatives are exploring the use of DevOps in security systems engineering, which is sometimes called DevSecOps.

2. A Reference Architecture for Securing Critical Infrastructures of the Financial Sector

2.1. FINSEC RA: Background and Rationale

In order to address these challenges, vendors and integrators of security solutions are in need of security middleware libraries and blueprints for the development, deployment and operation of security systems that address the limitations of existing platforms in terms of supporting integrated (cyber/physical) security, boosting regulatory compliance, increasing automation, as well as ensuring flexibility and speed in deploying security functions. In this direction, a security Reference Architecture (RA) offers a synthesis of best practices based on past experiences and relevant blueprints for security solutions. A Reference Architecture (RA) can also serve as a conceptual framework for building security systems faster, while minimizing development, deployment and operational risks. Furthermore, an RA serves as a device for communicating security contexts and solutions requirements across interested stakeholders. It therefore provides a common context and vocabulary, along with a repository of patterns for use by interested stakeholders. As such it facilitates teamwork in developing, deploying and operating security systems for the financial sector.

The initial proposal for a new NIS Directive and the discussions documentation [COM(2013) 48 final - 2013/0027 (COD)] states that an "insufficient level of protection against network and information security incidents, risks and threats across the EU [..., may undermine, ed.] the proper functioning of the Internal market". This statement is particularly relevant in the finance sector, where a failure of critical IT infrastructure can lead to major damages to financial markets with deep economic consequences. The H2020 FINSEC project is intended to support the need for better protection and resilience of this critical infrastructure.

FINSEC is a joint effort of security experts and financial organizations towards providing integrated (i.e. cyber/physical) solutions for the critical infrastructures of the finance sector. One of the main results of the project is a Reference Architecture (RA) for the development, deployment and operation of integrated solutions in the finance sector. The RA is motivated by the need to apply innovative patterns to the development and deployment of security systems for the critical infrastructures of the sector. As such it's a foundation for the solutions that the project provides to different financial organizations including banks, payments organizations and FinTech enterprises.

The development of FINSEC RA has considered concepts and building blocks from some well-known and accepted generic Ras, such as the RA of the Industrial Internet Consortium and its Industrial Internet Security Framework (IISF). In this way, the FINSEC RA leverages experiences from established communities, while at the same time being in-line with the evolution of security concepts that have emerged and/or evolved in these communities.

2.2. FINSEC RA: Driving Principles

Beyond basic compliance to popular and standards-based RA, the specification of the architecture is driven by the following basic principles:

- **Data Driven Principle**: The architecture enables the development, deployment and integration of data driven security systems. Therefore, it pays special emphasis on the collection and processing of security data, as well as on its seamless flow across the financial services supply chain. Key to the implementation of solutions based on the FINSEC RA is the formulation of data in-line with the FINSEC Reference Data Model (RDM), which is a STIX (STIX - Structured Threat Information

Expression) based format that supports the representation of physical and cyber security information for the financial sector.

- **Separation of Aspects and Concerns**: The Reference Architecture Logical Design will be defined in term of (services) modules. At the logical level modules are black boxes with proper and well-defined interfaces that executes specific functions (business logic). In simple words, every single module of the architecture should do one thing well.
- **Modules are Individually Manageable and Independently Deployable**: Each module of the RA should be implemented as manageable and independently deployable service component. In that respect, a module will follow a reference Implementation. Note also that every module should be defined in terms of its functionalities.
- **Clearly Defined Interfaces between the Modules**: Every module will expose a clearly defined Interface to other modules. Any module in the RA shall communicate with other modules via a well-defined set of Application Programming Interface (API). The definition of the API and functionalities defines univocally a module, including its behaviour, its communication means, the expected results and more.
- **Synthesis Principle**: Albeit the 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 (MSA). Each module could be defined through their API (REST API) exposed to other services, as part of an implementation view of the architecture.
- **Inter-Domain Collaboration Support:** The RA covers systems that span multiple administrative domains, as a means of supporting stakeholders' collaboration for increased resilience.
- **Managed Security Paradigm:** The RA enables the provision of security services as managed security services i.e. according to a utility driven, pay-as-you-go paradigm. In the context of the FINSEC project, such security services are conveniently coined SECaaS (Security as a Service).

These principles ensure the modularity of the systems that are implemented based on the RA, as well as the applicability of DevOps approach in implementing compliant security systems.

2.3. Logical Design

2.3.1. Tiered Approach

The main goal of the RA is to alleviate the currently "siloed" landscape of physical and cyber security through enabling financial organizations to deploy integrated security solutions. The latter are characterized by the seamless flow of security information for both cyber and physical assets to the security department and teams of the organization. Hence, FINSEC RA does not focus on the physical security and the IT departments only, but rather addresses the needs of the top level management of organizations, notably in terms of managers (e.g., CSO (Chief Security Officer) or CEO (Chief Executive Officer) that are in charge of the resilience of the organization.

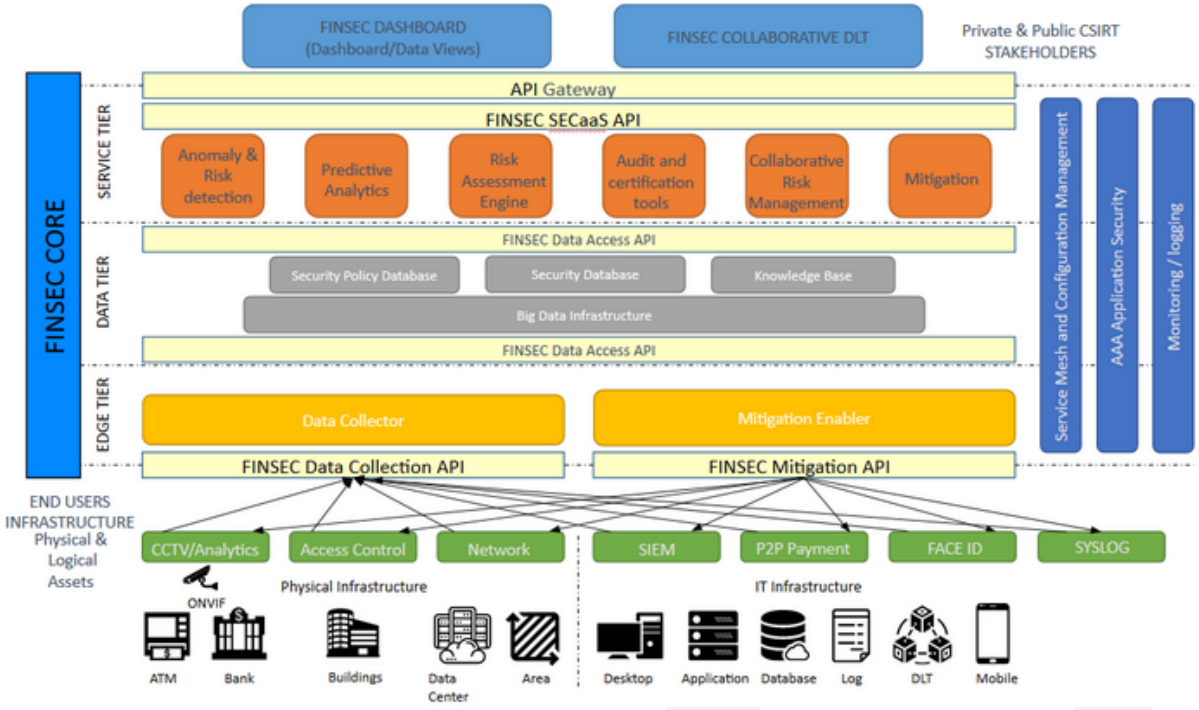
Solutions that adhere to the RA will leverage security monitoring probes available in the organizations, including existing cybersecurity applications (e.g., SIEM systems, antivirus applications, log scanning probes) and available physical security systems (e.g., a PSIM (Physical Security Information Management System), a CCTV (Closed Circuit Television System), biometric access control systems). These probes will provide security data that will drive security functionalities such as risk assessments, management of alerts and compliance auditing functions.

The RA is structured in tiered approach, yet it also includes cross-cutting elements that do not belong to a single but rather to multiple tiers. Nevertheless, in-line with the previously presented principles the architecture is modular and from a physical perspective it enables every module to communicate

with any other like a modern micro-services architecture. The following figure illustrates the main modules and tiers of the RA.

With reference to figure, the modules of the RA are structured based on the following tiers:

- **Field Tier**: The Field Tier is the lower level of the RA and includes the probes and their APIs, whose role is extracting raw data from the physical and logical assets to be protected against threats. For example, CCTV analytics and SIEM are involved in this layer to give useful information about potential attacks to the upper tiers.
- **Edge Tier**: The Edge Tier contains the Actuation Enabler and a Data Collection module, which is needed to filter the needed information during their flow towards the upper levels. The Actuation Enabler is responsible to allow some actions to be done from the upper layers onto the probes, such as the shutdown of a server in case of threat or the close of an automatic door of a protected room.
- **Data Tier**: The Data Tier is the logical layer where information is stored, and is organized into three different storage infrastructures, providing consisting data access API to all other modules.
- **Service Tier**: The Service Tier is where the kernel applications of the FINSEC and the security toolbox are running, able to be used by the external world.
- **Presentation and Communication Tier**: The Presentation and Communication tier offer interface to rest of the world (e.g., consumers of the security services that adhere to the RA). This tier provides dashboards that monitor data and assets, along with the FINSEC Collaborative Module that supports sharing of security information with other financial organizations regardless of whether the latter are running systems compliant with the RA or not.



Data Driven APIs

The FINSEC Core platform, delimited by the blue bar in the picture, comprises three tiers, namely the edge, data and service tiers. It also specifies the two main interfaces that are used to support the interactions of the data-driven platform with other systems and applications:

- The northbound API towards higher level applications (e.g. end-user applications), called FINSEC SECaaS API to align to the DoA and the core concept of FINSEC. It represents a consistent and

unified view of the individual APIs exposed by the service tier high level services that represent the "major intelligence" of the platform. The FINSEC SECaaS API is exposed by the API Gateway, which is the single-entry point to the system for external clients. Among other capabilities, the API Gateway provides and supports Authentication, Authorization, and accounting (AAA) services, which conceptually are part of the two vertical modules on the right of the figure (Application Security and Monitoring/logging).

- The southbound API interface, consisting of an EVENT API and PROBE API, allows communication between the Edge Tier and physical and cybersecurity probes.

The FINSEC SECaaS API is leveraged and invoked by external (north end) Business Client Applications (upper side of the figure). They are outside of the FINSEC core platform and interact with it only through the FINSEC SECaaS REST API. Some typical Examples of business client applications include:

- **The FINSEC Dashboard application**, which is a (WEB) GUI used by the profiled end-users of the platform. Note that in addition to the FINSEC dashboard application, additional dashboards can be implemented using the above-listed APIs.
- **The FINSEC Collaboration application**, which enables the collaboration of platforms and applications across the financial services supply chain (e.g., security data sharing). Likewise, additional applications for supply chain security can be implemented by leveraging these APIs, such as applications for collaborative risk scoring and assessment.
- **Other Third-Party Applications**, that exploit the data and security capabilities of FINSEC.

2.3.2. The Service Tier

The Service Tier defines the high-level services that represent the "major intelligence" of the platform. The Service Tier services communicate with each other in three possible ways as follows:

- **SYNCHRONOUS**, through their REST API (in this case, being the services internal to the platform, it is not necessary to use AAA)
- **ASYNCHRONOUS,** via an MQ bus, yet in this case, queues and messages formats must be defined.
- **ASYNCHRONOUS**, through the DB (Database) Infrastructure.

2.3.3. The Data Tier

The Data Tier provides an infrastructure to serve data that follow the FINSEC Reference Data Model (RDM), which extends the STIX standards and is illustrated in latter paragraph. It provides access in read/write via a Data Access API, exposed by an ad-hoc service of the platform (Data Manager). This module exposes convenient data access and manipulation functions to clients, is responsible for ensuring validation of input data against the data model and abstracts away the actual underlying DB engine(s), which can be changed without affecting upper-level services.

A possible alternative option, which allows to avoid an intermediate data access layer, is to use the CRUD (Create, Retrieve, Update, Delete) REST API already exposed by the DB engine (if available, depending on the DB engine chosen for the implementation) and rely on DB validation rules for ensuring consistency and validation of data with reference to the FINSEC RDM. The latter can be used by the modules of the Service tier to communicate with each other, in-line with the third of the above listed approaches for communication.

In addition to data conforming to the common data model, the DB infrastructure may contain additional ad-hoc data stores for private data reserved to the individual Service tier modules, useful for enabling their own internal logic. The concept in this case is that the individual service could still have a private DB schema for its own settings / local data, e.g. for processing with its own algorithms, and then proceed to publish data on the common DB schema (via the Data Access API) following the

FINSEC data model only once it has identified events useful for the common intelligence of the system, as previously mentioned.

The Data Tier provides the fundamental service for and will be based on:

- A Data Base suited to manage the non-structured Threat Information made by events, incidents, logs, etc. It can be either a non-traditional DB (e.g., NoSQL, memSQL) or a conventional SQL relational DB.
- A BigData Infrastructure to manage the large amount of data to be processed and distributed according to the requirements of the client modules, typically those ones of the Service tier needing BD / AI capabilities to perform their business logic.
- The Security Knowledge Base, which is used to automatically resolve observed data streams into known threats, vulnerabilities and attacks encoded in the database.

2.3.4. The Service TIer

The Edge Tier communicates with the infrastructure (IT / Physical) through the southbound API interface. This API consists of the union of two distinct APIs:

- **Event API**, which is implemented to receive events in push and/or pull modes and it is invoked by the probes.
- **Probe API**, which is implemented by probes to receive commands from FINSEC. In this case probes can operate as actuators as well.

Overall, probes send events formulated based on the FINSEC RDM, in all cases when they want to publish data on the Data Tier (e.g., the DB infrastructure and possibly ingestion in the Big Data Infrastructure).

2.4. Main Services and Building Blocks of the RA

Each of the modules of the RA is thought as a black box with proper interfaces executing specific functions. Moreover, each module can be implemented as a software manageable and independently deployable service i.e. respecting the micro-service architecture (MSA) paradigm and communicating with standard interfaces (i.e. REST API). The list of the modules and services of the Reference Architecture that are depicted in the above figure are as follows:

- **FINSEC Dashboard**: Web application that presents events, threats, incidents, logs, etc. in a User Graphical Interface. The application will be web-based and will interact with the other micro-services to gather information to be present to the dashboard graphically and intuitively.
- **FINSEC Collaborative Module**: Service application for collaborative security information sharing and Threat Intelligence. The application will have a micro-service interface that will provide APIs for exchange information about threats and mitigations. Exchanged data is based on FINSEC Data Model.
- **API Gateway**: API Gateway is a fully managed service that provides to other services ways to create, publish, maintain, monitor, and secure APIs at any scale.
- **Actuation**: Application that offers API to other services to operate on the physical and logical infrastructure sending commands to the physical or logical components.
- **Anomaly & Risk detection prioritization**: Application for anomaly and risk analysis. It consumes current data sources (logs, incidents, etc.) and produce incidents and alarms. Application consumes DATA Access API and push threat information using API of other services (e.g. Dashboard, Collaborative Module, etc.)

- **Predictive Analytics**: Application that will analyze risk and threats from current data sources (logs, incidents) and predicts threats and patterns of threats. Application uses DATA Access API and push threat information using API of other services (e.g., Dashboard, Collaborative Module, etc.)
- **Risk Assessment Engine**: Application for Real-time assessment of security risks, including business interpretation. It analyzes current model of assets associated with business risks levels stored as data model in DB and produces a risk assessment analysis. The Models are produced by the Audit and certification tool. Application uses DATA Access API push threat information using API of other services (e.g. Dashboard, Collaborative Risk Management modules etc.).
- **Audit and certification tool**: Web Application with HMI to produces a data model representation of assets of the infrastructure. Application will be basically a Data Entry application plus Import from other data sources. Application produces reports displayable and exportable (e.g., pdf)
- **Collaborative Risk Management**: Application for collaborative risk analysis and management in the financial supply chain. It can be implemented based on either centralized (e.g., a centralized database accessed by all stakeholders) or decentralized approaches (e.g., a distributed ledger approach). The module provides an API for other services to push threat information.
- **MQ BUS**: This is an asynchronous Message Passing Application. It provides Push/Pull APIs for basic message passing.
- **Security Database**: A NoSQL application for storing data according to the FINSEC Data Model.
- **Knowledge Base**: A NoSQL application for storing data according to the FINSEC Data Model. It incorporates knowledge from various sources (including vulnerability databases) and used to automate the resolution of threats and vulnerabilities as part of security functionalities like risk management. It provides a CRUD (Create, Retrieve, Update, Delete) API for storing Knowledge Base documents.
- **Big Data Infrastructure**: It is a distributed File System Application. It provides API for scaling data across multiple servers.
- **Data Collection**: Application module that provides API to EDGE services like CCTV or SIEM for pushing data (events, logs, etc.) to the Security Database. The application also performs normalization and prioritization to the information supplied by the EDGE applications.
- **Actuation Enabler**: Application module that provides API to the ACTUATOR service pushing action to the Logical and Physical infrastructure (e.g. shutdown of a server or close a door of a data center). The application performs abstraction and normalization to adapt to different EDGE components.
- **CCTV/Analytics**: Any Video Surveillance application can be integrated will use FINSEC Event API to push information to the FINSEC core and provides FINSEC Probe API to interact with the EDGE components.
- **SIEM**: Any Security Information and Event Management (SIEM) can be integrated as long as will use FINSEC Event API to push information to the FINSEC core and provides FINSEC Probe API to interact with the EDGE components.
- **Logical Probe**: Field-level logical sensor/actuator to give data on the status of the assets such as logs and actuation commands on logical assets (e.g., shutting down a server to protect it). Note that any probe can be integrated as long as will use FINSEC Event API to push information to the FINSEC core and provides FINSEC Probe API to interact with the EDGE components.
- **Pentest Tool**: Service application acting on the field to extract information on the status of the assets. The Pentest is an assessment of the capacity of an asset to react to a penetration attempt by an actor, through the simulation of an attack. Service provides APIs will give information about the status of the asset and the attack typology under simulation.
- **Service Mesh and Configuration Management**: Service application that provides API to discover services within the infrastructure; moreover, their configuration will be done via this building block. Its APIs will need to give the user the current configuration for each service within the RA.

- **AAA Application Security**: Service application that provides basic API for Authentication, Authorization and Accounting users and other services within FINSEC platform. It is part of the "vertical" building blocks, not belonging to any specific tier.
- **Monitoring/ Logging "Diagnostic" Module**: It provides API for storing and retrieving logs from other services (e.g. connection/disconnection, search for services, use of certain services, getting warning and alarms, actuation on cyber or physical assets, etc.).

All services must provide standard API to start/stop/ shutdown/monitor/status of the application.

2.5. FINSTIX: The FINSEC Reference Data Model

The data-driven operations and data flows specified in the FINSEC RA hinge on the adoption and use of common data semantics for the full set of data/information that are exchanged between the modules of the architecture. To this end, the FINSEC RA is accompanied by a Reference Data Model (RDM) specification, which specifies the format and the semantics of the security data that flow across the modules of the architecture. The RDM is based on the second version of the STIX™ (Structured Threat Information Expression) (STIX2), which is one of the most prominent standards for sharing threat intelligent information. In particular, the FINSEC RDM, which is conveniently called FINSTIX, is an extension of STIX2 into the physical and logical domain. FINSTIX has been developed based on the following principles that facilitate its implementation and integration with solutions that adhere to the FINSEC RA:

- The FINSTIX Data Model basic object is a sequence of key-values that can be passed as JSON (JavaScript Object Notation).
- The FINSTIX Data Model general object is an aggregate of more objects and relations still expressed in JSON.
- FINSTIX includes information relevant and specific to the financial sector, including common threats and vulnerabilities faced by financial organizations.
- FINSTIX defines other objects and relations to STIX2 to cope with the correlation of physical and logical data, as a means of supported cyber and physical security integration.

In the scope of solutions that comply with the FINSEC RA, probes generate events and observed data according to the FINSTIX Data Model. Likewise, Data Collectors (DC) have the function to gather data from probes normalizing, sanitizing, prioritizing and storing CPTI into the Data Layer. In other words, a DC knows the syntax-semantic and add or subtract further information to the FINSTIX objects passing through. Moreover, security knowledge (e.g., as of part of the Knowledge Base (KB) of the FINSEC RA) is represented with FINSTIX objects as well. Also, any analytics algorithms (including predictive analytics based on machine learning and Artificial Intelligence (AI) techniques) in security applications use events, observed data and the Knowledge base and Asset Models to produce Cyber Physical Threat Intelligence.

FINSTIX includes the STIX Domain Objects (SDO) already defined by STIX2, including Identity, Observed Data, Indicator, Intrusion Set, Vulnerability, Tool, Attack Pattern, Campaign, Malware, Threat Actor, Course of Action and Report. Nevertheless, FINSEC specifies several extensions to STIX2, notably extensions that address security use cases of the financial sector. These extensions are specified in terms of custom objects like:

- **Organization** that comprises information about a financial organization.
- **Asset** encoding information about an organization's valuable infrastructure such as PCs, server rooms, ATMs, applications and everything else inside the organization that is considered crucial.
- **Area of Interest** i.e. a logical/physical area inside an asset such as the screen/keyboard of an ATM or an indoor area (server room).
- **Service** which signifies a collection of assets forming a publicly exposed service.

- **Probe** that is used to support the security monitoring infrastructure. A Probe usually monitors one or more areas of Interest.
- **Probe Configuration** that provides data sent to a probe in order to configure details such as the area under monitoring or the bit rate of the monitoring process.
- **Event** including information of something that happened or is happening.
- **Person** which extends the STIX Identity objects and is used to describe people involved in the events created by the probes.
- **Risk** i.e. the calculated risk for a specific asset or service.
- **Risk Configuration** which provides information needed to optimize the risk assessment (e.g., triggers and other useful options).
- **Regulation** i.e. an object used to depict a regulation violation. The regulation violation information can be communicated to Regulatory authorities and other Organizations;
- **CPTI** which is the principal object that collects and provides threat information. One or more CPTI objects are used to generate the output of the threat intelligence process, i.e. a report about ongoing or possible future attacks on one or more assets belonging to the infrastructure.

A detailed presentation of the FINSTIX specification is out of the scope of this whitepaper. Interested readers shall contact the FINSEC Project coordinator.

3. Security Use Cases for Financial Institutions

The FINSEC RA, along with the FINSTIX specification enables the implementation of a wide range of security use cases for financial institutions. Some prominent examples follow.

3.1. SWIFT Network Attacks

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables financial institutions to send and receive information about financial transactions in a secure, standardized and reliable environment. It is a messaging network, which facilitates the secure transmission of information and instructions based on a standardized system of codes. The SWIFT network is one of the most critical infrastructures of the financial sector, as it enables many financial transactions with very high monetary value. Any disruption to the operation of this network can have significant socio-economic implications (including significant financial losses), as evident in a number of recent attacks against it.

The operation of SWIFT network is based on a supply chain of relevant stakeholders, while entailing both cyber (e.g., networks, computers) and physical (e.g., SWIFT devices, SWIFT transactions rooms). Therefore, integrated (cyber/physical) approaches to securing the SWIFT network, along with stakeholders' collaboration in the supply chain can increase its resilience. In-line with the FINSEC RA, probes can be used to collect security information about cyber and physical assets, as a means of identifying risks and non-obvious abnormalities. For example, a FINSEC compliant system can correlate information about attempts for unauthorized access to physical spaces or devices with information about vulnerabilities of the SWIFT ICT infrastructure. In this way strong protection from insider threats can be provided, along with resilience against combined cyber/physical attacks (e.g., cases of an intruder (or insider) who exploits cyber vulnerabilities in order to give malicious SWIFT commands from the inside). Likewise, the collaborative modules of the FINSEC RA can enable financial organizations that participate jointly in SWIFT transactions to share threat information and accordingly to use the shared information towards jointly scoring risks associated with SWIFT related assets.

3.2. ATM Network Protection

The network of ATM (Automatic Teller Machines) is another prominent example of financial sector infrastructure that includes both cyber and physical elements. A single ATM includes a PC, a vault and a printer, which are interconnected. Furthermore, ATM machines are themselves networked via ICT infrastructure. The integrated security capabilities of the FINSEC RA can be exploited in order to correlate cyber and physical security events that can indicate abnormal situations in the use of one or more ATM machines. To this end, appropriate probes like CCTV cameras and sensors that can provide information on the physical status of the ATM's objects are needed. Based on such probes and the analysis of their information, it is possible to extract and correlate a wide array of events and notifications such as a person entering or being the ATM area, detection of a use of a valid card, detection of whether the ATM case is open (e.g., based on vibration sensors), interaction between people in the ATM area (e.g., when two or more people are very close), people fighting, people leaving the ATM and more. The correlation of such events can enable the detection and timely sharing of CPTI information between relevant security stakeholders such as the security officers of a bank, their IT department, law enforcement agencies and more.

3.3. Regulatory Compliance

FINSEC RA can also enable the development and deployment of solutions that boost Data Privacy Compliance, as a means of boosting financial organizations' compliance with relevant directives and regulations such as the General Data Protection Regulation (GDPR) for organizations that operate in Europe or collaborate with European financial institutions. This is very important for financial organizations, as they typically handle large amounts of sensitive consumer data. In particular, the FINSEC RA can boost the implementation of SIEM and other probes that:

- Record all events associated with handling of personal data, as means of providing a complete and reliable audit trail for such data.
- Implementing and deploying advanced analytics algorithms over FINSTIX as a means of quickly detecting data breaches.
- Providing additional analytics tools for analysing those data breaches and finding their root causes, along with relevant (i.e. responsible or liable) actors.
- Monitoring, logging and analysing changes to credentials and security groups, notably groups that handle personal data.
- Auditing and verifying security controls to ensure that user data is treated appropriately and in-line with GDPR principles.

Overall, the FINSEC RA forms a basis for the development of compliance auditing services for all operations that access and/or process private data.

Moreover, the NIS Directive (Directive (EU) 2016/1148) advocates for a well-defined governance process, improved risk management and management of the overall supply chain. In this direction, the FINSEC RA specifies:

- Audit and certification services to support improved governance,
- Risk assessment, anomaly and risk detection to better support risk management
- A supply chain collaboration concept that describes how FINSEC integrates security and risk management across the supply chain. In particular, the Edge Tier and SECaaS services of the architecture, together with the FINSEC Collaborative Module and Dashboard provide integration / interaction with the supply chain.

ENISA in their work from 2014 on network and information security in the finance sector indicated also the need for risk transparency for the immediate operational circle in order to better manage the risks posed by the supply chain, which reinforces FINSEC's RA relevant for regulatory compliance.

3.4. Insider Threats

As briefly indicated in the scope of the SWIFT network protection use cases, insider threats can be a very big headache for financial organizations as they can be very hard to detect. This is because insiders can appear as legitimate users. Solutions compliant to the FINSEC RA can leverage SIEM-like functionalities in order to detect and understand insider threats based on recording and analysis of insiders' behaviour. In practice, this can be implemented as follows:

- Detecting cases where users move across multiple systems within the intranet of the financial organization.
- Identifying cases where users' privileges and authorizations change, thus enabling users to access different systems and possible gain additional authorizations.
- Detect "strange" and unusual behaviours, such as cases where users access systems during unusual days or times.

- Correlating events that do not have obvious links between them, such as changes in the quota or authorizations of specific groups of users and cybersecurity vulnerabilities of financial infrastructures (e.g., SWIFT/SEPA infrastructures).

3.5. IoT Devices Security

The Internet of Things (IoT) paradigm enables financial organizations to leverage data from the real world in designing and delivering their services (e.g., Point of Sales (POS) devices and RFID devices). These devices add new points of vulnerability, given that the users of these devices may not take appropriate measures for their security. The FINSEC RA can enable the implementation of systems that can security such devices through monitoring and analysing their data flows, while at the same time activating pentesting and vulnerability assessment functionalities. In particular, the FINSEC RA can enable the implementation of analytics applications that generate alerts whenever unusual flows or patterns of data are detected. Such alerts can be visualized on appropriate dashboards and/or shared with security teams like CERT/CSIRTs.

3.6. Managed Security

The FINSEC RA promotes the implementation of security solutions based on modern cloud-based micro-services architectures. As such it also provides the means for implementing cloud-based Security as a Service (SECaaS) applications. The latter are very important for financial organizations that lack the financial capacity and/or the technical knowhow to develop, deploy and operate on-premise solutions. As a prominent example, SMEs (Small Medium Enterprises) dealing with algorithms trading or payments do not typically have organized security departments and teams. Thus, they would rather dispose with a managed security paradigm like SECaaS. The FINSEC RA can enable these organizations to access services like pentesting, risk management and vulnerability assessments as a service (i.e. through a service provider) as soon as they can providing security data based on appropriate probes. The SECaaS model can provide them with flexibility as well, since they can request and access additional reports around compliance and privacy on demand i.e. where and when needed. Overall, the FINSEC RA provides the means for implementing a wide range of managed security use cases based on the SECaaS paradigm, as means of maximizing flexibility and obviating the need for significant capital investments on security infrastructures.

4. Conclusions

The critical infrastructures of the financial sector are increasing in size, complexity and sophistication, while at the same time comprising both cyber and physical elements. At the same time financial organizations are obliged to comply with many and complex regulations and directives about security, privacy and data protection. As a result, financial enterprises must deal with increased security vulnerabilities and threats in a rapidly evolving regulatory environment. To this end, they are increasing their investments in cybersecurity and its intersection with physical security. Despite the rising investments, they remain vulnerable to security and privacy threats, as evident in several notorious incidents that have occurred during the last couple of years.

In order to properly secure the critical infrastructures for the financial sector there is a need for a new integrated approach that addresses physical and cybersecurity together rather than having them treated by dedicated systems and processes. Likewise, financial organizations should benefit from the capabilities of emerging technologies like Big Data and AI analytics for security monitoring and automation, while at the same time leveraging the flexibility of the DevOps paradigm that provides opportunity for frequent changes to security measures and policies (e.g., patching on a daily basis). In response to these requirements, the FINSEC project has introduced a Reference Architecture, as a blueprint for implementing, deploying and operating integrated (cyber/physical) security systems.

The FINSEC RA is a modular architecture that adopt modern principles of micro-services architectures and DevOps methodologies. It is a data-driven architecture that relies on the collection, analysis and sharing of security information, as means of identifying vulnerabilities and threats, but also as a means of instigating relevant remedial issues and actions. Along with the FINSEC RA, FINSEC has also introduce FINSTIX, a novel STIX2 based format for integrated cyber/physical threat intelligence in the financial sector.

Based on the FINSEC RA a wide range of security use cases can be implemented and deployed. We have discussed some sample and very prominent use cases concerning attacks against the SWIFT network, protection of the ATM network, confronting insiders' threats, boosting compliance to GDPR and other data protection regulation, securing IoT devices, as well as implementing managed security based on the SECaaS paradigm.


FIN
SEC


innov-acts
GFT
Atos
Hewlett Packard Enterprise
FUJITSU
UTi GRUP
IBM
sia
Singular Logic
HDI Assicurazioni
nexi
jrc
Liberbank
NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
wirecard
Consiglio Nazionale delle Ricerche
CCA
Clear Communication Associates Limited
Assentian Limited
ORT FRANCE
INNOVATION ET DEVELOPPEMENT
FONDAZIONE BRUNO KESSLER
cini
consorzio interuniversitario nazionale per l'informatica
Zanasi & Partners
Security Research and Advisory
ALPHA BANK