Integrated Framework for Predictive and Collaborative Security

of Financial Infrastructures

Start Date of Project: 2018-05-01

Duration: 36 months

D2.3 Modeling and Specifications for Integrated, Collaborative and Predictive Security

Deliverable Details	
Deliverable Number	D2.3
Deliverable Title	Modelling and Specifications for Integrated, Collaborative and Predictive Security Sec SE Security
Revision Number	3.0
Author(s)	AS
Due Date	31/01/2019
Delivered Date	31/01/2019
Reviewed by	JRC, Z&P
Dissemination Level	PU
EC Project Officer	Christoph CASTEX

Contributing Partners	
1.	AS (author)
2.	ATOS (contributor)
3.	IBM (contributor)
4.	HPE (contributor)
5.	UTI (contributor)
6.	SiLO (contributor)
7.	LIB (contributor)
8.	SIA (contributor)
9.	CCA (contributor)
10.	INNOV (contributor)
11.	Z&P (contributor)
12.	NRS (contributor)
13.	CNR (contributor)

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

14.	ORT (contributor)
15.	FBK (contributor)
16.	CINI (contributor)
17.	GFT (contributor)
18.	FUJITSU (contributor)
19.	HDI (contributor)
20.	JRC (contributor)
21.	NEXI (contributor)

Document Status

☐ draft

☒ WP leader accepted

☒ Consortium reviewed

☒ Project coordinator accepted

Revision History

Version	By	Date	Changes
0.1	AS	13/07/2018	Initial ToC, bullet points,
0.2	AS	23/07/2018	First Draft
0.3	NRS	16/08/2018	Re-structured ToC and added 3 subsections
0.4	AS	17/08/2018	Partners responsibilities and Section 2 update
0.5	AS	03/10/2018	Update to document structure and update to section 2.4
0.6	AS	08/11/2018	Update to Sections 2, 3, 4,5 and 6
0.7	AS	15/11/2018	Update to Sections 2,3,4,5,6 and 7
1.0	AS,NRS	18/12/2018	Update and Review of All Sections
2.0	AS,NRS	07/01/2019	Update to Section 3, 4,7, 9 and 10
2.1	AS	08/01/2019	Update to Section 3, 4,7,9 and 10
2.2	NRS,AS	10/01/2019	Update to Section 5 and 7
2.3	NRS,AS	11/01/2019	Update to Section 4
2.4	AS,NRS	15/01/2019	Update to all sections
2.4.1	NRS,AS	15/01/2019	Updates to sections 5 and 7
2.5	AS	16/01/2019	Re-structure of Sections
2.6	AS	26/01/2019	Update to all Sections after Reviewers Comments
2.7	AS	27/01/2019	Final Draft
2.75	JRC	29/01/2019	Quality review by JRC
2.8	INNOV	29/01/2019	Quality control by the QM
3.0	INNOV, GFT	31/01/2019	Version for Delivery to EC

Abbreviations

Adaptive Collection Frequency Adjustment Strategy Based on Predicted Variation Ratio (ACFAS_PVR)

Advanced Cyber Defence Centre (ACDC)

Automated Teller Machine (ATM)

Collaborative and Predictive Security (CPS)

Common Attack Pattern Enumeration and Classification (CAPEC™)

Common Base Event (CBE)

Common Configuration Enumeration (CCE)

Common Criteria Recognition Arrangement (CCRA)

Common Event Expression (CEE™)

Common Event Format (CEF)

Common Information Model (CIM)

Common Intrusion Detection Framework (CIDF)

Common Intrusion Specification Language (CISL),

Common Platform Enumeration (CPE™)

Common Security Model (CSEC)

Common Vulnerability Enumeration (CVE)

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS)

Computer emergency response team (CERT)

Computer Security Incident Response Team (CSIRT)

Computer Security Incident Response Teams (CSIRTs)

Critical Infrastructure Notification System (CINS)

Cyber Information Sharing Partnership (CISP)

Decision Trees (DT)

Density-Based Spatial Clustering of Applications with Noise (DBSCAN)

European Union Agency for Network and Information Security (ENISA)

Financial Services Information Sharing and Analysis Center (FS-ISAC)

Incident Object Description Exchange Format IODEF

Information Security Management System (ISMS)

Information Sharing and Analysis Center (ISAC)

Information Sharing and Analysis Organizations (ISAOs)

Information Technology Infrastructure Library – former acronym (ITIL)

Information Technology Security Evaluation Criteria (ITSEC)

Intrusion Detection Message Exchange Format (IDMEF)

JavaScript Object Notation (JSON)

Logistic Regression (LR)

Long short-term memory units (LSTM)

National Information Exchange Model (NIEM)

National Institute of Standards and Technology (NIST)

Network Security Incident eXchange (n6)

Open Network Video Interface Forum (ONVIF)

Open Web Application Security Project (OWASP)

Open Web Application Security Project Security Verification Standard (OWASP ASVS)

Physical Security Interoperability Alliance (PSIA) for physical security information modelling

Recurrent Neural Network (RNN)

Reference Model of Open Distributed Processing (RM-ODP)

Resource Description Framework (RDF)

Security-related Data Description Language (SDDL)

Semantic Web Rule Language (SWRL)

SPARQL Protocol and RDF Query Language (SPARQL)

STIX Domain Objects (SDO)

Structured Threat Information eXpression (STIX)

Structured Language for Cyber Threat Intelligence Information (STIX™)

Target of Evaluation (TOE)

Threat Intelligence Sharing Platforms (TISP)

Trusted Automated eXchange of Indicator Information (TAXII™)

Trusted Computer System Evaluation Criteria (TCSEC), commonly known as The Orange Book

Vehicular ad hoc networks (VANETs)

Web Ontology Language (OWL)

Executive Summary

This deliverable combines the outcomes of Task 2.3 and 2.4. It describes the FINSEC integrated models and building blocks of the FINSEC approach. The specifications here will be determined additionally by the work done in D2.1 Requirements Analysis and Reference Scenarios.

The deliverable provides a set of specifications for the FINSEC architecture and framework covering the approach for integrated, collaborative and predictive security that will feed into the work done in the technical workpackages 3, 4 and 5. In so doing it shows the main components that will facilitate a combined cyber/physical approach to security. The deliverable provides integrated models of physical and cyber assets and their relationships including a proposal for the overall FINSEC Data Model. It provides an approach for predictive security analytics combining both the algorithmic approaches and the architecture to support the analytics process. Finally, the deliverable provides an approach by which to model the security processes in financial services critical infrastructure based on international standards including ISO 27001, ISO 28000, ISO 27005 and ISO 31000 amongst others.

The integrated model covering both cyber and physical is further elaborated in Section 3.2 and shows how STIX can be extended respecting the requirements that relate to physical infrastructure as well. Predictive Analytics will be core to FINSEC providing the ability to predict when the systems/infrastructure are under attack, threatened and/or compromised.

Section 4 details the approach taken for Assurance on the basis of modelling the system based on a number of viewpoints: Enterprise, Informational, Computational, Engineering and Technology (**see Section 4.2**). The approach proposed in FINSEC builds on what is done in ISO 10746 and provides an approach that: Is based on international open standards; captures system specific properties; documents basic security concepts; includes models that are appropriate and useful for security design as well as analysis and implementation and testing.

Sections 5 and 6 provide an approach for analytics in FINSEC that meets the need to provide rapid feedback with a multi-layer adaptive data collection approach. Combinations of Deep Learning algorithms and statistical approaches will be utilised to deliver intelligence on anomalies and attacks with the sort of speed to maximise the value of that intelligence.

Section 7.1 shows how FINSEC will implement the security knowledge base. It focuses on the collection of threat intelligence from asset types relating to typical cyber and physical infrastructure that are prevalent in financial institutions. The incoming information from external intelligence sources will be represented through the FINSEC Data Model.

In Section 8.5 a blockchain approach is proposed for sharing information across different security systems and stakeholders. This will provide a means by which the data can be validated, and a smart contract can be used to provide alerts when new entries appear. Each Participant must agree to share information with other participants on the network however there are always likely to be conflicts of interest and confidentiality issues emerging which will require the appropriate granular access control within the network.

Section 9.3 describes the proposed model for Security Process Modeling. Security Process Models are primarily standards based and generally follow a three-stage process: Implement, Evaluate and Maintain. The model proposed here is based on the ITIL Security Management Process and it has been extended to bring both cyber and physical into an overall model. It is designed to ensure that the confidentiality, integrity and availability of an organization's information, data and IT services are kept.

Finally managing risk in the organisation is a critical component of its approach to protection and mitigation. The approach described for FINSEC in Section 10.2 combines the traditional approach taken by widely accepted mature international standards like ISO 27001, ISO 27005 and ISO 31000 and the incorporation of the three tier model advocated in NIST SP-800-39. This is in-line with the

standards and approaches already used and implemented by financial institutions but puts it within the context of the three tiers: 1. Organisation, 2. Mission/business processes, 3. Information Systems.

This deliverable provides input into the further work on the definition of the reference architecture in Task 2.5 and for the subsequent workpackages, to define and implement the lower level components and services.

TABLE OF CONTENTS

List of figures

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement no 700071.

1. Introduction

1.1. Motivation and Objective

FINSEC aims to develop, demonstrate and bring to market an integrated, intelligent, collaborative and predictive approach to the security of critical infrastructures in the financial sector.

To achieve this, it is necessary to understand and review the existing approaches, technologies, models and standards that can potentially contribute to the overall system and its functions.

This deliverable combines the outcomes of Task 2.3 and 2.4. It describes the FINSEC integrated models and building blocks of the FINSEC approach. The specifications here will be determined additionally by the work reported in D2.1 Requirements Analysis and Reference Scenarios and the work on the most applicable standards and regulation reported in D2.2.

The main outcome of the task is a set of specifications that will form the basis for the work to be done on the specification of the reference architecture and the work on specifying the lower level detail for all the specific FINSEC Components and Services. The content of this deliverable complements the insights gained by the activities of the requirements' definition achieved in T2.1 and T2.2.

It further sets out the high-level specifications covering the approach for integrated, collaborative and predictive security. In so doing, it identifies the main components that will facilitate a combined cyber/physical approach to security. The deliverable provides integrated models of physical and cyber assets and their relationships. Finally, the deliverable models the security processes in financial services critical infrastructure based on widely recognised international standards. The Deliverable will provide input into the work done in D2.4 on the reference architecture – most importantly through providing the high-level description of the FINSEC data model combining both physical and cyber security. It will also provide the basis for further technical work in Workpackages 3, 4 and 5.

2. Methodology

The gathering of information presented in this report was based on the results of a desktop survey covering:

- the different approaches and standards for data modelling for physical and cyber security,
- the existing approaches and services for information sharing of cyber incidents and threats,
- the applicable standards-based approaches for risk management for cyber security,
- existing approaches to security process modelling,
- a review of the plethora of different approaches to predictive analytics that have been widely used over the last 30 years
- standards based approaches for the assurance of cyber physical systems

On completing this review, and with the collaboration of consortium partners, decisions were made about the best approach for FINSEC. Interaction with other partners was based on a one-to-one meeting in Month 4 and a meeting with several partners in Month 6. This was also complemented by several phone conversations and email exchanges.

3. Main Elements of a Cyber/Physical Approach

3.1. Integrated Data Modelling

The H2020 FINSEC project is developing a unified approach to implementing security in the financial services industry based on the integrated management of both cyber and physical security threats. This unified approach is motivated by the need to reduce the fragmentation of the security systems and teams in financial organizations, while at the same time streamlining their activities and gaining extra efficiencies from possible correlations between cyber security and physical security incidents.

The development of an integrated approach that unifies physical and cyber security hinges on an integrated handling of information for both cyber and physical assets, including the interrelationships between them. To this end, two different approaches to managing can be envisaged, namely a loosely coupled and a tightly coupled approach to integrated security information modelling.

3.1.1. Loosely Coupled Models

Loosely Coupled Systems are ones where the components have little or no knowledge of the definitions of other separate components. Subareas include the coupling of classes, interfaces, data, and services. It can almost be seen as a "black box with interfaces" architectural design pattern. It is in essence a design approach that subdivides a system into smaller parts called modules or skids that can be independently created and then used in different systems. A modular system can be characterized by functional partitioning into discrete scalable, reusable modules; rigorous use of well-defined modular interfaces; and making use of industry standards for interfaces.

Pros

- Ability to build much more complex systems due to clear isolation of functionality into discrete units (services, microservices etc.), thereby increasing the ability of the system to manage all of the complex inter-dependencies inherent in the system
- Ease with which component plug and play is facilitated allowing the system to more quickly evolve and improve via component upgrades. Improvements can take the form of increased performance, increased functionality or reduced cost. These are realised by the ability to easily introduce new and improved components with minimum change management overhead.

Cons

- Loosely coupled/modular systems incur higher communication overhead as inter-dependencies must be managed through standard interfaces as much as possible, which by their nature, are more complex to manage than simple, custom direct connections.
- Data and transaction integrity can also get pretty tricky. Making sure that data integrity does not become a major performance bottleneck is a real challenge as these systems grow in size (often well beyond what would be achievable with an Integrated/Tightly Coupled design).

3.1.2. Linking Security Information within Existing Repositories – Interoperability Registry Approach

This approach involves the development of a new (meta) data model, which should aim at link security information contained in other security repositories including cyber and physical security information. The aim of this (meta) model will be to provide associations of cyber and physical assets and cyber & physical security incidents on the basis of their location, their business/security context or even their temporal relationships (e.g., attacks happening within the same time window). This linking would accordingly enable "integrated" security intelligence through analytics systems that reason over interrelated or correlated assets. From an implementation perspective, this linking can be implemented based on an interoperability registry, which shall provide the linking of different schemas from different security information repositories. The main advantage of this approach is that organizations can dispose their existing information models such as the Common Security Model (CSEC) of the Physical Security Interoperability Alliance (PSIA) for physical security information modelling and Structured Language for Cyber Threat Intelligence Information (STIX) for cyber security information modelling, while combining them in a value-added approach. Moreover, this approach is extensible, as new information repositories and schemas can be linked through the meta model and the interoperability registry. On the other hand, the downside of the approach is that there is only loose connection between the different entities, which may limit the power of analytics, while at the same providing limited data management opportunities as the data reside essentially in their original repositories.

3.1.3. Tightly Coupled

Tight coupling is a coupling technique in which hardware and software components are highly dependent on each other. It is used to refer to the state/intent of interconnectivity between two or more computing instances in an integrated system.

Tight coupling is primarily used in enterprise systems and applications that work on the interconnectivity and inter-processing of two or more systems simultaneously to deliver a cohesive/integrated solution. Typically, a tightly coupled system's entire logic is distributed across several hardware and software components, which all need to be operational and connected to deliver the business logic/process. For example, a bank ATM machine depends on the ATM machine hardware, built-in firmware/applications and the primary banking application to allow a customer to withdraw cash or access any ATM-specific services. If any of these components is unavailable, the ATM will not work.

Besides hardware and software coupling, tight coupling is also used within software programming to define components that are interlinked and depend on each other to perform or deliver a specific output or process.

Pros:

- The best tightly coupled systems tend to be fast and very efficient as there is very little management overhead
- When relatively low in complexity these systems are relatively easy and quick to change (within the basic constraints of the system itself). Data integrity is also relatively easy to maintain (mainly because of the low system complexity)

- Performance characteristics can hold even when the size of the system grows but the bigger it gets the more rigid/less tolerant to change it will get.

Cons:

- This design pattern becomes very rigid when scaled up. Once you get to a certain level of complexity, performance can still be good but general flexibility reduces as making changes, even small ones, becomes really difficult due to the challenges of managing complex system inter-dependencies.

3.1.4. Physical Security Data Models

Video and audio surveillance are the first data sources regarding physical security. There are many different types of equipment implemented by different providers, to allow the interoperability of these devices ONVIF and PSIA standard association comes into play. ONVIF is a global industry association promoting the use of an open standard to exchange information between physical IP-based security products. PSIA is a global consortium of more than 65 physical security manufacturers and systems integrators focused on promoting interoperability of IP-enabled security devices and systems across the physical security ecosystem as well as enterprise and building automation systems. They promote a standard with open specifications. In addition to the format, other types of specifications have been defined, including a Common Security Model.

3.1.5. Cyber Security Data Models

There are a vast munber of approaches, standards and protocols for how cyber security data is represented. This includes:

- Common Vulnerability Enumeration (CVE)
- The Common Vulnerability Scoring System (CVSS)
- The Common Base Event (CBE) format
- The Common Event Format (CEF)
- The Common Intrusion Specification Language (CISL)
- Intrusion Detection Message Exchange Format (IDMEF)
- Incident Object Description Exchange Format (IODEF)
- The DMTF Common Information Model (CIM)

STIX is one of the more widely used comprehensive approaches.

STIX 2.0 is an open source data format for cyber events and incidents. Its open features make it possible to integrate with existing tools. It is implemented and storable as JSON, thus making it easy to be machine-read. The data structure in based on STIX Domain Objects (SDOs) and STIX Relationship Objects (SROs). An SDO object can represent: attack tactics, "campaign", preventive or response action, identity of individuals or groups, patterns to identify suspicious activities, behaviours with common characteristics, malware, system or network information, reports, threatening individuals or groups, software that can be used for attacks, system or network vulnerabilities.

SROs are the relationships between all the defined SDOs and can be visualized in a graph that helps to understand the text (where the SDOs are the nodes and the SROs are the edges). They are relationships of different types (objective, use, indication, mitigation, attribution, variant of,

impersonation). In addition, there are the Sightings, which determine when a threat is "sighted": what has been seen, what kind of attack, with the aim of tracing the behaviour of the attack. It carries three levels of information: who has seen who (or what) do what. It is an interpretation of raw information, such as observed data.

Events have a modular structure with each event made up of relationships between 2 or more SDOs of a different nature.

```
{
    "type": "campaign",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created": "2016-04-06T20:03:00.000Z",
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against targets in the financial services sector."
}
```

Figure 1: data structure example for a ""Campaign" type SDO

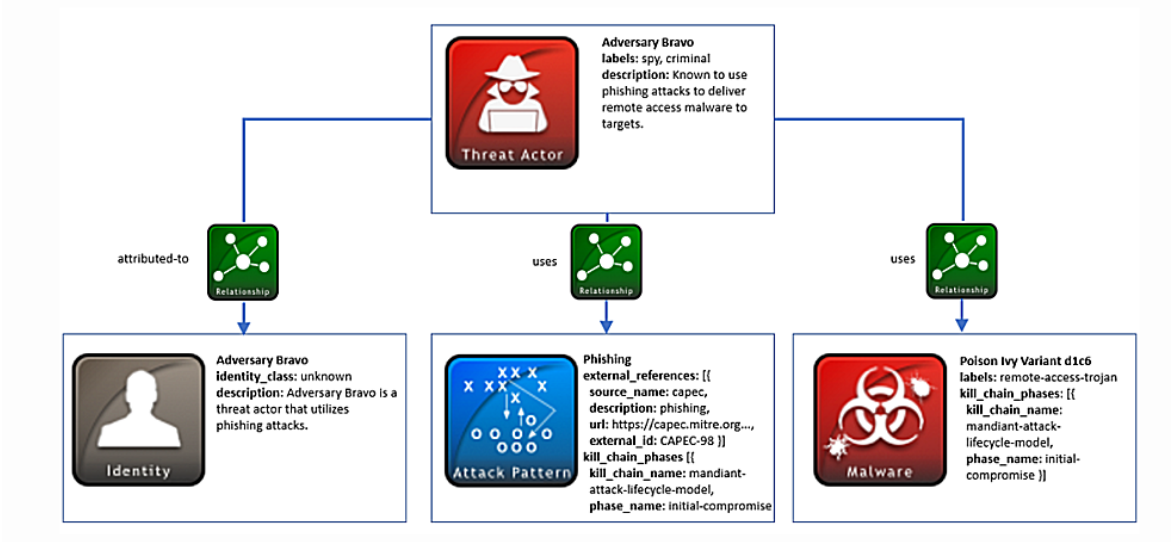

Figure 2: graph representation example of SDOs + SROs composed event

3.1.6. Languages for Data Representation

3.1.6.1. OWL (Web Ontology Language)

The W3C Web Ontology Language (OWL) is a Semantic Web language designed to represent rich and complex knowledge about things, groups of things, and relations between things. OWL is a computational logic-based language such that knowledge expressed in OWL can be exploited by computer programs, e.g., to verify the consistency of that knowledge or to make implicit knowledge explicit. OWL documents, known as ontologies, can be published in the World Wide Web and may refer to or be referred from other OWL ontologies.

3.1.6.2. RDFS (RDF Schema).

Resource Description Framework (RDF) is a standard for data interchange, developed and agreed by W3C. While there are many conventional tools for dealing with data and more specifically for dealing with the relationships between data (i.e., with the semantics embedded in it), RDF is claimed to be the easiest and most powerful. RDF provides a uniform structure, which expresses information by connecting data piece by piece and link by link, allows for any resource (authors, books, publishers, places, people, hotels, goods, articles, search queries) to be: identified; disambiguated; meaningfully interlinked.

RDF Schema (RDFS) is extending RDF vocabulary to allow describing taxonomies of classes and properties. It also extends definitions for some of the elements of RDF, for example it sets the domain and range of properties and relates the RDF classes and properties into taxonomies using the RDFS vocabulary.

3.1.6.3. SPARQL Protocol and RDF Query Language (SPARQL)

SPARQL is a query language to the data presented on the RDF model as well as the protocol for these requests and responses.

3.1.6.4. SWRL (Semantic Web Rule Language)

SWRL is a proposal for a Semantic Web rule language, based on a combination of OWL sublanguages with RuleML sublanguages.

3.2. FINSEC Approach: Integrated Data Modelling (Cyber and Physical)

An integrated physical and cyber security model would comprise information about cyber assets and cyber security incidents, physical assets and related security incidents and more. Information on existing repositories would then have to be transformed to the new schema, in order to allow for the instantiation of a repository of integrated security information and its population with data. This integrated security model could therefore serve as a basis for implementing a security data warehouse and/or a security BigData infrastructure (e.g. a Hadoop/NoSQL infrastructure), that would hold all information that is essential for the FINSEC integrated security applications. This is certainly a tightly coupled approach, as it requires security information repositories and data collection applications to transform their data to a rigorous schema. The advantage of this approach is that it would provide finer control over the security information, along with enforcement of specific types for security information. Nevertheless, the downside of the approach is that it is not very easily expandable with new information, as this requires extensions to the central/integrated scheme and to the middleware functions that are performing the transformations from the existing repositories to the integrated data warehouse or BigData datastores.

One of our aspirations here is to bring into the financial sector some of the approaches that have been used in other sectors to expand the depth and scope of data models in ways that are operationally-attractive and that combine system privacy, resilience and capacity to self-explain their algorithms (captured in the phrase “a viable and informative data model”). Our target is a modelling methodology that can help stakeholders to better manage existential threats (e.g. common-cause failures or rare-but-important combinations of cyber and physical faults or attacks). An example of a candidate approach, potentially applicable to the financial sector and to other sectors dependent on security, is to use multi-fault-tree/multi-attack-tree modelling within a framework for FFIP, functional failure identification and propagation. To summarise:

A viable and informative Data model will be the backbone of our project. This task may be split in two steps:

- Modelling the data to be stored.
- Modelling the operations as well as the relationships available.

Building such a demanding data model is a tough process and maybe overwhelming for most of the cases. Hence, we propose a modular approach where we define the core modelling and then depend on the FINSEC collaborators to enhance this model. This way the model will be adaptive and up to date to face potentially new challenges in future.

Our model will extend STIX to support both cyber and physical threats. Key notions presented in PSIA will be adopted as well.

The STIX protocol was chosen for a number of reasons:

- Sufficiently documented
- Already defined json schemas
- Already implemented validators
- Flexible
- Informative
- STIX also defines the relationships between objects. This is a very powerful feature since it provides the model with potential to be extended and improved in future just by adding a new relationship.

Defining a json representation along with the suitable schema to validate it, is crucial, mainly for the task of information exchange. Regarding the persistence of information, the model has to be accustomed to our needs and data should be stored having in mind analytic, predictive, assessment and monitoring tools. In this case, we might use a relational database or even a no SQL solution such as Cassandra, Redis, or MongoDB.

Just selecting the protocol for the FINSEC project is not enough. We have to adjust and extend the protocol selected to support our needs. An issue that has to be addressed is the creation of new Observables like “network-traffic” which is used by STIX to model observed data. Extending and adding Observables will also affect Sightings. A simple example would be the new observable “temperature”. Another example derived from PSIA may be the “motion” observable. STIX observables can be extended in 3 ways (the rules of each of them are defined inside the document “Stix v2.0 part3 Cyber Observables Core Concepts):

- custom object extensions
- custom observable objects
- custom properties

We should also define new open-vocabularies when needed or enhance the already defined vocabularies. An example case is the enhancement of the “report-label-ov”.

In addition, STIX does not define notions important for FINSEC. Thus, we have to extend STIX with some new SDO (STIX Domain Objects). We propose the following SDOs:

1. Organization
2. Asset
3. Probe
4. Probe Configuration
5. Threat

It is also useful to define the new Relationships.

STIX already defines a set of relationships for its SDOs (provided below for document completion). In fact though, these relationships are not embedded. An SDO can exist with or without a relationship.

For our needs forcing relationships should be considered. This would eliminate cases where a Sighting exists in the FINSEC context without defining the probe which produced this Sighting. Forcing relationships could be implemented by adding more embedded STIX relationships inside the appropriate JSON schemas.

Extending STIX can be achieved either by using custom properties or Custom Objects. The rules for STIX custom properties are:

- A STIX Object MAY have any number of Custom Properties.
- Custom Property names MUST be in ASCII and MUST only contain the characters a–z (lowercase ASCII), 0–9, and underscore (_).
- Custom Property names SHOULD start with "x_" followed by a source unique identifier (such as a domain name with dots replaced by underscores), an underscore and then the name. For example, x_example_com_customfield.
- Custom Property names MUST have a minimum length of 3 ASCII characters.
- Custom Property names MUST be no longer than 250 ASCII characters in length.
- Custom Property names that do not start with "x_" may be used in a future version of the specification for a different meaning. If compatibility with future versions of this specification is required, the "x_" prefix MUST be used.
- Custom Properties SHOULD only be used when there is no existing properties defined

Regarding the Custom Objects approach:

- Producers MAY include any number of Custom Objects in STIX documents.
- Custom Objects MUST support the Common Properties as defined
- The definitions of these properties are the same as those defined in Common Properties and therefore those properties MUST NOT be used to represent the custom properties in the object.
- The type property in a Custom Object MUST be in ASCII and MUST only contain the characters a–z (lowercase ASCII), 0–9, and hyphen (-).
- The type property MUST NOT contain a hyphen (-) character immediately following another hyphen (-) character.
- Custom Object names MUST have a minimum length of 3 ASCII characters.
- Custom Object names MUST be no longer than 250 ASCII characters in length.
- The value of the type property in a Custom Object SHOULD start with "x-" followed by a source unique identifier (like a domain name with dots replaced by hyphens), a hyphen and then the name. For example, x-example-com-custom object.
- A Custom Object whose name is not prefixed with "x-" may be used in a future version of the specification with a different meaning. Therefore, if compatibility with future versions of this specification is required, the "x-" prefix MUST be used.
- The value of the id property in a Custom Object MUST use the same format as the identifier type, namely, [object-type]--[UUIDv4] .
- Custom Objects SHOULD only be used when there is no existing STIX Object defined by the STIX specification that fulfils that need.

attack-pattern	targets	identity	intrusion-set	targets	identity
attack-pattern	uses	malware	intrusion-set	targets	vulnerability
attack-pattern	uses	tool	intrusion-set	uses	attack-pattern
campaign	attributed-to	intrusion-set	intrusion-set	uses	malware
campaign	attributed-to	threat-actor	intrusion-set	uses	tool
campaign	targets	identity	malware	targets	identity
campaign	targets	vulnerability	malware	targets	vulnerability
campaign	uses	attack-pattern	malware	uses	tool
campaign	uses	malware	malware	variant-of	malware
campaign	uses	tool	threat-actor	attributed-to	identity
course-of-action	mitigates	attack-pattern	threat-actor	impersonates	identity
course-of-action	mitigates	malware	threat-actor	targets	identity
course-of-action	mitigates	tool	threat-actor	targets	vulnerability
course-of-action	mitigates	vulnerability	threat-actor	uses	attack-pattern
indicator	indicates	attack-pattern	threat-actor	uses	malware
indicator	indicates	campaign	threat-actor	uses	tool
indicator	indicates	intrusion-set	tool	targets	identity
indicator	indicates	malware	tool	targets	vulnerability
indicator	indicates	threat-actor			
indicator	indicates	tool			

STIX defines the Identity SDO. However for the purposes of FINSEC it seems more viable to model a new entity called Organization. The reason behind this approach is that the Organization should be forced to have a specific type and the Asset SDO will always be owned by an organization. The Organization SDO, identifies a FINSEC financial institution. External references can be used to expose data outside the FINSEC scope. Relationships from Organization can provide Assets owned by the organization and link to other organizations if necessary.

Common Properties
type, id, created_by_ref, created, modified, revoked, external_references, object_marking_refs, granular_markings
Organization Specific Properties
name, description, contact_information

Property Name	Type	Description
type (required)	String	The value of this property **MUST** be organization.
name (required)	String	The name of this Identity. When referring to a specific entity (e.g., an individual or organization), this property **SHOULD** contain the canonical name of the specific entity.
description (optional)	String	A description that provides more details and context about the Identity, potentially including its purpose and its key characteristics.
contact_information (optional)	String	The contact information (e-mail, phone number, etc.) for this Identity. No format for this information is currently defined by this specification.
asset_refs (optional)	List of type identifier	A list of asset identifiers belonging to this organization

Embedded Relationships	
created_by_ref	identifier (of type identity)
object_marking_refs	identifier (of type marking-definition)

Common Relationships			
duplicate-of, derived-from, related-to			
Source	**Relationship Type**	**Target**	**Description**
Organization	Owns	Asset	This Relationship documents that this organization owns an asset.
Organization	part-of	organization	This Relationship is used to document that one organization is part of a bigger organization. An example may be a partner.
Reverse Relationships			
Malware	Targets	organization	See forward relationship for definition.
threat actor	Targets	organization	See forward relationship for definition.
Tool	Targets	organization	See forward relationship for

			definition.
Campaign	Targets	organization	See forward relationship for definition.
attack pattern	Targets	organization	See forward relationship for definition.
intrusion-set	Targets	organization	See forward relationship for definition.

Next SDO to be defined is the Asset object. Asset SDO identifies an asset belonging to an organization. These Assets may be physical (Hardware like ATMs, computers, servers, racks etc), or cyber (Operating systems, Applications, Firewalls). Thus an open vocabulary is created for the domain representation. If the Asset belongs to a domain "cyber" it will probably belong to a network. So, useful information about this network may be its IP address, the subnet mask or even the network type (wireless or not).

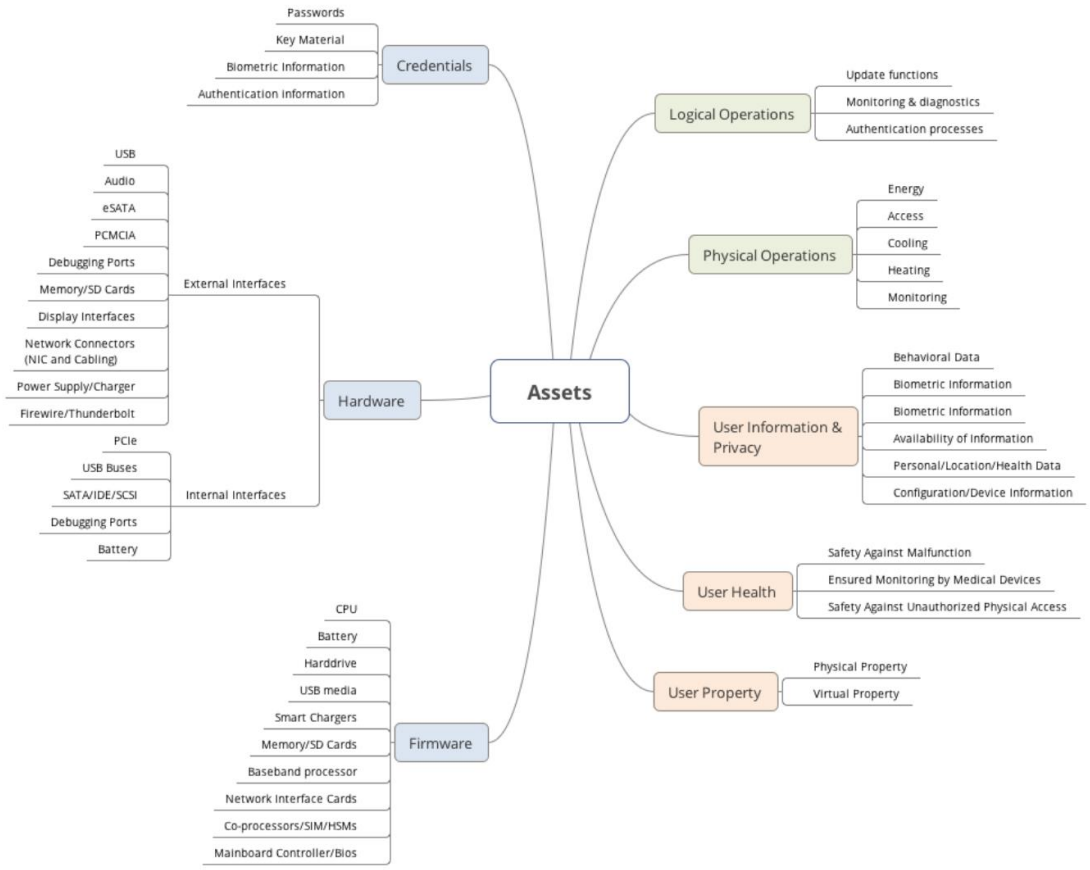

Figure 3 - ENISA Asset Taxonomy (source: ENISA Threat Landscape)

An Asset could be part of other Assets and provides information about the vendor, the version, the organization it belongs or even its current status (switched off/on, under attack etc). In addition another open vocabulary will limit the creator of the asset to specific options (e.g. server room, Operating System, application, server). ENISA (European Union Agency for Network and Information Security) defines employees as a possible asset of an organization. Adopting this logic may be under consideration (this would demand the direct relationship of an Identity with an Asset as well). If needed the vocabulary can be extended after agreement between the partners.

We could also follow the ENISA Asset taxonomy shown in Figure 3.

Common Properties		
type, id, created_by_ref, created, modified, revoked, labels, external_references, object_marking_refs, granular_markings		
Asset Specific Properties		
name, description, asset-domain, asset-type, version, product-name, product_vendor, status_identifier, operating_system, operating_system_version, domain_name, ipv4_addr, ipv6_addr, network_type, subnet-mask, probes_refs		
Property Name	**Type**	**Description**
asset-domain (required)	list of type open-vocab	The value of this property **SHOULD** be a value of the open vocabulary (cyber or physical).
name (required)	String	The name of this Identity. When referring to a specific entity (e.g., an ATM machine), this property **SHOULD** contain the canonical name of the specific entity.
description (optional)	String	A description that provides more details and context about the Identity, potentially including its purpose and its key characteristics.
asset_type (required)	list of type open-vocab	This property has to be a value of the defined open vocabulary (e.g hardware or application).
version (optional)	String	This property represents the version of an asset. It should be defined in case an asset has asset-type of software, hardware or application.
product_name(optional)	String	This property represents the name of the product the asset supports. It should be defined in case an asset has asset-type of software, hardware or application.
product_vendor(optional)	String	This property represents the vendor of the asset (e.g Microsoft, Intel e.t.c). It should be defined in case an asset has asset-type of software, hardware or application.
status_identifier (required)	String	This property identifies the current status of the asset. It can be applied as TLP

operating_system (optional)	list of type open-vocab	This property defines the OS supported by the asset. It should be defined if the asset type is Operating System.
operating_system_version (optional)	String	This property defines the OS version supported by the asset. It should be defined if the asset type is Operating System.
domain_name (required)	String	This property identifies the domain name of an asset. It **SHOULD** be defined in case the asset-type is server.
subnet_mask (optional)	String	This property identifies the subnet mask of the network containing the asset.
network_type (optional)	String	This property identifies the type of the network. It should have a value defined in an open vocabulary (e.g. ethernet or wireless).
probes_refs(optional)	list of type identifier	The probes which belong to this asset

Common Relationships			
duplicate-of, derived-from, related-to			
Source	**Relationship Type**	**Target**	**Description**
Asset	is-owned	organization	This Relationship documents that this asset is owned by an organization.
Asset	part-of	Asset	This Relationship is used to document that one asset is part of another asset (e.g server inside a server room). An example may be a partner.
Asset	Controls	Probe	This Relationship is used to document that one asset controls a number of probes.
Reverse Relationships			
Malware	Targets	Asset	See forward relationship for

			definition.
threat actor	Targets	Asset	See forward relationship for definition.
Tool	Targets	Asset	See forward relationship for definition.
Campaign	Targets	Asset	See forward relationship for definition.
attack pattern	Targets	Asset	See forward relationship for definition.
intrusion-set	Targets	Asset	See forward relationship for definition.

In the figure below we provide an initial architecture for the FINSEC approach to extend the STIX protocol project (only the extra SDOs). As we can see a "Probe" is associated with an "Asset". A Probe can produce Observed Data or even a Sighting (event). The Sighting SDO defined in STIX also provides location information which would be very useful, though we have to extend the "where-sighted-refs" to support assets as well. For our system a Probe is a "smart" entity. Due to the volume of data that can be produced as well as the wasted bandwidth, a probe should be configured to provide only useful data inside specific intervals. Thus a "probe-configuration" object is to be defined and implemented.

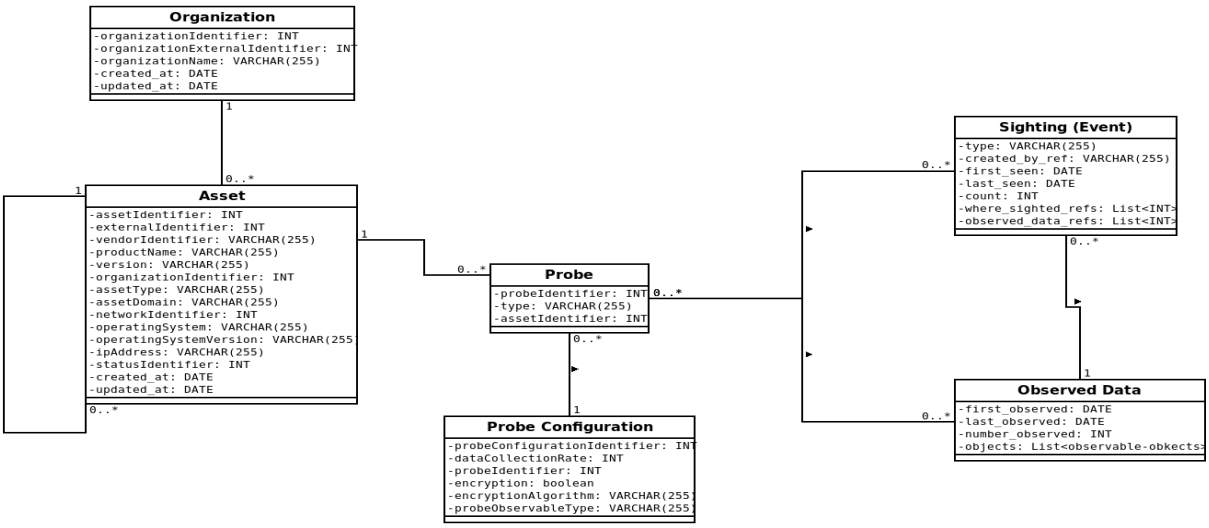

Figure 4 - Architecture proposed by FINSEC to extend STIX

The Probe could be modelled as follows:

Common Properties		
type, id, created_by_ref, created, modified, revoked, labels, external_references, object_marking_refs, granular_markings		
Probe Specific Properties		
name, description, probe-domain, ipv4-addr, ipv6-addr		
Property Name	**Type**	**Description**
probe-domain (required)	String	The value of this property **MUST** be a value of cyber or physical.

name (required)	String	The name of this Identity. When referring to a specific entity (e.g., an ATM machine), this property **SHOULD** contain the canonical name of the specific entity.
description (optional)	String	A description that provides more details and context about the Identity, potentially including its purpose and its key characteristics.
ipv4_addr (required)	String	IP address of the Probe.
ipv6_addr (optional)	String	IP v6 of the Probe.

Common Relationships			
duplicate-of, derived-from, related-to			
Source	**Relationship Type**	**Target**	**Description**
probe	Generates	observed-data	This Relationship is used to document that on probe can produce observed-data.
Probe	Generate	sighting	This Relationship is used to document that one probe can produce a sighting.
Reverse Relationships			
Probe	is_configured	probe_configuration	See forward relationship for definition.
Probe	is_owned	Asset	See forward relationship for definition.

Regarding the Probe Configuration SDO useful information would be the data collection rate, the observed data type as well as the probe it refers to.

Common Properties		
type, id, created_by_ref, created, modified, revoked, labels, external_references, object_marking_refs, granular_markings		
Probe Configuration Specific Properties		
data_collection_rate, encryption, encryption_algorthm, probe_observable_type		
Property Name	**Type**	**Description**
data_collection_rate (required)	Integer	The value represents the interval this probe SHOULD provide its data.
encryption (required)	Boolean	The value represents whether the data will be encrypted or not.
encryption_algorithm (optional)	type of open-vocab	The algorithm that will be used for encryption.
probe_observed_data	type of observable	The type of data the probe under

(required)		configuration will monitor.

duplicate-of, derived-from, related-to			
Source	**Relationship Type**	**Target**	**Description**
probe-configuration	Configures	Probe	This Relationship represents the connection of a Configuration object to a specific probe.

STIX defines a Malware SDO. In our project a more generic entity should be adopted. We name this entity Threat. After the Probe has produced observed data or sightings, reasoners can analyse the data and decide, if the data "Indicate" a Threat. It is under consideration if this threat will be realized by more specific objects and follow the taxonomies proposed by ENISA (figure below). As a first step a Threat will contain information such as the type of threat, external references (e.g. CAPEC), along with the description of the threat and possible solutions. We should also extend the malware-label-vocab for the Threat case. When the system identifies a threat a Course of Action has to take place. Finally, a report will be generated containing the organization, the assets and probes involved, the data coming from the probe as well as the threat indication and the measures taken. Threat actors, vulnerabilities targeted as well as possible campaigns discovered may be part of this report.

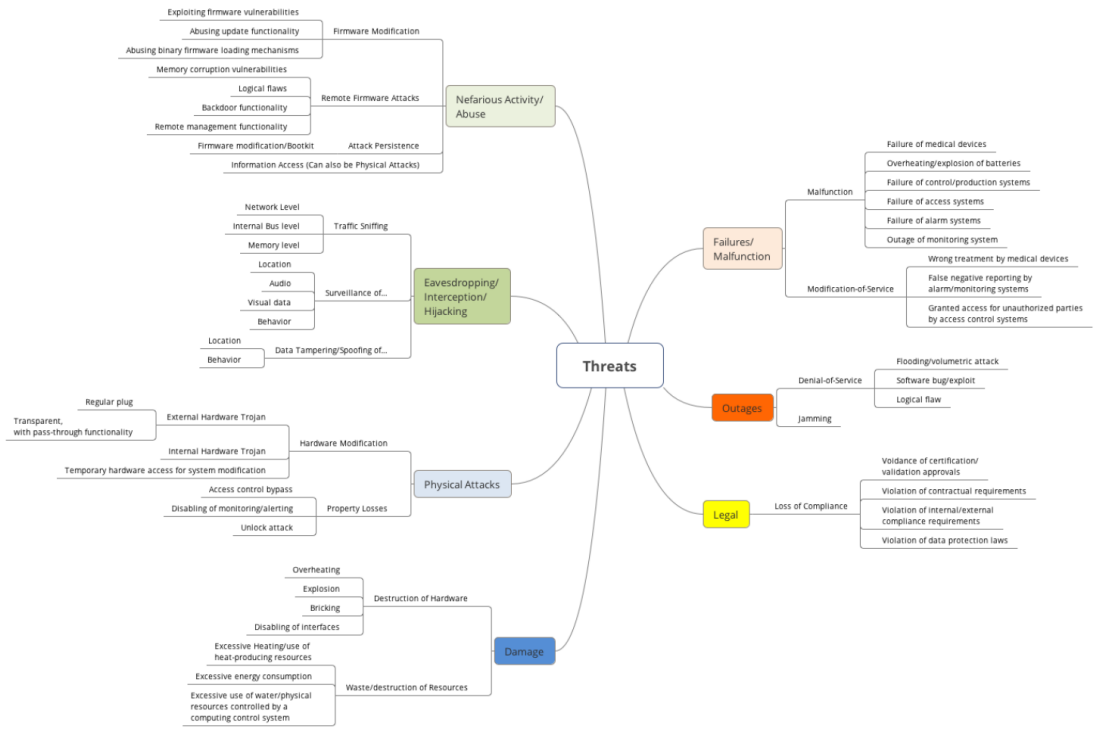

Figure 5 - Taxonomy of threats proposed by ENISA (source: ENISA Threat Landscape)

The following table defines a Threat SDO:

Common Properties		
type, id, created_by_ref, created, modified, revoked, labels, external_references, object_marking_refs, granular_markings		
Threat Specific Properties		
threat_domain, name, description, threat_type, risk, impact		
Property Name	**Type**	**Description**
threat_domain (required)	String	The value of this property **SHOULD** be a value cyber or physical
name (required)	String	The name of this Threat.
description (optional)	String	A description that provides more details and context about the Threat, potentially including its purpose and its key characteristics.
threat_type (required)	String	This property has to be a value of the defined open vocabulary (e.g malware or fire).
risk (optional)	Integer	A risk evaluation number (1-10)
impact(optional)	String	This property represents the impact this threat may result in. It **SHOULD** be a TLP data-marking

Threat inherits its relationships from Malware SDO as defined in STIX.

Embedded Relationships	
created_by_ref	identifier (of type identity or probe)
object_marking_refs	identifier (of type marking-definition)
Common Relationships	
duplicate-of, derived-from, related-to	

Source	Relationship Type	Target	Description
Threat	Targets	identity, vulnerability	This Relationship documents that this Threat is being used to target this Identity or exploit the Vulnerability. For example, a targets Relationship linking a Threat representing a downloader to a Vulnerability for CVE-2016-0001 means that the malware exploits that vulnerability. Similarly, a targets Relationship

			linking a Threat representing a downloader to an Identity representing the energy sector means that downloader is typically used against targets in the energy sector.
Threat	Uses	Tool	This Relationship documents that this Threat uses the related tool to perform its functions.
threat	variant-of	threat	This Relationship is used to document that one piece of Threat is a variant of another piece of Threat. For example, TorrentLocker is a variant of CryptoLocker.
Reverse Relationships			
indicator	Indicates	threat	See forward relationship for definition.
course-of-action	Mitigates	threat	See forward relationship for definition.
attack-pattern, campaign, intrusion-set, threat-actor	Uses	threat	See forward relationship for definition.

To identify higher level notions such as “Threat”, “Tool” and so on, we need a connection to the Knowledge Base as well as components intelligent enough to perform the mapping of observed data. For example, STIX 2.0 defines a “Tool” object which describes well known software than can be used to perform attacks by threat actors. Another example is the “Course Of Action” object which describes a series of actions taken to deal with an attack (similarly Intrusion Set is defined for attack actions). In addition, the “Campaign Model” describes known attacks that are monitored to take place in time intervals. To identify if we have such an entity, we need “intelligent” components.

Our approach is driven by ENISA (figure below). The architecture we have selected is pretty much the same. Attack Vectors can be mapped to STIX Attack Patterns, Countermeasures can be mapped to Course Of Action SDO and Owners to Organizations. Risk is not yet defined but it the Risk Assessment task will introduce this notion in a later step as well.

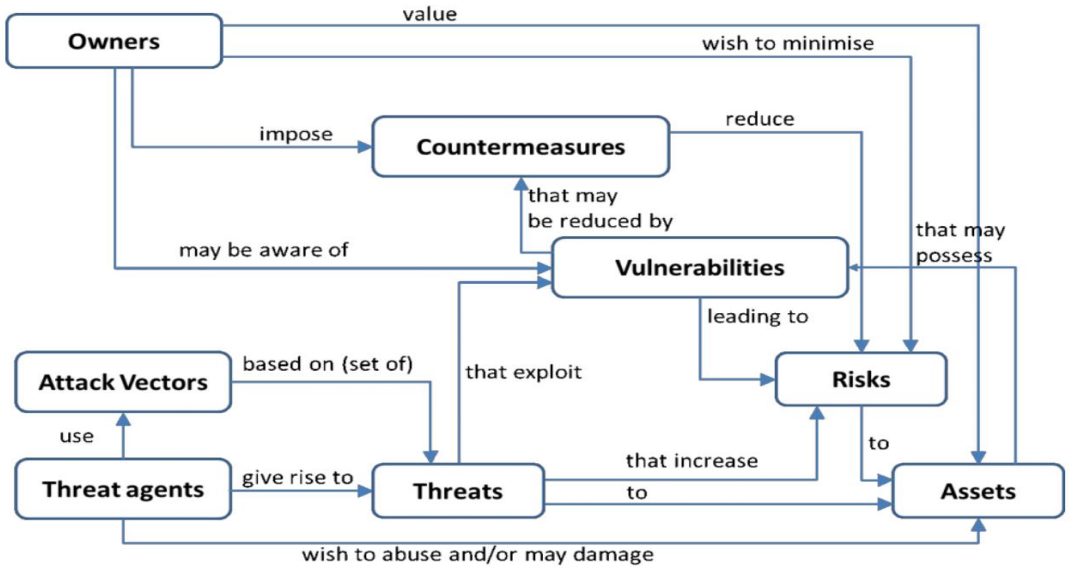

Figure 6: Relationships and Mappings between Entities of the FINSEC Model

4. Assurance Models for Cyber Physical System (CPS)

NIST defines Cyber Physical Systems as:

"Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas"

A CPS, is a system in which the computational elements interact closely with physical entities, thus controlling individual, organizational processes or mechanics through the use of information and communication technologies (computer, software and networks). CPSs are exposed to a wide range of new attacks that are possible even in the absence of a direct or indirect connection of the device to the network. In these systems, a hacker can succeed in gaining control of the physical portion of the system and therefore in causing a cyber-attack to affect the physical world, with possible consequences on the environment.

Innovation and Digital Transformation in Financial Services is occurring at an increasing pace.

It is entirely feasible that we will see the increase in cyber physical systems in the very near future where[1]:

- branches and operation centres staffed by sophisticated robots instead of human tellers
- everyone from high net worth investors to high school teachers taking financial advice from artificially intelligent apps – and then investing across asset classes, currencies and geographies on a real-time basis
- where launching a bank, an asset manager or an insurance company was as simple as plugging in an appliance

[1] PwC Financial Services Technology 2020 and Beyond (PwC White Paper, 2016)

These advances, through the proliferation of cyber physical systems, are becoming increasingly pervasive and complex and require methods by which the security of them can be evaluated.

4.1.The State-of-the-Art

4.1.1. The NIST CPS Framework

The NIST CPS Framework [NIST 1500-201] describes the CPS environment and stakeholder concerns, and provides an overview of the CPS Framework analysis methodology with its core concepts of aspects (groupings of cross-cutting concerns) and facets (components of the systems engineering process with associated activities and artifacts) of which Assurance is one of the three facets. The Assurance facet (how to prove things actually work the way they should leading to CPS assurance) provides a methodology for understanding the scope and limits of CPS capabilities. According to the standard elements of the CPS assurance consists of statements built from data produced during the activities of the first two facets of the framework, conceptualization and realization. The elements, are: Claims, Evidence, Argumentation, Estimate of confidence:

The typical statement of assurance (an assurance judgment) takes the form:

> *"The [Evidence] is sufficient to conclude that the [Claims] are true based on the [Argumentation] with this [Estimate of Confidence]."*

This relationship between evidence, claims, argumentation, and estimate of confidence can be formalized. Elements of Assurance, how Evidence is formed from artefacts, and how Argumentation is formed from a variety of things, are respectively depicted in figures Fig. 10, Fig. 11, and Fig. 12 of [NIST 1500-201].

An example is a CPS that has fully secured time. This must possess the necessary assurance and resilience attributes; Source channel assurance, Source data assurance, User-provided assurance, Predictable failure, and Availability and Diversity described in Table 1 of [NIST 1500-202].

ISO/IEC/IEEE 42010 defines the following terminology:

- An *architecture framework* consists of the "conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders."
- A *concern* is an "interest in a system relevant to one or more of its stakeholders."
- An *architecture view* consists of "work product expressing the architecture of a system from the perspective of specific system concerns."
- An *architecture viewpoint* consists of "work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns."

Within the context of this model, ISO 10746 (RM-ODP) is an architecture framework that defines the following five architecture viewpoints that address specific concerns:

- The *enterprise viewpoint*, which focuses on the purpose, scope and policies for the system.
- The *information viewpoint*, which focuses on the semantics of information and information processing.
- The *computational viewpoint*, which focuses on the functional decomposition on the system into objects which interact at interfaces.

- The *engineering viewpoint*, which focuses on the mechanisms and functions required to support distributed interactions between objects in the system.
- The *technology viewpoint*, which focuses on the choice of technology of the system.

4.1.2. Common Criteria

A very traditional method for security assurance in information handling systems is the Common Criteria (CC) [ISO 15408]. This method has been applied to many types of products and services, but historically the principles go back to the Trusted Computer System Evaluation Criteria (TCSEC) commonly known as *The Orange Book* [DoD 5200.28-STD] and systems that handle military classified information. Other developments that constitute the background for the criteria are the European ITSEC criteria [Information Technology Security Evaluation Criteria] and the Canadian CTCPEC criteria that combined ITSEC with TCSEC. The overall purpose of the CC is to establish consistent and internationally recognized evaluation regime for security products. The overall objectives were:

1. to ensure that evaluations are done to a high and consistent standard, and seen to contribute significantly to confidence in the security of those products/profiles;
2. to improve the availability of evaluated and security-enhanced products and profiles;
3. to re-use evaluations of IT products and protection profiles;
4. to improve the efficiency and cost-effectiveness of the evaluation process itself

There are four key concepts that have been built into the CC, these are:

i) the Security Target (ST); it is a structured statement giving an implementation-dependent description of the security needs for an identified TOE
ii) the Target of Evaluation (TOE); a specified set of software, firmware and/or hardware
iii) Protection Profiles (PP); implementation-independent statement of security needs for a TOE type, and
iv) Evaluation Assurance Levels (EAL1-7); a set of assurance requirements drawn from ISO/IEC 15408-3, representing a point on the predefined assurance scale that form an "assurance package" from a defined set of "assurance components".

The main advantage from applying these concepts is that the evaluation process is fairly predictable and one is developing and evaluating a Security Target and TOE that is stable (but maybe not static) throughout the evaluation. Through the use of comparable and established Protection Profiles one can also re-use previous work to increase efficiency. A common methodology for evaluation based on the CC has also been established. This is together with the CC the foundation for mutual recognition of Certifications between 15 member countries through the Common Criteria Recognition Arrangement (CCRA).

A stable TOE in combination with the predefined Protection Profiles can also become a significant problem as the TOE and ST will need to be fairly constant over the full product/service life-cycle. It means that CC Certified products for all practical purposes are (rather) small, at least smaller as the assurance levels goes above *EAL 4+*. Hence, we cannot expect the CC to be very useful for evaluation of evolving/dynamic large systems at high assurance levels. This is in particular the case for agile or DevOps based organisations working on complex systems in changing environments, i.e. like in FINSEC. So, when systems are evolving or under almost continuous development, we also need to base assurance and evaluation activities on more flexible methods.

Another issue with CC evaluation is that the level of detail needed to "specify" the security target and the security measures tends to be very detailed and bottom-up. Hence, at a certain level of complexity it becomes too resource demanding to keep all the required textual documentation up to date.

An alternative is to take a more risk-based approach; creating high level system models of the product/service including assets, threats and security controls - then we do not need to have all the textual documentation that the CC mandates. If needed further detailed design models can be used to supplement the high-level models and improve the confidence in assurance evidence and argumentation.

4.2.The FINSEC Assurance Method

The FINSEC Assurance Method will be based on work done in a previous project by the partners – EU FP7 PCAS.

The overall goals for this assurance method are that it shall:

- be based on international open standards as far as possible
- capture system specific properties (for example, functionality, timing, storage)
- document basic security concepts (for example, assets, threats, security requirements, and controls)
- include models that are appropriate and useful for security design as well as analysis and implementation and testing
- be technology neutral, that is, not assume specific technologies or products to be realized

The method consists of two main activities: first the system is modelled comprehensively in a viewpoint architecture (RM-ODP) and then, based on various features in the model, a risk assessment is carried out. If the risk is higher than the acceptable threshold in any area, the system description is modified and the risk assessment is repeated.

RM-ODP (ISO 10746/ITU-T X.901-X.904) is an architecture framework that defines five architecture viewpoints that address specific concerns of the system:

The first step of the assurance method is to model the system in the five RM-ODP viewpoints, addressing separate security-relevant concerns in each one.

The plan for assuring various security properties of the FINSEC system is to model it in the relevant RM-ODP viewpoints, addressing separate concerns in each one.

- **The objectives of the CPS should be modeled in the enterprise viewpoint.**
- **The information processed and stored in the CPS can be modeled in the information viewpoint.**
- **The system architecture of the CPS will be modelled in the computational viewpoint.**
- **The distributed realization of the CPS should be modeled in the engineering viewpoint.**
- **The technology used to realize the CPS can be modeled in the technology viewpoint.**

Which of these viewpoints that are needed for particular assurance purposes can vary, but the engineering viewpoint is important as it includes the concept of a 'node' and this can in most cases be mapped to a physical entity. Hence, by extending the engineering viewpoint one should enable a combination of both cyber and physical assets in the same model.

When these views have been modeled, correspondences can be established between them, including the following:

- A correspondence between the enterprise and the computational viewpoints, to show how the functional decomposition supports the objectives of the system.
- A correspondence between the computational viewpoint and the information viewpoint, to show how information is created, transformed, and stored in computational objects.
- A correspondence between the computational and the engineering viewpoints, to show how the functional decomposition is supported by the engineering structures.
- A correspondence between the engineering and the technology viewpoints, to map abstract engineering objects to concrete technologies.

Using the resulting model as a basis, a risk analysis can be performed on the engineering model, the information model, and the technology model. The assets identified in the system are the engineering objects and the information that is processed by these objects. The technology viewpoint model provides important supporting information for scoring risks, since risks may vary depending on the concrete technology employed. The risk analysis entails identification of threat sources, which are further detailed into threat events affecting various properties of the assets.

The risk analysis of the CPS needs to consider a wide range of objectives for the properties of the assets within it. The set of properties considered transcends the regular CIA triad (confidentiality, integrity, and availability). NIST SP 1500-202 recommends an interdisciplinary design approach to CPS engineering, consisting of the following areas:

- Safety
- Reliability
- Privacy
- Cybersecurity
- Resilience

Concrete objectives in these categories will be modeled in the enterprise viewpoint. They will guide the risk analysis by providing valuation of the assets identified in the other viewpoints.

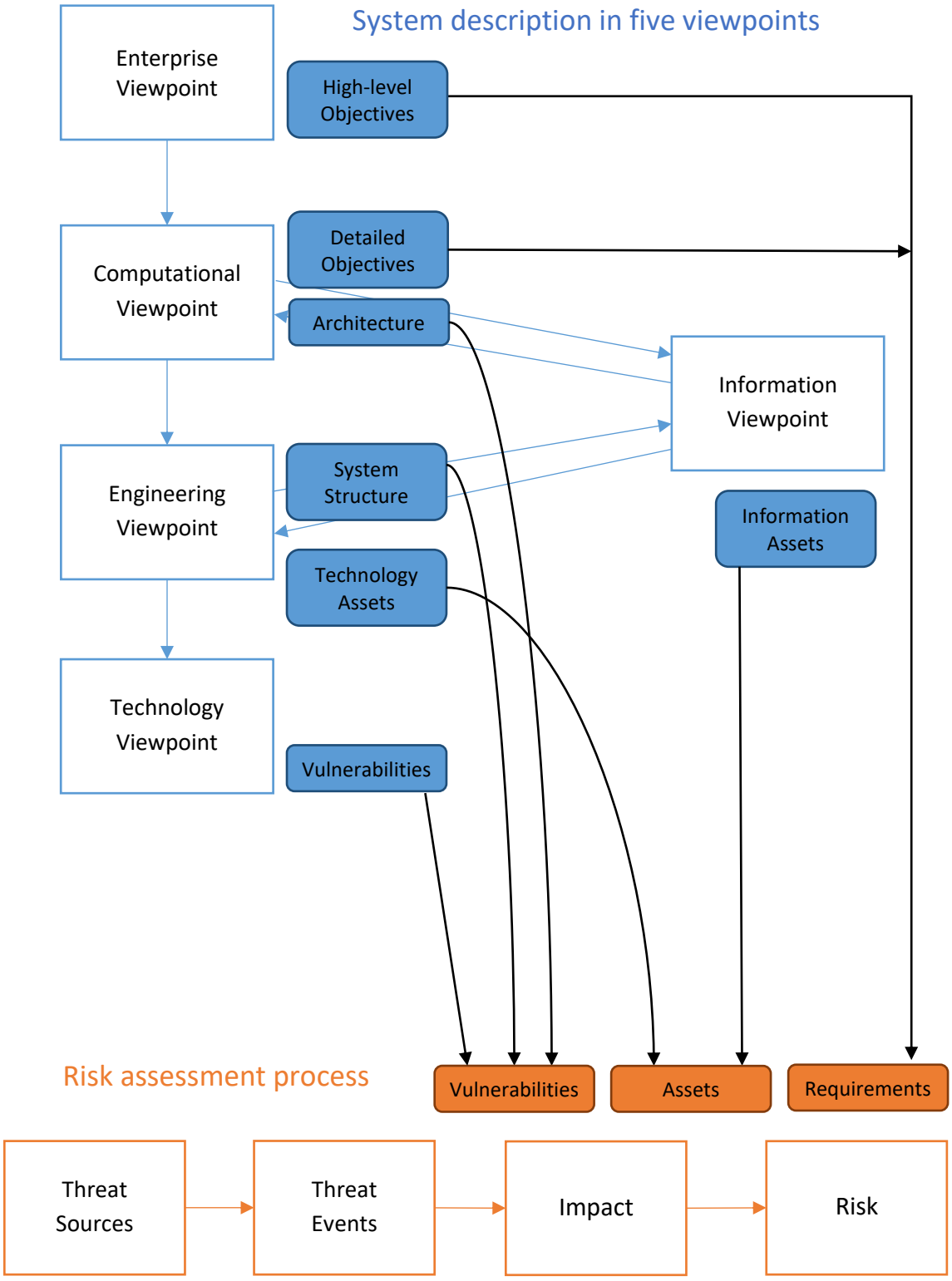

Figure 7: Description in the five viewpoints

When these views have been modeled, correspondences are established between them to show that they are consistent with one another.

Using the resulting model as a basis, a risk assessment can be performed, with inputs from features modeled in the five viewpoints, providing precise information on assets, vulnerabilities, and security objectives.

4.2.1.1. Enterprise Viewpoint Modelling

The Enterprise Viewpoint focuses on the purpose, scope and policies for the system. In this viewpoint, the system is modeled as a set of objects that form a part of the environment in which the system operates. The relationship between the objects representing the system and the external objects is described. Specifically, the description includes the roles played by the system, the activities undertaken by the system, and policy statements about the system. These policy statements include the contracts that exist between the system and its environment. A contract may express obligations, permissions, and prohibitions between its involved objects.

There is considerable overlap between the Enterprise Viewpoint description and what is normally called requirements to the system. In particular, high level security objectives are modeled here and provided as input to the risk assessment process.

4.2.1.2. Information Viewpoint

An information specification defines the semantics of information and the semantics of information processing. It specifies how information is created, how it evolves, how it is destroyed, and what it means. All information assets identified in the risk assessment phase are modeled as information objects, and these objects can be modeled at any given level of abstraction. In particular, information object must be described at abstraction levels suitable for establishing correspondences to the computational and the engineering viewpoints.

The modeling of information objects starts in parallel with the modeling of the objects comprising the system architecture in the computational viewpoint. It continues with the development of the concrete system structure in the engineering viewpoint and correspondingly more detailed information objects. All these information assets are provided as input to the risk assessment process.

4.2.1.3. Computational Viewpoint

The Computational Viewpoint describes the functional decomposition of the system into objects that interact at interfaces. This description is independent of both location and technology. In other words, it corresponds to what is normally called the "architecture" of the system. From a given architecture it is possible to configure an endless variety of concrete distributed systems conforming to that architecture. It must be possible to establish a correspondence between the Computational Viewpoint description and the Enterprise Viewpoint description, so that computational objects can be clearly assigned to roles, responsibilities, and domains. It must also be possible to establish a correspondence between computational objects and interfaces and information objects at a suitable level of abstraction.

The computational viewpoint description also includes more detailed security objectives, which are input to the security assessment process.

4.2.1.4. Engineering Viewpoint

The Engineering Viewpoint describes the actual distribution of the system as a structure of engineering object spanning across a set of physical locations. This distributed system must conform to the architecture described in the computational viewpoint. In other words, a correspondence between the engineering objects and technology objects must be established. It is possible for one

computational object to be mapped to a whole substructure of engineering objects that span several geographical locations. A correspondence must also be established between engineering objects and information objects, normally at a lower level of abstraction than the one with the computational viewpoint. Finally a correspondence with the Technology Viewpoint is needed in order to map the engineering objects to concrete technologies.

The Engineering Viewpoint is the focal point of the risk assessment of the system. It contains abstract descriptions of all the technology assets to be subjected to risk assessment, and the corresponding information objects contain all the information assets to be subjected to risk assessment. The mapping from engineering objects to technology objects in the Technology Viewpoint provides information on how to score the risk based on a particular technology.

4.2.1.5. Technology Viewpoint

The Technology Viewpoint describes the chosen technology to be used in the system, whether this is ready-made or custom-made technology. From a risk assessment point of view, the chosen technology usually has a direct influence on individual risk assessments regarding the technology and information assets. Data on the different technologies vulnerabilities is input to the risk assessment process.

4.2.1.6. Risk Assessment Process

The risk assessment process is based on NIST SP 800-30, which is designed to be consistent with the ISO 31000 processes. Here we use the results from the ODP viewpoints directly as input to the Risk Assessment process as described in NIST SP 800-30. Architectural vulnerabilities are collected from the computational viewpoint, structural vulnerabilities from the engineering viewpoint, and technological vulnerabilities from the technology viewpoint. Technology assets are collected from the engineering viewpoint and information assets from the information viewpoint. High-level security objectives are collected from the enterprise viewpoint and detailed security objectives from the computational viewpoint.

Physical assets are not explicitly modeled in the viewpoints of ODP, but the Engineering and Technology viewpoints are candidates to be extended to also cover related physical assets and security zones. The details of such potential extension will be covered in a later deliverable (D 5.4).

When preparing for the risk assessment process, appropriate risk scales and risk thresholds are established. The risk assessment process starts by identifying threat sources and threat events in relation to the identified vulnerabilities and assets. Impact (consequences) is then analyzed in relation to the identified assets. A final risk score is computed and evaluated against the risk acceptance criteria and policies given. Prioritized risk must then be handled, typically by adding appropriate security services (controls). The process should then be repeated until the residual risk is below the acceptable thresholds.

5. Predictive Security Approaches

Methods of Predictive Security Analytics can be classified into three categories: statistical methods, machine learning, and knowledge-based methods, as shown in Figure 8.

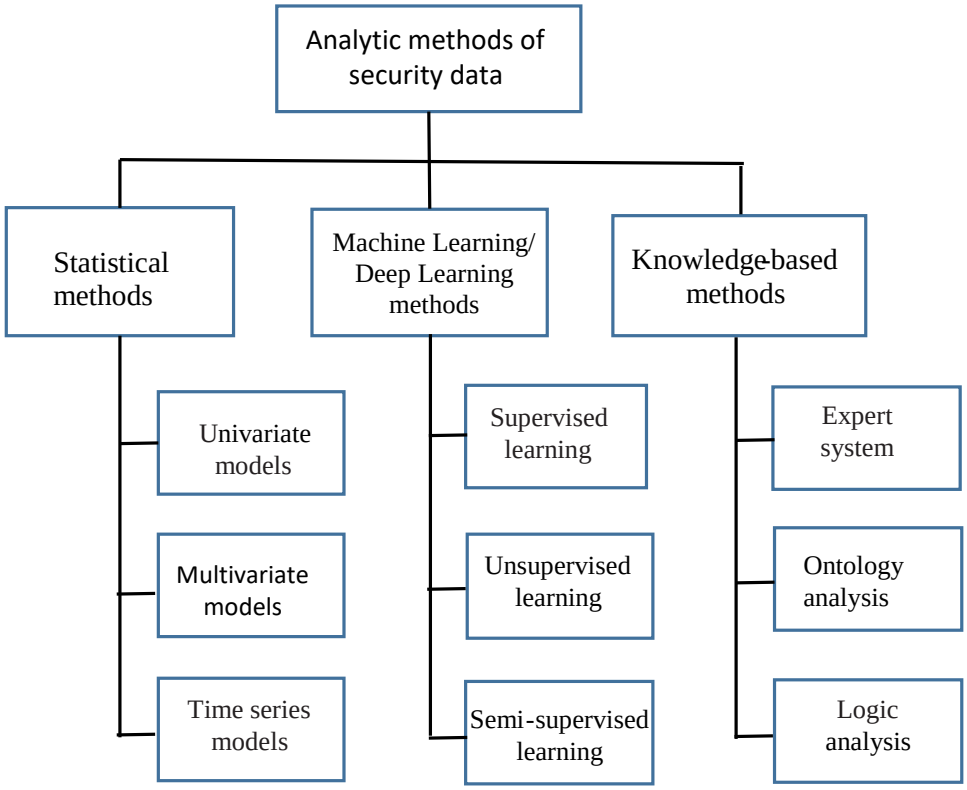

Figure 8 Classification of analytic methods of security data [Jing 2018]

The ensuing sections describe briefly the three classes.

5.1.Statistical Methods

In this approach, network traffic activity is captured and a profile representing its normal behaviour is generated. This is done using metrics such as packet level data and flow level data. For instance, a statistical inference is applied to calculate an anomaly score which is generated based on currently observed traffic. If the score is higher than a given threshold, then an alarm of anomaly is generated. We distinguish three relevant models applied in statistical methods: **Univariate models**, **multivariate models** and **time series models.**

There are several used examples of statistical methods in attack detection. One can cite the information entropy, which consists in to summarize the traffic distribution by capturing the important characteristics of traffic features. Entropy-based methods are suitable for detecting attacks launched by Botnet based on anomalous patterns in networks.

Another statistical method is Cumulative Sum (or CUSUM) algorithm which is a sequential technique used to detect irregular changes in traffic traces.

The statistical methods have some number of advantages. We can cite:

- They do not require prior knowledge of network attacks. Hence, they are capable to detect zero-day attacks.
- They use few features to characterize the network traffic leading to considerably reduce their time and space complexity.

These methods have also some drawbacks that we cite below:

- These methods can be trained by an attacker.
- An appropriate threshold is difficult to set in order to better balance false positives and false negatives.

5.1.1. Bayesian Inference

Bayesian inference is a collection of statistical methods which are based on Bayes' formula. Statistical inference is the procedure of drawing conclusions about a population or process based on a sample. Characteristics of a population are known as parameters. The distinctive aspect of Bayesian inference is that both parameters and sample data are treated as random quantities, while other approaches regard the parameters non-random.

An advantage of the Bayesian approach is that all inferences can be based on probability calculations, whereas non-Bayesian inference often involves subtleties and complexities. One disadvantage of the Bayesian approach is that it requires both a likelihood function which defines the random process that generates the data, and a prior probability distribution for the parameters. The prior distribution is usually based on a subjective choice, which has been a source of criticism of the Bayesian methodology. From the likelihood and the prior, Bayes' formula gives a posterior distribution for the parameters, and all inferences are based on this.

Bayesian inference can be used to model "normal" behaviour on a company's corporate network. Once that model has been built, any unusual or suspect behaviour can be identified in "real time".

Security log analysis is retrospective: if an attacker has compromised your network, analysing the logs is too little, too late. Other so-called "behavioural" mechanisms, which attempt to identify suspicious activity, are rules-based, and therefore cumbersome to manage.

5.2.Machine Learning

Machine learning aims to establish an explicit or implicit model of analyzed patterns. The machine learning is mainly divided into three categories: (i) supervised learning, (ii) unsupervised learning, and (iii) semi-supervised learning. In the supervised learning, the algorithm learns knowledge from labeled data and uses the obtained knowledge to classify the unknown data. Several supervised learning algorithms (e.g., K-Nearest Neighbor (KNN), Support Vector Machines (SVM), and Artificial Neural Network (ANN), Decision Trees, etc.) have been widely applied to detect network attacks. In the unsupervised learning, the algorithm finds the underlying structure of the data without any labels. The unsupervised learning methods that mainly work based on similarity or distance computation are divided into partitioning methods (e.g., K-means, K-medoids, etc.), hierarchical methods (e.g., BIRCH, Chameleon, etc.), density based methods (e.g., DBSCAN, OPTICS, etc.), and grid-based methods (e.g., STING, CLIQUE, etc.).

In machine learning, classification refers to a set of computational methods for predicting the likelihood that a given sample belongs to a predefined class, like whether a piece of email belongs to the class "spam" or a network connection is benign or associated with a botnet.

Classifiers can often produce excellent results under favourable conditions. However, this is not always the case. For example:

- It can be extremely difficult for analysts to obtain a sufficiently large and accurately classified set of labelled data.
- Accuracy will be compromised if the samples selected don't precisely reflect the actual prevalence of positive and negative cases.
- In addition, the ratio of positive to negative cases must fall within acceptable tolerances for classification to work well. Generally speaking, however, analysts can usually build accurate models if they can secure a sufficient quantity of data from each class.

5.2.1. Classification via Logistic Regression (LR)

Mathematically, Logistic Regression (LR) is a linear classifier, meaning that it utilizes straight lines and planes to distinguish vectors belonging to one class from another. In binary classification, the analyst's goal is to build a model that carves feature space into two regions, with each region enclosing vectors that belong to one class only. This process is referred to as fitting the data. In LR, the line or plane that separates one region from another is referred to as the decision boundary.

Distortions can be caused by regression weights with very large values. Consequently, the LR algorithm provides a number of penalty parameters that analysts can use to mitigate these effects.

Logistic regression pitfalls and limitations. The logistic regression algorithm in scikit-learn is efficient and can produce excellent results given certain limitations:

- The underlying data must intrinsically support linear classification. Operationally, this means that it must be possible to accurately classify vectors using decision boundaries that carve up feature space with straight lines and planes. If the dataset is not linearly separable in this way, more complex methods of representing features may be employed or the analyst may decide to use a different classification algorithm.
- LR is vulnerable to under-fitting when datasets have many outliers, features with disproportionately large values, and sets of features that are highly correlated. Normalization and regularization can only partly offset these effects.

5.2.2. Classification with Decision Trees (DT)

Decision tree algorithms determine whether a given vector belongs to one class or another by defining a sequence of "if-then else" decision rules that terminate in a class prediction. The type of DT algorithm selected depends on whether the class label will have categorical or continuous values.

- If the class label is categorical, e.g., we want to predict whether or not a given network connection is associated with a botnet, we would utilize DT classification.
- If the class label has continuous values, e.g. we want to predict the best selling price for a new product, then we would utilize DT regression.

Mathematically, DT is a non-linear classifier. This means that, unlike LR, DT does not construct decision boundaries with straight lines and planes. Instead, it carves feature space into rectangles that may

contain as little as a single vector each. This difference has important implications for the fitting process and how this influences the resulting models accuracy.

Decision Tree pitfalls and limitations. Even with its default hyper parameter settings, the DT algorithm works well and requires comparatively little advance effort to prepare the sample data. It can also produce models that are highly efficient since they employ only the subset of features required to classify rather than the entire feature set. In contrast, LR models generally include all of the features in the sample matrix except for those intentionally removed through regularization. However, decision trees are subject to certain characteristic errors and limitations.

- All DT classifiers, can produce overly complex trees that over-fit the data and perform poorly when exposed to test data.
- In general, the larger the feature set, the more likely over-fitting is to occur.
- The implementation of split points is determined based on "local" optimizations between a parent node and its child leaf rather than on what might be optimal for the tree as a whole. Consequently, there is no way to ensure that a given tree has taken the optimal form. Decision trees can be unstable. Small variations in the sample data can cause a completely different tree to be produced.

Analysts can address these issues by creating ensembles of trees from random subsets of the training data. Each tree is then able to "vote" on whether a given sample belongs to one class or another. The prediction that receives the most votes wins. In scikit-learn, this is accomplished using the Random Forest algorithm.

5.2.3. Classification with the Naive Bayes Algorithm

Bayes Theorem provides the means to calculate the probability that a given event A will occur when condition B is true. In a classification problem, Bayes Theorem enables us to compute the conditional probability that a sample belongs to a particular class given its feature attributes.

The Bayes Theorem can be difficult to solve because it takes conditional probabilities into account. The Naïve Bayes Theorem dramatically simplifies this process by making the assumption of class conditional independence. In other words, it ignores the potential effects of conditional probabilities when it assigns samples to classes. In almost every case, this assumption is untrue. It's in this sense that this formulation of the Bayes Theorem is naïve. Surprisingly, however, the Naïve Bayes often produces excellent results and with great efficiency since it requires only four components to classify a sample.

Naïve Bayes pitfalls and limitations. Naïve Bayes is surprisingly effective in producing accurate classifications based on computed priors, although with some limitations:

- Naïve Bayes assumes that features are conditionally independent. In most real-world problem scenarios, this assumption is untrue. Despite this, Naïve Bayes often produces excellent results.
- When the dataset available is sparse, we may not be able to capture all of the actual feature/ class combinations that exist in the underlying data environment. Fortunately, we can ameliorate these effects with Laplace and other smoothing techniques.

5.2.4. Clustering

Clustering encompasses a variety of techniques for sub-dividing samples into distinct sub-groups or clusters based on similarities among their key features and attributes. Clustering is particularly useful in data exploration and forensic analysis thanks to its ability to sift through vast quantities of data to identify outliers and anomalies that require further investigation.

The purpose of cluster analysis is to segregate data into a set of discrete groups or clusters based on similarities among their key features or attributes. Within a given cluster, data items will be more similar to one another than they are to data items within a different cluster. A variety of statistical, artificial intelligence, and machine learning techniques can be used to create these clusters, with the specific algorithm applied determined by the nature of the data and the goals of the analyst.

5.2.4.1. Assessing Cluster Validity

At the conclusion of every clustering procedure, we're presented with a solution consisting of a set of k clusters. There however remains the need to assess whether these clusters are accurate representations of the underlying data. The problem is compounded when we run a clustering operation multiple times with different algorithms or the same algorithm multiple times with different hyper parameter settings.

Fortunately, there are numerous ways to validate the integrity of our clusters. These are referred to as "indices" or "validation criteria."

5.2.4.2. Key Clustering Take-aways

Clustering provides a mathematically rigorous approach to detecting patterns and relationships among network, application, file, and user data that might be difficult or impossible to secure in any other way.

- Cluster analysis can be applied to virtually every kind of data once the relevant features have been extracted and normalized. In cluster analysis, similarity between samples and their resulting cluster membership is determined by measuring the distance between vectors based on their locations in feature space. A variety of distance metrics can be applied, including Euclidean, Manhattan, Manhattan, Cosine, and more.
- Clustering results must be statistically validated and also carefully evaluated with respect to real-world security threats. This requires a significant amount of domain expertise and a deep understanding of the capabilities, pros, and cons of each clustering method.
- Clustering is particularly useful in data exploration and forensic analysis because it allows us to sift through vast quantities of data to identify outliers and anomalies.

5.3. Deep Learning

Deep Learning is a type of Neural Network Algorithm that takes metadata as an input and processes the data through a number of layers of the non-linear transformation of the input data to compute the output. This algorithm has a unique feature i.e. automatic feature extraction. This means that this algorithm automatically grasps the relevant features required for the solution of the problem. This reduces the burden on the programmer to select the features explicitly. This can be used to solve supervised, unsupervised or semi-supervised type of problems.

In a Deep Learning Neural Network, each hidden layer is responsible for training the unique set of features based on the output of the previous layer. As the number of hidden layers increases, the complexity and abstraction of data also increase. It forms a hierarchy from low-level features to high-

level features. With this, it becomes possible that a Deep Learning Algorithm can be used to solve higher complexity problems requiring a large number of non-linear transformational layers.

Deep learning is not a silver bullet that can solve all the cyber security problems because it needs extensive labelled datasets. Unfortunately, no such labelled datasets are readily available. However, there are several use cases where the deep learning networks are making significant improvements to the existing solutions. Malware detection and network intrusion detection are two such areas where deep learning has shown significant improvements over the rule-based and classic machine learning-based solutions.

Network intrusion detection systems are typically rule-based and signature-based controls that are deployed at the perimeter to detect known threats. Adversaries change the malware signatures and easily evade the traditional network intrusion detection systems.

Deep learning (DL)-based systems using self-taught learning have proved promising in detecting unknown network intrusions. Traditional security use cases such as malware detection and spyware detection have been tackled with deep neural net-based systems.

The DL-based neural nets are now getting used in User and Entity Behaviour Analytics (UEBA). Traditionally, UEBA employs anomaly detection and machine learning algorithms which distill the security events to profile and baseline every user and network element in the enterprise IT environment. Any significant deviations from the baselines were triggered as anomalies that further raised alerts to be investigated by the security analysts. UEBA enhanced the detection of insider threats, albeit to a limited extent.

5.3.1. Log Analysis

There are various methods that are introduced for the analysis of a log file such as pattern recognition methods like K-N Algorithm, Support Vector Machine, Naive Bayes Algorithm etc. Due to the presence of a large amount of log data, these traditional methods are not feasible to produce efficient results. Deep Learning Neural Network shows excellent performance in analysing the log data. It consists of excellent computational power and automatically extracts the features required for the solution of the problem. Deep learning is a subpart of Artificial Intelligence. It is a deeply layered learning process of the sensor areas in the brain.

Some of the different Techniques for Deep Learning are: Convolutional Neural Networks; Restricted Boltzmann Machine; Recursive Neural Network and Recurrent Neural Network (RNN)

Some Key Take Away's for Deep Learning are:

- Neural networks are extremely flexible, general-purpose algorithms that can solve a myriad of problems in a myriad of ways. Unlike other algorithms, for example, neural networks can have millions or even billions of parameters applied to define a model.
- Neural networks employ layers of processing, with each layer and its set of nodes performing a particular kind of computation. At least one of these layers will be hidden. It is this multi-layered approach employing hidden layers that distinguishes deep learning from all other machine learning methods.
- All of the nodes in each hidden layer are randomly assigned a set of weight values, one for each feature in the sample set. During processing, each node multiplies the feature value by its corresponding weight, sums the products, and then passes the result through an activation function that performs the calculation specified for that layer. The result is an activation value that reflects the aggregate effect of that node's processing.
- After each training cycle, a loss function compares the classification decision assigned at the output layer to the class labels in the training set to determine how the weights in all of the

hidden layers should be modified to produce a more accurate result. This process repeats as many times as required before a set of candidate models can proceed to the validation and testing phases.

5.4. Knowledge Based Methods

In these approaches, network or host events are matched with predefined attack rules or signatures to examine them for the presence of known attack instances. The most used among knowledge-based methods is the **Expert System.** They extract the specific features from training data and build rule classifying new data. There exists also another approach called **ontology analysis** which expresses the relationships between collected data and uses them to infer particular attack types. Another approach is **logic analysis** and consists of a logic structure and uses this structure to determine whether network events are legal.

As we discussed the advantages and drawbacks of the cited methods, the knowledge-based methods have also some advantages such as:

- They are simple and robust
- They have a high detection rate

Unfortunately, these methods have also some drawbacks such:

- They cannot detect unknown attacks
- These methods may trigger some false alarms due to non-availability of attack datasets.

5.5. The FINSEC Approach: Predictive Analytics

To illustrate the importance of predictive analytics for FINSEC and the critical financial infrastructures it aims to protect, we **propose to investigate an adaptive approach based on a necessary feedback from the processing node to the data collection layer** that will be identified in the sequel:

Once the data is collected using a "Data Collector", **operations such as data filtering and normalization occur** before data storage in a specific and accessible data base. This data base will serve later to provide the necessary and required data to be analyzed in different layers before extracting a decision if an attack or an anomaly is detected.

The **data analytics is then important to decide if the CPS has anomalies or attacks and then take an action or a decision accordingly**.

The project's analytics approach are based on learning algorithms: deep learning algorithms, and on statistical approaches often combined to refine the accuracy of the obtained data model (for details on the approaches see Section 5.1-5.4 above)

The global approach in FINSEC to reach an adaptable Predictive Analytics is described in the sections below.

5.5.1. Approach

We describe the components of our architecture and propose to discuss the data collection and analysis infrastructure when considering big data issues.

Our data model or architecture for a data collection and analysis is composed by three levels given as follows:

Data Collection Level

This layer composed by a Data Collector is fed by different cyber and physical probes (Network protocols, CCTV, servers…). The Data Collector consists in collecting security event data that will be stored in data storage server or in a dedicated storage data base. This data base is updated from time to time to be used by the other two layers, and this will be described in the sequel.

Before sending data from the collector to the storage data base, the data collector is normalizing and filtering the data to facilitate the data exploitation by other components of our architecture.

Thus, the data sent from the Data Collector to this storage data base, should be secured using encryption for instance. This induce a communication latency to be considered in this operation as this can impact the performance of our architecture.

Data Pre-processing Layer

The objective of this layer is to prepare the processing of the data provided by the described storage data base. This layer is composed by various operations with the goal of preparing the data processing. One can cite feature extraction which consists in selecting the most relevant features that should be identified and then will be considered in the learning analytics of the processing Layer. For instance, an operation in the pre-processing layer consists in applying a certain number of rules. These rules can be statically defined but also can be generated dynamically and according to the objectives we would like to attend. For instance, Data CutOff operation can be applied to eliminate unnecessary data that we do not need for our analysis. At the end of these operations, the pre-processing layer is then able to send (with a given latency) the pre-processed data to the processing and analysing layer. This is detailed in the following.

Data Analysis Layer

This layer is composed of a Global Analysis Center and a Response module. We believe that this layer is relevant, thus, we propose to describe its components and we start with the “Global Analysis Center”.

The Global Analysis Center is composed of:

- **Data fusion module:** The processing layer is fed with homogeneous data from the pre-processing layer. This module merges the cybersecurity data with the physical security data provided by the different probes as mentioned earlier. There is important information and messages hidden in the data which data fusion allows us to discover. Patterns that will be discovered by the learning analytics following these operations.
- **Machine Learning algorithms**: In this module, we deploy several analytics algorithms based on machine learning. It is important to deploy and use fast algorithms to detect anomalies and attacks very quickly, nevertheless, even if some algorithms can converge slowly, but their combination with other fast approaches can lead to more efficient attacks or anomalies detection in the concerned cyber-physical system. Note that the architecture for deploying and implementing the different servers for machine learning algorithms should take into account an important element which is big-data treatment in few seconds. In fact, this is important when addressing large volumes of data containing relevant information to be depicted. Thus, a specific architecture of this module will be addressed below to better cope with big-data analysis and this can be reached

using data split and then analysed using Map-Reduce processes, or parallel servers dedicated to the analysis of data blocks, before merging the different results.

- **Coarse-grained Detection:** After the convergence of the multiple learning algorithms, the obtained results can inform us if there is a suspicious attack or that an anomaly has been detected. In case of eventual existing attacks, and to reinforce the decision of our algorithms, this module can ask the Data Collector for more data. This will be used and analysed before confirming or not the existence of attacks or anomalies in our system. The data feedback requested by the Coarse-grained module consists to adjust the accuracy of the data rate that should be used to collect different data types. Next to this, a new analysis will be run and then a decision is recommended.
- **Decision making module:** This module shows the result of the smart analysis operated by the previous modules in different steps. A decision aid is then proposed and sent to the Response Module.
- **The Response Module** has the role to show and display in different manners (send email, make an alert, provide a report, …) and an action will be taken accordingly.

In the FINSEC project, our data model and architecture have also to communicate to existing data collection and analysis systems that are customized and enhanced to FINSEC requirements in the scope of WP4 of the project. These include systems like a SIEM, a Risk Assessment Engine and an AI-based CCTV system.

For the implementation of detection and prevention algorithms, the project will be integrating tools like the Open Source H2O.ai framework[2]. This framework, already used by PayPal, can be used, based on Models, integrated with the Apache Spark[3] and the Apache Kafka[4] platforms for high performance streaming and data processing/analysis. H2O.ai will be used for the implementation of the cross-cutting predictive security functionalities of FINSEC.

5.5.2. Key Performance Indicators (KPIs)

The authors in [Ullah 2018] present a systematic review aimed at identifying the most frequently reported quality attributes and architectural tactics for big data security analytic systems. Their findings are twofold: (i) identification of most frequently reported quality attributes and the justification for their significance for big data cybersecurity analytic systems; and (ii) identification and codification of architectural tactics for addressing the quality attributes that are commonly associated with big data cybersecurity analytic systems. The identified tactics include six performance tactics, four accuracy tactics, two scalability tactics, three reliability tactics, and one security and usability tactic each. The most important quality attributes for cyber security analytic systems (big data cybersecurity analytic systems) are as follows [Ullah 2018] and after establishing a FINSEC predictive analytics architecture, it is important to discuss its reliability according to different KPIs as indicated in the following:

- ***Performance*** *i*s a measure of how quickly a system responds to user inputs or other events
- ***Accuracy*** is a measure to which a system provides the right results with the necessary degree of precision
- ***Scalability*** is a measure of how easily a system can grow to handle more user requests, transactions, servers, or other extensions
- ***Reliability*** is a measure of how long a system runs before experiencing a failure

[2] https://www.h2o.ai/products/h2o/
[3] https://spark.apache.org/
[4] https://kafka.apache.org/

- ***Usability*** is a measure of how easy it is for people to learn, remember, and use a system
- ***Interoperability*** is a measure of how easily a system can interconnect and exchange data with other systems or components
- ***Adaptability*** is a measure of how easily a system adapts itself to different specified environments using only its own functionality
- ***Modifiability*** is a measure of how easy it is to maintain, change, enhance, and restructure a system
- ***Generality*** is a measure of the range of attacks covered by a security analytic system
- ***Privacy assurance*** is the measure of the ability of a system to carry out its business according to defined privacy policies to help users trust the system
- ***Security*** is the measure of how well a system protects itself and its data from unauthorized access. "Privacy preservation is not an option. Another big issue that current network monitoring practice needs to address is the compliancy with current legislation in terms of privacy preservation" [Blefari-Melazzi 2011]
- ***Stealthiness*** is the measure of the ability of a security analytic system to function without being detected by an attacker

These quality attributes also provide the Key Performance Indicators and help to determine some of the architectural and algorithmic decisions that are made.

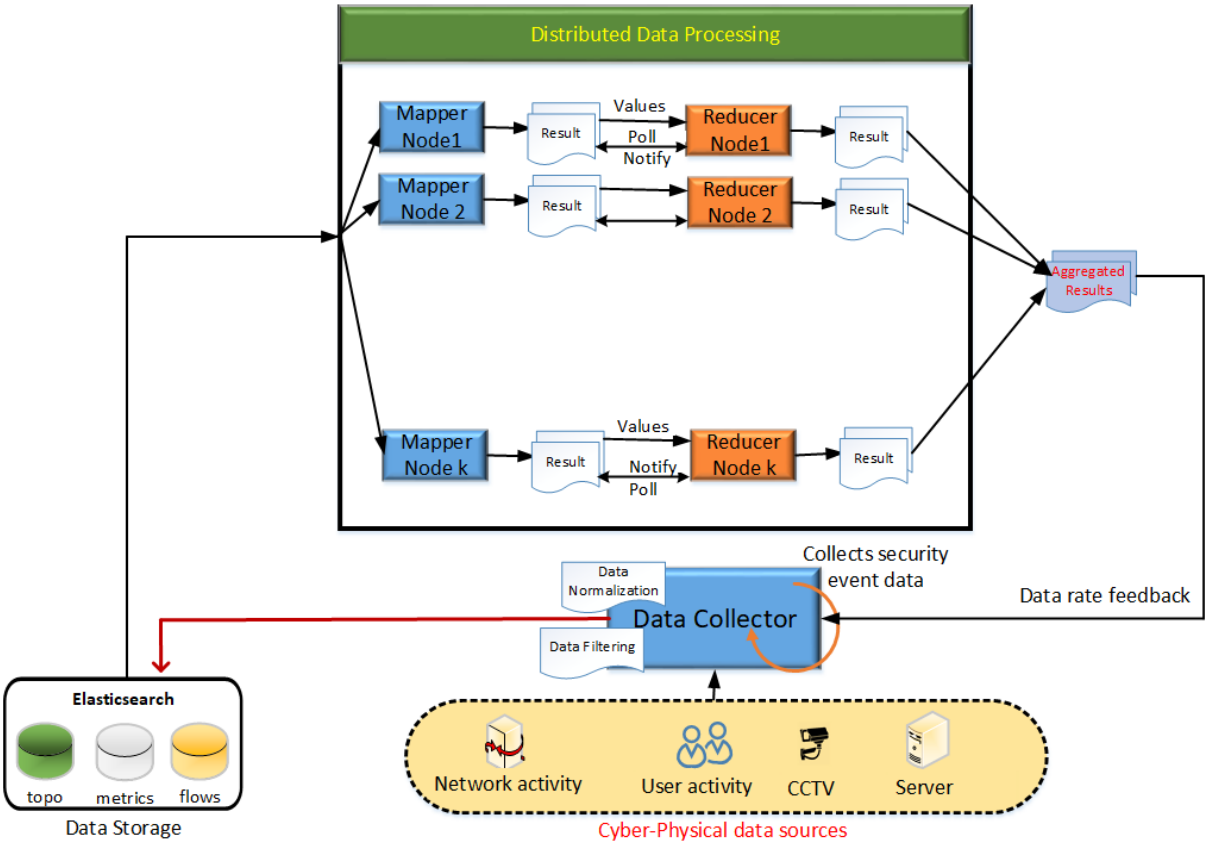

Figure 9 Data Collection and Analysis: Big Data processing

We will here further discuss some of the KPIs such as performance and scalability. Indeed, the mapping and the deployment of the predictive analysis architecture is subject to some latency, bandwidth and storage constraints. Some layers, (pre-defined above), are expecting very weak latencies and must be

deployed on the fog or the in edge of the CPS. Otherwise, the data collection architecture will suffer from performance, scalability, etc.

Figure 9 proposes a schema to address big data analysis guaranteeing the scalability of the proposed architecture. Indeed, a Big Data processing based on result polling operations is proposed and consists in replicating the nodes/servers to process the data fed by the Data Collector as illustrated by Figure 9. The Distributed Data Processing consists of Mappers and Reducers that depend on the number of available nodes already deployed in a cluster. The mapper read the data in parallel and produce intermediate key-value pairs shown as the result in Figure 9. When all the map jobs are completed, the key-value pairs are passed to the reducers. The reducers merge the various values to produce the final results.

In the following figure one may observe how scalability, reliability, accuracy, security, privacy, etc. quality attributes are addressed in the adaptive multi-layer data collection module.

6. Data Collection and Security Probes

6.1. Data Collection

Collecting security related data, which indicates relevance to security, safety, privacy and trust, in the big data era poses challenges due to its 5Vs (volume, variety, value, velocity and veracity) characteristics. Further the 5G networks' characteristics of being heterogeneous, supporting device-to-device, machine-to-machine and other communication technologies, and different networks such as Internet, Mobile Ad hoc Networks, mobile cellular networks and wireless sensor networks make data collection difficult [Lin 2018]. Security related data fundamentally affects the efficiency and accuracy of detection methods. Jing et al. [Jing 2018] survey existing studies about security-related data collection and analytics for measuring the Internet security. They argue that for measuring the security of the internet and detecting the Internet attacks, collecting different categories of data and employing methods of data analytics are essential. They divide the data related to network security measurement into four categories: packet-level data, flow-level data, connection-level data, and host-level data:

1. Packet-level Data includes packet header information, packet payload information, and packet activity information. **Collection Method** - packet capture (pcap), Libpcap and Winpcap, TCPdump, Wireshark, Snort, Nmap, libtrace. **Classification**: Source/Destination IP address, Source/Destination port, Time to Live, Timestamp, Packet payload, Packet size, Protocol (TCP/UDP).

2. Flow-level Data: includes a stream of packets that have one or more same attributes. These same attributes, usually called flow keys, commonly include packet header information, packet contents and meta-information. **Collection Method**: There are two flow collection strategies: (i) depth-first, choosing specific flow keys to aggregate packets in order to meet collection demands, (ii) breadth-first, collecting as much as possible information in order to have a global view on network traffic. **Classification**: Flow-level data represents the statistical information of a flow and can be classified into the following types: flow count, flow type, flow size, flow direction, flow duration, flow rate

3. Connection-level Data: describes the traffic statistical information (includes inbound traffic and outbound traffic) exchanged between two IP addresses. The authors argue that it has a higher granularity of network traffic than the flow-level data because it provides global information of exchanged traffic between two IP addresses in a given time. **Collection method**: The collection method of connection-level data is actually the process of collecting packet-level or flow-level data. **Classification**: The connection-level data can be classified into connection size, connection duration, connection count, connection type.

4. Host-level Data: describes the data collected from a local host and can describe any internal changes in the host. Collection Method: Various open-source tools can be used to collect host-level data, such as Collectl and Loadrunner in Linux and Windows, respectively. Classification: host-level data can be classified as CPU and memory usage, and operation logs. Operation logs can further be classified into equipment operation logs and application operation logs. The equipment operation logs collect the running events of equipment that connects with host, such as keyboard and mouse click events, cursor changes, writable objects, etc. The application operation logs represent user-related activities when using a specific application, e.g., local port creations or destruction events, the number of login events, software usage events, system calls, etc.

A number of surveys of data collection approaches exist. Just to mention a few: improving data comprehension for digital security and forensics [Erbacher 2008], security data collection and data analytics in the Internet [Jing 2018], network data collection [Zhou 2018], network security-related data collection technologies [Lin 2018], data fusion for network intrusion detection [Li 2018], data collection for attack detection and security measurement [Liu 2018], security data collection and analysis for LTE/LTE-A network security measurement [He 2018]. In their survey [Lin 2018], the authors specify 13 functional requirements and 5 security requirements, and 9 functional objectives and 6 security objectives, and the relationship between these. They also defined a taxonomy of network data collection technologies based on literature reviews:

Collection nodes:

- Distributed collection – can collect multiple types of data to comprehensively understand the status of an entire network system.
- Centralized collection – can facilitate the management and coordination of collection nodes.
- External collection - can only collect external communication data.
- Internal collection - can collect the communication data inside a system.

In a network system, common data collecting nodes include routers, switches, gateways, IDSs/IPSs, firewalls, honeypots, sensors, proxy servers/collecting servers, agents, mobile terminals (including smartphones, tablets and wearable smart devices), and distributed collection nodes.

Collection tools:

- SW (Software) collection (Libpcap, improved libpcap, improved Driver and Network Stack, simulation SW) such as SDN (Software Defined Network) or NS3 –(Network system simulation software)
- HW (Hardware) collection (Sensor, HW probe, DAG Cards, Port Mirroring, Inline taps, Network Interface card, Mobile Terminal, IDS/IPS, Firewall, Proxy Server, Agent, Honeypot)
- Protocol collection (SNMP, Telnet, IPFIX, NetFlow)
- Offline collection: collects data offline, does not use much network resources and has low real-time performance.
- Online collection: collects data online and has a high real-time performance but could burden the network system.
- Direct collection: can collect many types of data with high accuracy but could overload the system.
- Indirect collection: relies on existing data; it has low accuracy but high performance.
- Passive collection: uses sniffers to implement network data collection through centralised management.
- Active collection: injects test traffic into normal network traffic for network quality measurements; the quality of networking can be judged and evaluated according to the response of the network.

Collection mechanisms

- Full collection - active traffic collection, linear scaling based with multiple HW devices, locality buffering based, distributed data collection
- Partial collection - Traffic prediction based, sampling-based, traffic similarity based, adaptive data collection, rule-based, load balancing based, flow based, stream-oriented
- Packet-oriented collection - collects data in the form of data packets
- Flow-oriented collection – collects flow information

Lin et al. [Lin 2018) suggest four steps to design a complete data collection solution in a traditional network system:

- determining the data that needs to be collected, that is, collection target.
- determining the location of data collection, that is, collection node.
- deciding which devices or tools to use for data collection, that is, collection tool.
- designing an adjustment algorithm or mechanism according to the requirements of the data collection, that is, collection mechanism. They argue that collection mechanism is the heart of a data collection solution, data collection mechanisms need to adjust data collection process to increase the collection efficiency and reduce the burden on the network system.

The authors [Lin 2018] introduce three traditional statistical sampling algorithms and two proposed adaptive sampling algorithms to adjust collection frequency in order to improve collection efficiency and reduce the amount of collected data. Collection frequency adjustment strategies generally have three trigger modes: count trigger (i.e., counters), timing trigger (i.e., timers), and event trigger. Statistical sampling algorithms include [Lin 2018):

- Simple random sampling generates a random number N before collecting one data and compare it with a threshold set in advance. If the random number is smaller than the threshold, the next data is collected; otherwise, the next data is not collected. The choice of threshold determines the collection frequency.
- Systematic sampling. Data collection based on systematic sampling is relatively simple. We only need to set a fixed period length T in advance, and then the collector collects data at a fixed collection frequency
- Poisson sampling is recommended by Internet Engineering Task Force (IETF) RFC 2330 for network data collection in IP network measurement and is based on Poisson distribution.

6.2. Data collection levels, sources and aggregation

Data Collection Levels. Classical data collection is achieved at several levels at endpoint (first level), data collector (second level) and data collector/aggregator (third level). The access methods at the endpoint include standard interfaces (e.g. SNMP MIB), remote login (e.g. Telnet, RDP), agent (e.g., antivirus, patch management, or dedicated SACM agent), etc. At the first and second levels of collectors, the data collection methods include periodic data pull, periodic data push and event-driven data push. Data collection levels are also referred to as statistics levels whose variation affect storage and system requirements[5].

Data Collection Sources. Current data sources from which security event data are collected include, but are not limited to, network traffic data, firewall logs, web logs, system logs, router access logs, database access logs, and application logs, system statistics, [Erbacher 2008]:

- ***Network traffic data*** – include typical packet information and/or network flows.
- ***System log files*** – include snort alert logs, message logs, security logs, email logs, router logs, web logs, database logs, etc. Identification of contrasts between system log files and network traffic data is one mechanism for rapidly identifying intrusions or otherwise anomalous activity.
- ***Firewall logs*** – include details related to blocked and accepted activity and are important as initial indicators of attacks and aid in fine-tuning of the firewall itself.

[5] https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vcenterhost.doc/GUID-25800DE4-68E5-41CC-82D9-8811E27924BC.html

- ***System statistics*** – provide information such as system load, disk usage, etc. and can rapidly identify anomalous usage of a system.
- ***Router logs and transmittal statistics*** – include connectivity and statistics on data transmission. This data can be useful for identification of network health, network misuse, worm spread, etc.
- ***Process accounting logs*** – identify the processes or commands a user has executed. This is often useful for the identification of insider threats.
- ***Library function accounting logs*** – monitoring the functions that a process executes aids identification of the real purpose or functionality of a process.
- ***Biometric data*** – include data collected as to users' behavioral patterns in the use of the computer hardware; the keyboard and mouse for instance and attempt to ensure the validity of the systems physical security.
- ***IDS alerts*** – provide value in terms of identifying anomalous activities.

Data Aggregation. In order to reduce the overhead and achieve efficient data collection, data must be aggregated and collated. This will make the operation of FINSEC systems both resource effective and cost effective, through economizing on bandwidth and probe data access operations. This resource and cost-efficiency can be extremely important when offering FINSEC based on the SECaaS (Security as a Service) modality involving access to public cloud resources. Two main aspects of solving data aggregation issues are discussed in the literature. Some focus on the manner of routing the aggregable messages along farther distance in order to improve the aggregation ratio (data collection). Others concentrate on expressing data to be aggregated differently by using compressing and merging methods to reduce the overhead. [Soua 2013] focuses on how to route the aggregable packets to a specific destination node in order to improve the data collection ratio. To achieve this, an adaptive data collection protocol using reinforcement learning for VANETs (Vehicular ad hoc networks) is proposed, based on a distributed Qlearning technique making the collecting operation more adaptive to nodes mobility and topology changes, and using a reward function to take into account the delay and the number of aggregable packets. The use of the VANETs techniques in FINSEC is driven by their ability to deal with highly dynamic and volatile environments (e.g., environments where sensors joint and leave dynamically), which is in-line with FINSEC's dynamic nature.

6.3.Adaptive Data Collection

Adaptive data collection refers to the collection of security related data to improve collection efficiency, ensure collection accuracy, reduce the amount of collected data to minimize the effect of data collection, and automate the data collection by adjusting to different environmental contexts and situations. Several authors address adaptive data collection in different settings. Lin et al. [Lin 2019] present the design and implementation of an adaptive security-related data collector based on network context in heterogeneous networks. They argue that sampling methods to collect data, and the collection frequency need to be determined according to specific conditions. For instance, if the data variation is large, the collection interval should be reduced so as to reflect the variation trend of data and if the data variation is small, the collection interval can be increased, so as to reduce the amount of data collected while ensuring the accuracy of data collection. They propose an Adaptive Collection Frequency Adjustment Strategy Based on Predicted Variation Ratio (ACFAS_PVR). They argue that regression algorithms can be used for prediction, such as linear regression, Support Vector Regression (SVR), logistic regression, KNN regression, etc. and data variation can also be represented by calculating the ratio of predicted accuracy, which is the ratio of the predicted value of the data to the real value of the data. It indicates data variation as follows: When the predicted value of the data is close to the real value, it indicates that the data variation is small, and when the predicted value of the data is very different from the real value, the data variation is large [Lin 2019]. In authors' model,

the issue of heterogeneity of network system is solved by a Security-related Data Description Language (SDDL) to instruct security related data collection in various networking contexts, and adaptive sampling algorithms is used to reduce the amount of collected data.

Habib et al. [Habib2016] investigated self-adaptive data collection and fusion for health monitoring based on body sensor networks. Their approach uses an early warning score system to optimize data transmission and estimates in real time the sensing frequency and uses a data fusion model on the coordinator level using a decision matrix and fuzzy set theory. Their adaptive sampling algorithm adapts the sampling rates of sensors to the vital sign dynamic evolution. An Adaptive Data Collection protocol was proposed in [Al-Qurabat 2017], which collects periodically sensor readings and prolong the lifetime of a Periodic Sensor Network (PSN). Authors' sampling rate adaptation is based on the similarity between periods of cycles using Euclidean distance measure to adapt its rate of sampling according to the dynamic modification of the monitored environment. An efficient adaptive sampling approach based on the dependence of conditional variance on measurements varies over time was proposed in [Laiymani 2013]. Other works (e.g., [Kemal 2016]) present adaptive data collection mechanisms for smart monitoring of critical infrastructures (e.g., electrical distribution grids with adaptive smart metering infrastructures). Three main aspects of adaptiveness of the system are studied, adaptiveness to smart metering application needs, adaptiveness to changing communication network dynamics and adaptiveness to security attacks.

Ji and NI [Ji 2009] present an adaptive data collection method based on the network data correlation and variation routines. Their method selects the data collection content in association with network data variation and adjusts collection frequency based on the ratio of the data variation amplitude. In this way the method can adjust data collect content according to network/server load value and decrease collect amount while achieving the same network management tasks as static collection, and then reduce the burden on network bandwidth and processing resources. The frequency adjustment strategy can reduce data collection times when the data vary gently and increase data collection times when data vary dramatically. Tang and Xu [Tang 2008] investigate data collection strategies in lifetime-constrained wireless sensor networks. Their objective is to maximize the accuracy of data collected.

As demonstrated above there exist many adaptive data collection methods using different strategies. However, few of them are aimed at adaptive multi-layer data collection combining physical and cybersecurity information from different probes, yet in the same business context.

6.4.Security Probes

Security probes are created to capture and assess the overall security of servers, networks, databases, etc and to generate events when they find problems[6], and have the following abilities:

Topology probes: Ability to capture network topology, interface, bridge, namespace attributes.

- ethtool – a utility for Linux kernel-based operating system for displaying and modifying some parameters of network interface controllers (NICs) and their device drivers.
- Network system simulation software – this includes Software-Defined Network (SDN) or similar software to simulate the real network functions. An example is the Open vSwitch Database (OVSDB) management protocol.
- Simple Network Management Protocol (SNMP) – an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

[6] https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_9.0.1/admin/admn_securityprobes_c.html

- Telnet – protocol to provide a bidirectional interactive text-oriented communication facility, which can be used to connect to network equipment and extract management data.
- Network Interface Filtering Card (NIFIC) – a hardware-based probe that can be remotely configured to focus in more detail on selected traffic and/or filter out malicious forms.

Flow probes: ability to follow a flow along a path in the topology.

- sFlow ("sampled flow") – an industry standard for packet export at Layer 2 of the OSI model.
- Data Plane Development Kit (DPDK) – a set of data plane libraries and network interface controller drivers for fast packet processing, currently managed as an open-source project under the Linux Foundation.
- libpcap – commonly used packet capture library, which also defines the de facto external format for packets.
- sCap -- a more efficient implementation of the standard libpcap, using shared memory and so-called subzero packet copy.
- Internet Protocol Flow Information Export (IPFIX) – a protocol for exporting Internet Protocol flow information from routers, probes and other devices.
- NetFlow – a feature of Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface.
- Flowmon probe – a hardware-based probe that uses IPFIX protocol

For example, Skydive (http://skydive.network/) is an open source real-time network topology and protocols analyzer providing agents that act as data collectors, employing efficient mechanisms to control the granularity of data collected and collection intrusiveness, in terms of CPU, memory and network overheads. These mechanisms allow for extra flexibility in capturing network topology and network flows data, as compared to other existing methods. The challenge of efficiency is to get access to collect data with minimal disturbance to the production workloads that are sharing the same system resources. This includes memory and CPU but also the network itself that is shared in some level between the monitoring and data acquisition tooling and the production workloads. In addition to the common methods, sFlow, netFlow, pcap etc, we are utilizing a modern advanced networking infrastructure for Host level capturing known as bpf[7] and eBPF. Those capturing methods make use of Linux Kernel and outperform legacy captured in most scenarios. With ebpf/bpf capturing it is possible on one hand to limit and slice the networking data captured to some defined value, and even to change dynamically the capture to fit to on-going security demands and on the other hand allow much more efficient capturing that required significant less CPU and Memory. All this optimization will be achieved thorough configuring and re-configuring of the frequency of data collection based on different adaptive strategies. This will be achieved using the probe configuration data model described in Section 3.2.

6.5.The FINSEC Adaptive Multi-layer Data Collection Approach

To secure financial critical infrastructures and services security related data must be collected and analyzed in an intelligent, resilient, reliable, secure and timely manner fulfilling all the communication requirements and standards to detect attacks.

To achieve this the FINSEC approach includes the design and deployment of the concept of adaptive multi-layer data collection by adapting different approaches. FINSEC will integrate smart security probes and a set of adaptive strategies for the multi-layer data collection functionality, which

[7] https://en.wikipedia.org/wiki/Berkeley_Packet_Filter

includes how to render adaptiveness and intelligence, optimize bandwidth and storage of security information, and boost the intelligence of the project's probes by ensuring adaptive multi-layer data collection. Security data analytics methods described in section 5 will be integrated at appropriate level specific analytics. Predictive/regression algorithms such as linear regression, Support Vector Regression (SVR), logistic regression, KNN regression will be investigated for the lightweight analysis of adaptive strategies. Deep learning mechanisms will be used for the identification of complex risk and attack patterns. A set of rules (both static and adaptive) will be defined for processing, analyzing, configuration, collection, and adaptation.

In terms of the FINSEC architecture, we specifically designed our solution to achieve most of the quality attributes described in section 5.7.2. For example, we use a cloud-based architecture that supports scalability by design and by implementation (see also FINSEC Deliverable D2.4) and we address the issue of false positives to ensure reliability and accuracy.

The detection capability can be greatly improved by correlating a wide-range of data sources and by multi-layer data collection and analytics. IBM implements multi-layer data collection & analytics using Skydive (see Figure 10) for topology view exploration as shown in the following figures. Skydive is an open source real-time network topology and protocols analyzer providing a comprehensive way of understanding what is happening in your network infrastructure[8].

As described above Skydive agents act as data collectors, allowing for extra flexibility in capturing network topology and network flows data, as compared to other existing methods. At the same time, they enable capturing rich sets of metadata attributes from network entities, both in the physical and in the virtual domains.

Skydive architecture allows to capture information in various locations of the infrastructure, both horizontally (network entities, e.g. interfaces, switches etc., on the same layer of the stack) and vertically (network entities on multiple layers of the stack, e.g. application layer, virtual networking layer, physical networking layer, etc.). Having data collected with flexible granularity on the one hand and with high redundancy on the other allows us to correlate information between locations and layers and to use various algorithms to produce insights.

[8] http://skydive.network/]

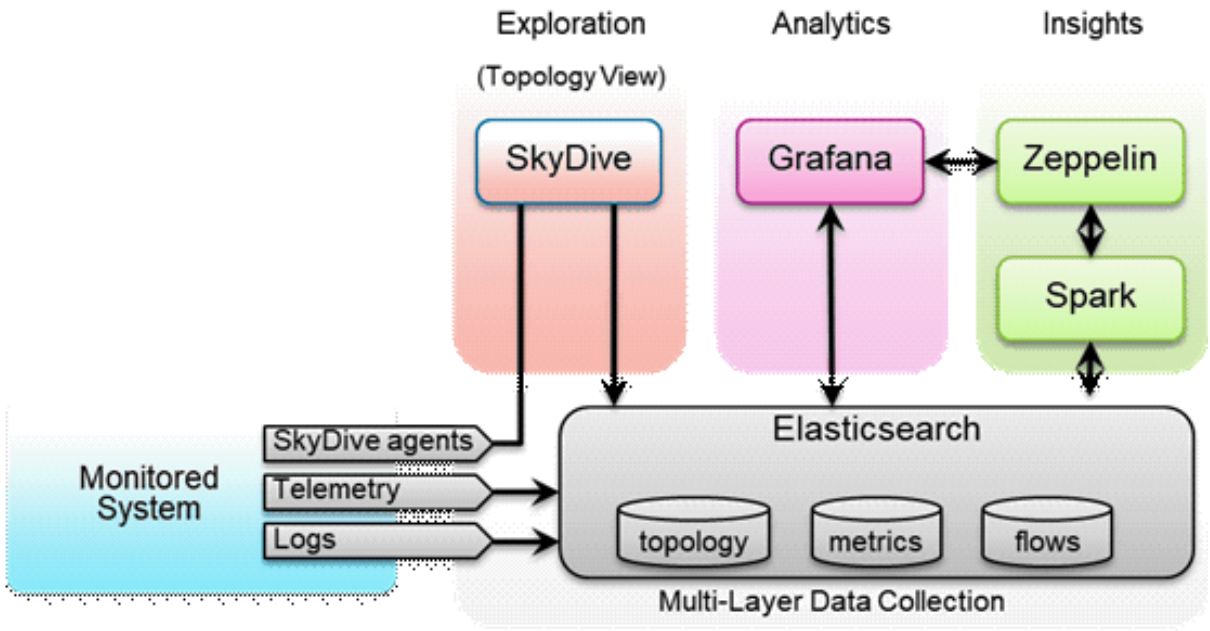

Figure 10: IBM multi-layer data collection and analytics

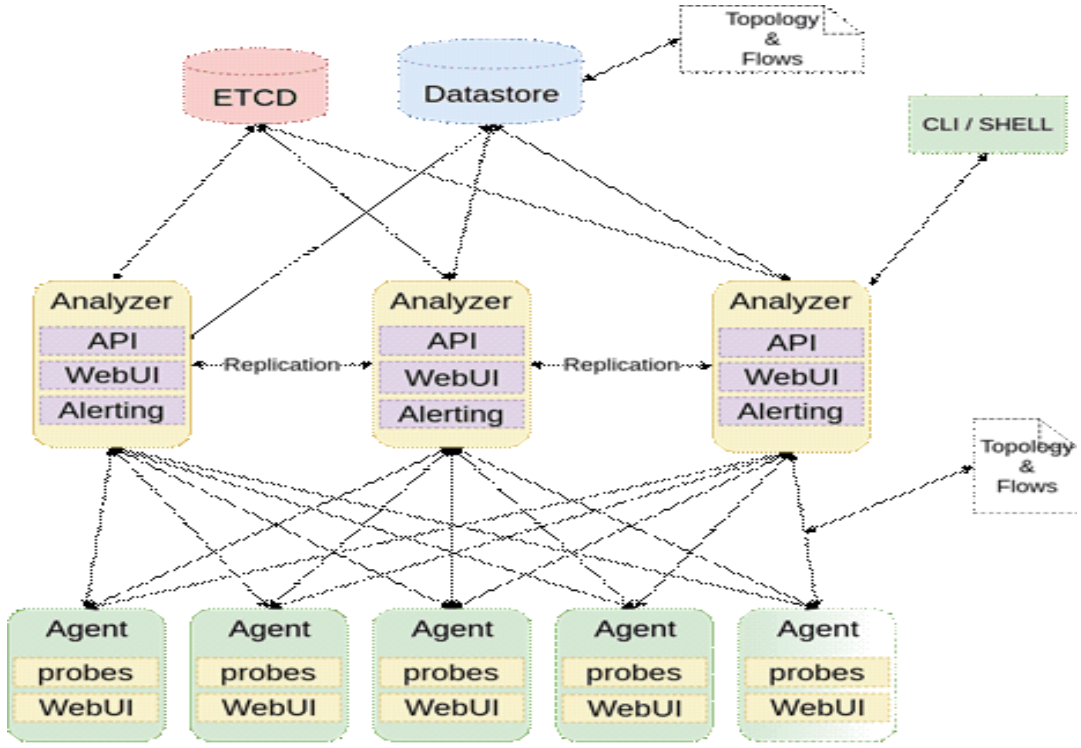

Figure 11: Skydive Network Documentation (Source: http://skydive.network/documentation/)

The architectures shown above do not depict the notion of adaptivity, adapting to levels, collection and detection strategies and automation. To fill this gap **FINSEC has designed adaptive multi-layer data collection and analysis by extending the classical data collection and analytics process which include data collection, data parse, data analysis and data processing. The FINSEC approach makes this process adaptive by introducing feedback control phase and letting the data collection depends**

on the result of the last data process as shown in Figure 12. The process modules include data collector (Monitor), data parser & analyzer (Analyzer), and data processor (Adapter). The arrow between modules is data flow and control direction. The Monitor instruct the multi-layer probe skydive to collect data. The multi-layer skydive collect data from cyber and physical assets at different levels (individual asset, combined assets, integrated process, and supply chain) and store the data and notify the Monitor module. The Monitor module inputs the data to the Analyzer module. The Analyzer module transforms the raw data to standard data in accordance with data model defined in the project and converts the standard data to service data (threats, anomalies, attacks, etc.) and pass this to the Adapter module. The Adapter module disposes the service data depending its value such as adapt collection strategies and control the Monitor module, send notification to external modules such as alarms and/or send data to visualization tool or database. In this way, automated adaptive multi-layer data collection with optimized bandwidth and storage of security information is achieved using adaptive collection strategies such as security threats, content variation, collection/sampling rate, bandwidth variation/communication dynamics, application needs, context changes, and storage needs. In the first phase only the security threats and collection rate strategies will be implemented. The privacy and security of the collected data will be achieved using the FINSEC vertical AAA Application security and encryption.

A FINSEC Data Collection API will be provided to facilitate interactions with the other FINSEC services. For example, interface to user application such as DB, Display, Alert/notification, configuration/re-configuration of probes, etc. will be provided through this API.

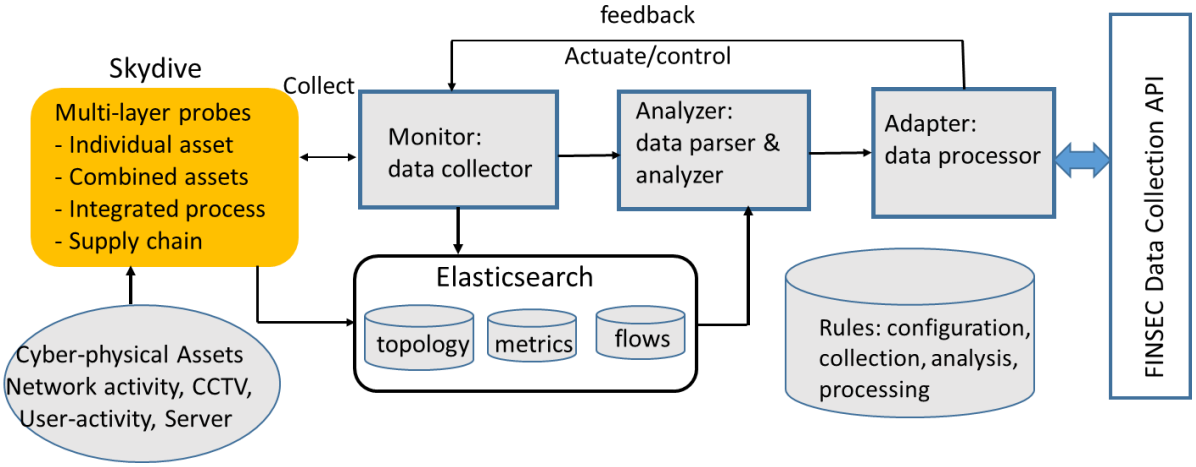

Figure 12 Adaptive Multi-layer Data Collection Module in FINSEC

7. Security Knowledge Base

7.1. OWASP Security Knowledge Framework

The OWASP Security Knowledge Framework (SKF) is intended to be a tool that is used as a guide for building and verifying secure software. It can also be used to train developers about application security. Education is the first step in the *Secure Software Development Lifecycle*.

The *OWASP Security Knowledge Framework* is an expert system web-application that uses the OWASP Application Security Verification Standard and other resources. It can be used to support developers in pre-development (security by design) as well as after code is released (OWASP ASVS Level 1-3).

7.2. The FINSEC Security Knowledge Base

The Security Knowledge Base is a module based on threat intelligence information concerning both the cyber and physical assets typical for infrastructures of the financial sector. That information will be collected from various publicly available sources of threat intelligence information, such as CVE (Common Vulnerabilities and Exposures) databases (nvd.nist.gov, cve.mitre.org, cvedetails.com), CAPEC (Common Attack Pattern Enumeration and Classification) patterns from MITRE (capec.mitre.org) and existing OVAL specifications.

The structure of the Security Knowledge Base will be predicated on the definition of the different physical and cyber assets (such as cloud infrastructures, data centers, devices, blockchains, buildings, networking infrastructures) and their interactions as part of the critical infrastructures. Moreover, the Knowledge Base will be enriched with known and newly identified attack patterns against these specific assets.

In order to promote homogeneity and integrity among the FINSEC services, all the information composing the Security Knowledge Base will be represented through the FINSEC REFERENCE DATA MODEL. Before being stored, all the information incoming from external sources will be translated by the FINSEC connectors into the FINSEC REFERENCE DATA MODEL.

The Security Knowledge Base will expose REST API to enable interactions with the other FINSEC services. In addition to being integrated into the wider FINSEC tool set, it will be accessible and browsable through a visual interface included in the FINSEC DASHBOARD.

8. Collaborative Approach

8.1. Overview

A principle innovation of the FINSEC security approach lies in the support provided for the collaborative tackling of security issues in the financial services supply chain. In particular, FINSEC plans to support collaborative security processes based on proper and timely sharing of information across supply chain participants. As a prominent example, stakeholders can collaborate in joint risk assessments, over shared information. Collaborative security processes are likely to be more effective, given that they enable stakeholders to assess risks based on a richer set of information, while at the same time enabling them to view the same problem (e.g., security incidents) from multiple perspectives.

By exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that community to gain a more complete understanding of the threats each organization may face. Using this knowledge, organizations can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analysing cyber threat information from multiple sources, organizations can also enrich existing information to make it more actionable. This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information through the reduction of ambiguity and errors. Organizations that receive threat information and subsequently use it to remediate a threat confer a degree of protection to other organizations by impeding the threat's ability to spread. Additionally, sharing of cyber threat information allows organizations to better detect campaigns that target industry sectors and sector generic systems and services.

The collaborative nature of the FINSEC approach is orthogonal to the integration and prediction dimensions that are analysed elsewhere in the present deliverable. Hence, collaborative processes in FINSEC should be executed based on the sharing of integrated security information about both cyber and physical assets. Likewise, predictive analytics can be applied both for collaborative processes and for processes that concern a single financial organization rather than a value chain of organizations.

The FINSEC collaborative approach will be enabled by the following elements and building blocks:

- **Information Sharing framework,** which shall provide the means for sharing security information across different stakeholders of the financial supply chain.
- **Common Integrated Data Modelling** as a prerequisite for interoperability across the wide array of security systems and information models of the individual supply chain participants.
- **Shared Situation Awareness** for physical processes, which shall allow supply chain participants to have the same understanding about the context of physical security processes.
- **Common Reporting and Visualization**, as a tool for facilitating stakeholders' collaboration.

8.2. Information Sharing

8.2.1. Information Sharing Specifications for Security Information

The increasing exchange of cybersecurity information, and more specifically threat intelligence, to support the process of cyber-attack countering and managing vulnerabilities and threats, is a trend that is extending. Many factors contributed to this trend beyond the known benefits that sharing high

quality information among trusted peers has to improving accuracy of detection, obtaining an efficient and faster response and foster preparedness through collective learning.

The development of standards and protocols that facilitate the automated exchange (e.g. OpenIOC, CybOX, IODEF, STIX or TAXII and RID protocols), and the efforts of CERTs, ISACs and other initiatives (e.g. ENISA, NIST) to promote their use are two key factors. Another critical factor is the existence of threat intelligence platforms that facilitate the exchange of information, in some cases by exploiting the standards and protocols already in use by many CERTs/CSIRTs across the EU.

C. Sauerwein et al.[9] reviewed the state-of-the-art software vendor landscape of Threat Intelligence Sharing Platforms (TISP), comparing 22 platforms, identify key findings and discussing gaps and research challenges for the future.

One of the most significant findings is that there is no common understanding on what is a TISP. Consequently, among the platforms analysed, only 8 allow the sharing of threat intelligence. Many platforms allow the sharing of security information or aggregated data but not intelligence as such. Others only focus on sharing technical data (e.g. SNORT rules, malware hashes) or simply are central repositories of security relevant information (e.g. information related to malware).

International in scope and free for public use, TAXII, STIX and CybOX are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defence and sophisticated threat analysis.

TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organizational, product line and service boundaries. TAXII is not an information sharing program itself and does not define trust agreements, governance, or other non-technical aspects of collaboration. Instead, TAXII empowers organizations to share the information they choose with the partners they choose.

STIX builds upon standards (CybOX) and permits embedding IODEF, OpenIOC, XML namespaces (e.g. MITRE, CAPEC, MAEC, ATT&CK), extensions for rules (YARA, SNORT) and non-XML bindings using JSON for example. STIX architecture is very modular, composed of eight core cyber threat concepts: Campaigns, Indicators, Observables (e.g. IP addresses, file names, hashes), TTP (Tactics, Techniques and Procedures-; including attack patterns, kill chains, etc.), Incidents, Threat Actors, Exploit Targets (e.g. vulnerabilities, weaknesses) and Courses of Action (e.g., incident response, mitigation strategies). STIX allows binding together a diverse set of cyber threat information into a structured common data format that can be correlated and further analysed. This data can be collected, aggregated and then normalized into a structured data feed that can be enriched and analysed to become Threat Intelligence, ready for injection into SIEMs for further processing and analysis.[10]

8.2.2. FS-ISAC

FS-ISAC, or the Financial Services Information Sharing and Analysis Center, is the global financial industry's go-to resource for cyber and physical threat intelligence analysis and sharing. Constantly gathering reliable and timely information from financial services providers, commercial security firms,

[9] Clemens Sauerwein, Christian Sillaber, Andrea Mussmann, Ruth Breu, "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives". Wirtschaftsinformatik 2017.

[10] Ref: *The Homeland Security (HS) System Engineering and Development Institute (SEDI), operated by the MITRE Corporation serves as the moderator of the STIX, TAXII and CybOX communities on behalf of the Department of Homeland Security.* https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

federal/national, state and local government agencies, law enforcement and other trusted sources, FS-ISAC can quickly disseminate physical and cyber threat alerts and other critical information to its members. This information includes analysis and recommended solutions from leading industry experts. FS-ISAC is currently active with members and partners across countries and regions throughout North and South America, Europe, the Middle East and Asia/Pacific. The Critical Infrastructure Notification System (CINS) allows FS-ISAC to speed security alerts to multiple recipients around the globe near-simultaneously while providing for user authentication and delivery confirmation.

FS-ISAC also provides an anonymous information sharing capability across the entire financial services industry. Upon receiving a submission, industry experts verify and analyze the threat and identify any recommended solutions before alerting FS-ISAC members. This assures that member firms receive the latest tried-and-true procedures and best practices for guarding against known and emerging security threats.

8.2.3. NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing

The NIST Special Publication 800-150, provides guidance to help organizations exchange cyber threat information. The guidance addresses sharing of cyber threat information within an organization, using cyber threat information received from external sources, and producing cyber threat information that can be shared with externally.

8.3.Interoperability Framework

8.3.1. Centralised Approach: Shared Database

State of the art efforts for sharing security information are generally through a common database, which is accessible by all stakeholders, and structured based on a common agreed and in most cases a standards-based data model. This is the approach followed by projects such as CIPSEC.

A shared database approach offers simplicity and a straightforward model for sharing information across stakeholders. However, it also imposes the need for a trusted third party (TTP) in charge of managing and maintaining the database in a trustworthy manner. The TTP should cater for securing the shared database against adversaries or malicious parties that would like to change information for their own interests.

Despite the deployment and use of leading edge security technologies and relevant processes, experience shows that centralized systems are vulnerable. The most recent example is the notorious Cambridge Analytica case, where over than 87 million Facebook profiles were compromised[11].

8.3.2. De-Centralised Approach: Blockchain

The rise of distributed ledger technologies (i.e. blockchains [Babich16]) provides an alternative decentralized way for sharing data, which does not rely in a TTP. As such it can be appropriate for sharing security data across different stakeholders of the financial services supply chain. Furthermore, a blockchain approach offers several some additional advantages such as anti-tampering capabilities and transparency in the information sharing process. Note also that the rise of permissioned blockchains (such as the Hyperledger Fabric [Androulaki18] and the Corda

[11] https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

[Brown16] blockchains), alleviate some of the shortcomings of public blockchains for enterprise use and make a blockchain approach more viable and more compelling for use as part of the FINSEC platform.

8.4. Relevant Projects

Several projects (including EC funded projects) have designed and implemented solutions for sharing security information across different administrative entities. The type of informaiton shared and the semantics of the information may differ from FINSEC. However, all these projects provide insights about how an information sharing system can be implemented. A discussion of some representative project follows in the same paragraphs.

The CIP-PSP ACDC project (Advanced Cyber Defence Centre)[12] aimed at deploying an infrastructure of interconnected support centres (including CERTs, CSIRTs) across European Member States linked to a central ACDC clearing house, to provide solutions to users to fight botnets. This central data clearing house (CCH) is the central data storage repository, designed to provide open standards and a wide flexibility in supporting data formats[13]. After an analysis of relevant data formats (binary and textual), the agreement across project participants was to use JSON and implement a basic standardisation of the submitted data fields, called an ACDC Schemata, in order to simplify the submission and retrieval of information by peers in the identified use cases[14]. The CCH provided a REST API that permitted submitting data to registered entities only (in possession of so-called write keys). Data sharing is done in ACDC through XMPP server governed by data sharing policies based on previously established trust relationships between members of the Community. Other project-specific solutions provided some (limited) support to standard data formats, e.g. FP7-ICT MASSIF project[15] offered features to export information using IDMEF.

FP7 NECOMA project[16], a Nippon-European collaboration for improved resilience against cyber threats, focused on data collection, threat data analysis, and development of new cyber defence mechanisms. NECOMA designed an architecture with components for threat information sharing, threat information exploitation, data analysis and distributed data storage to incorporate different datasets in a secure way[17]. However, due to the number and complexity of the requirements that pose many security and privacy restrictions, the project did not implement the distributed storage. Nevertheless, to implement the threat information exploitation component, the project developed the so-called NECOMAtter, a tool aimed at facilitating man-machine collaboration: human security analyst, various data sources, and network equipment. Also, NECOMA leveraged n6 network security incident exchange[18] project, developed and promoted by CERT Polska, as the main machine-to-machine interface. n6 (Network Security Incident eXchange) is a platform for acquisition, processing and exchange of information regarding Internet threats released under open source license. n6 uses an event-based data model for representation of all types of security information. Each event is

[12] ACDC Project, https://www.acdc-project.eu/

[13] ACDC Project, "D1.2.2 Specification of Tool Group "Centralised Data Clearing House", 2015. https://acdc-project.eu/wp-content/uploads/2016/05/D1.2.2_ACDC_Centralized_Data_Clearing_House-s.pdf

[14] ACDC Project, "D1.7.2 – Data Format Specification", 2015. https://acdc-project.eu/wp-content/uploads/2015/11/ACDC_D1.7.2_Data_Format.pdf

[15] MASSIF project, https://cordis.europa.eu/project/rcn/95310_en.html

[16] NECOMA project, http://www.necoma-project.eu/

[17] NECOMA project, "Deliverable D2.1: Threat Analysis ", 2014. http://www.necoma-project.eu/m/filer_public/f0/65/f0654584-6fe2-40cd-8204-4781dfc6f7a8/necoma-d21r1345-public.pdf

[18] N6, https://www.cert.pl/en/projekty/n6-network-secident-exchange/

represented as a JSON object with a set of mandatory and optional attributes. Additionally, n6 supports export data in alternative output formats: IODEF, CSV[19]. For the data analysis, relied on a hadoop-based analysis platform called MATATABI [20] serving as Data storage and Data analysis framework functionality, providing a scalable platform to analyse and detect various types of threats based on the big-data technology. NECOMA integrated n6 and MATATABI to offer an easy and intuitive API to external entities (i.e. main machine-to-machine interface). The n6 platform is used and extended in ongoing H2020 project SISSDEN[21].

DiSIEM has conducted a comparative study of CIF, CRITs, MISP and Soltra Edge considering the support offered by these platforms in terms of capabilities for importing data in different data formats (.pdf, .doc, .txt, .xls), integration with standard security tools (e.g. SIEM), support for collaboration and sharing capabilities, data exchange standards supported, analysis capabilities, graphical support provided, license and hardware requirements[22]. The result of this comparative study is that MISP is the best option for collecting and sharing data, flexible and easy to integrate with other TISP (e.g. CSIRTs) and with SIEMs but have poor in-built analysis capabilities. CIF provides very high-speed information exchange, by using technologies such as Elastic Search and Zyre (ad-hoc zeroMQ technology). On the other hand, CIF is not very flexible if you want to handle specific standards such as STIX and post-processing capabilities are limited to IoCs (Indicators of Compromise).

CRITs and Soltra Edge are centralized repositories (private or shared) of the threat intelligence that focuses more on collaborative analysis than information sharing. MISP allows for a decentralized approach, where different entities can hold their own private database and enable peer-to-peer interaction among instances if required. CRITs has better visualization support than MISP and CIF but has poor sharing and data collection capabilities, and although it is flexible so new services can be easily integrated, not as much as MISP. Soltra Edge is built for working with STIX/TAXII, but the free version is very limited in terms of importing, exporting and analysis capabilities, as well as API support for integration with custom solutions.

8.5.The FINSEC Approach: Information Sharing

FINSEC will implement tools and techniques for sharing information across different security systems and stakeholders. The information sharing techniques of the project will serve as a basis for implementing collaborative security in the financial sector supply chain, where security systems and critical infrastructures of multiple stakeholders are involved.

The implementation of the information sharing infrastructure will include definition of the data exchange format, implementation of techniques for data & semantic interoperability across different cyber and physical security systems, as well as the definition and implementation of security information exchange protocols

[19] NECOMA project, “Deliverable D3.3: Security Information Exchange – Results”, 2015. http://www.necoma-project.eu/m/filer_public/ef/8b/ef8bda53-edd2-4943-9c1f-95b30dbad1d1/necoma-d33r1946-public.pdf

[20] H. Tazaki K. Okada Y. Sekiya Y. Kadobayashi "Matatabi: Multi-layer threat analysis platform with hadoop" BADGERS 2014.

[21] SISSDEN project, https://sissden.eu/

[22] DiSIEM project, “D4.2 - OSINT data fusion and analysis architecture”, 2018.

Meaningful information could include:

- Evidence (data, metadata) about physical breach of security (ONVIF data format, PSIA metadata about area affected, type of attack)
- Evidence (data, metadata) about cyber attack (the IP addresses of the attacker and details of the attacked ports, identified by the detection system)
- The context (time, location, actors involved) and other context of the incident(s) reported
- A proposed data modelling could be based on PSIA (Physical Security Interoperability)

FINSEC will introduce a collaborative way of dealing not only with threats (cyber and physical), but also other challenges of the financial supply chain. Therefore messaging could refer to:

- Requirements
- Threats
- New regulations (that organizations may have to comply with)
- Counter measures to mitigate risks
- Alerts (referring to possible threats discovered by FINSEC's AI prediction tools)
- Legal Advises

Defining the data model for each of the message types mentioned above is not enough. We need to:

- Validate data that are going to be stored (e.g. permanently in the blockchain)
- Sanitise data to remove sensitive information
- Define a cascading mechanism after the message is retrieved from collaboration layer (e.g. the blockchain)

FINSEC proposes the definition of the architecture needed for the message life-cycle. A smart contract could notify organizations for a new entry message in the blockchain. A modelling scheme is required for communicating events, threat details, regulation information etc. Data models will be stored in a distributed database (a model may change in future) and will be used to generate the messages to be sent.

The type of message to be communicated (threat alert, regulation-related notification, etc.) defines the corresponding data model to be used. According to the message/event type the Generation Component (Collaboration toolbox) will produce the messages in the correct form.

The data model used here will be an integrated one (cyber and physical) extending the existing STIX model to support both cyber and physical threats respecting the key concepts presented in PSIA as well. (See Section 3.2)

In the proposed collaborative security scheme, each participant agrees to share the attack information with the member of the network. However serious confidentiality concerns arise and need to be considered; the vulnerabilities and weaknesses include details about the deployment of IT systems of any organization.

We propose the implementation of a collaboration mechanism. The respective communication protocol will be based on a blockchain ledger.

9. Security Process Models

Specific process frameworks and models for security management need to clearly differentiate between ISMS (Information Security Management System) core processes, supporting processes and management processes, as well as the security measures controlled by ISMS processes. Adjustment and cost effectiveness are key elements of a successful ISMS. A detailed framework of ISMS processes (input, output, interfaces) and their interaction at an activity level help to ensure an appropriate interaction of the ISMS processes.

ISO 27001 as the international standard from ISO/IEC JTC 1 SC27 WG1 for information security management systems, (herein after referred as "ISMS"), is the security standard in enterprises. ISO 27001 contains the requirements for planning, implementing, operating, and improving an ISMS. Requirements are formulated in a general manner to fit for all organizations independent of their size, objectives, business model or location. In ISO 27001 absolutely no requirements are formulated for any specific technology but the standard contains requirements for ISMS core process. Therefore, this standard forms the basis to identify ISMS core processes.

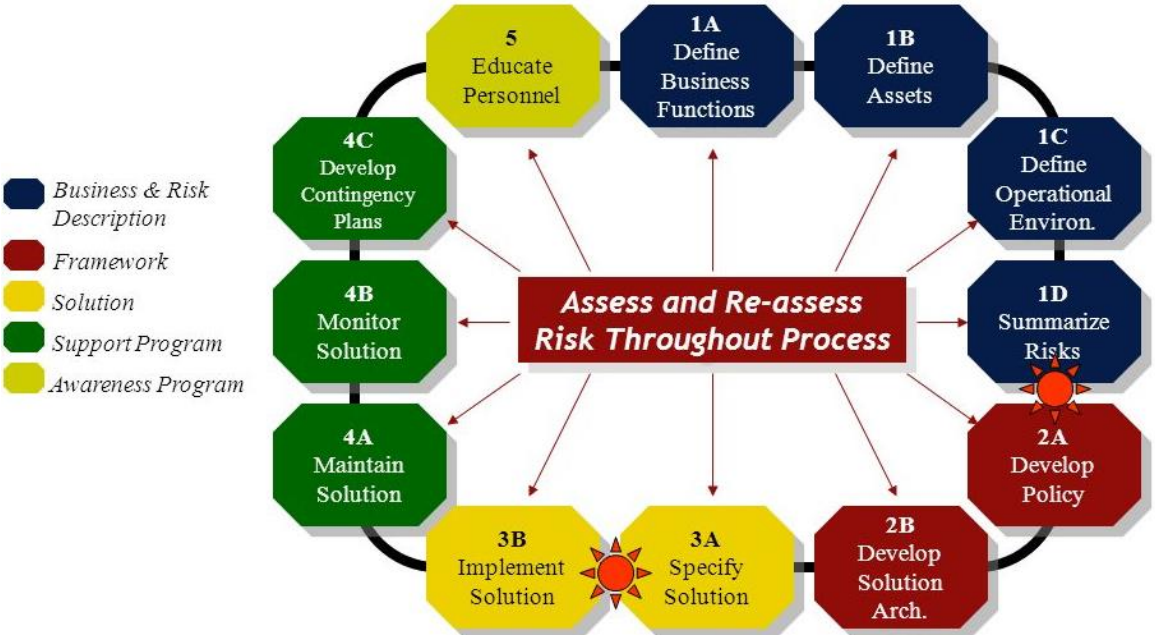

Figure 13 Information Security Process Model

The process steps involve: Business & Risk Description, Framework, Solution, Support, Awareness

9.1. ITIL Security Management Process Model

The first activity in the security management process is the "Control" sub-process. The Control sub-process organizes and manages the security management process. The Control sub-process defines the processes, the allocation of responsibility for the policy statements and the management framework.

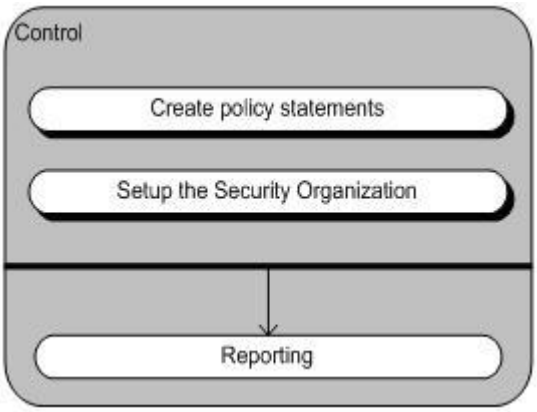

Figure 14 Concept and definition Sub-Process

The meta-process model of the control sub-process gives an overview of the activities of the Control sub-process. The grey rectangle represents the control sub-process and the smaller beam shapes inside it represent activities that take place inside it

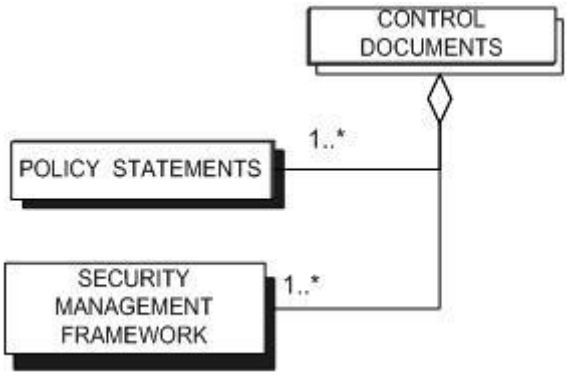

Figure 15 Meta-process model control sub-process

Figure 15 shows the shows the meta model of the control sub-process. The CONTROL rectangle with a white shadow is an open complex concept. This means that the Control rectangle consists of a collection of (sub) concepts.

9.1.1. Plan

The Plan sub-process contains activities that in cooperation with service level management lead to the (information) Security section in the SLA (Service Level Agreement). Furthermore, the Plan sub-process contains activities that are related to the underpinning contracts which are specific for (information) security.
The operational level agreements for information security are set up and implemented based on the ITIL process. This requires cooperation with other ITIL processes.

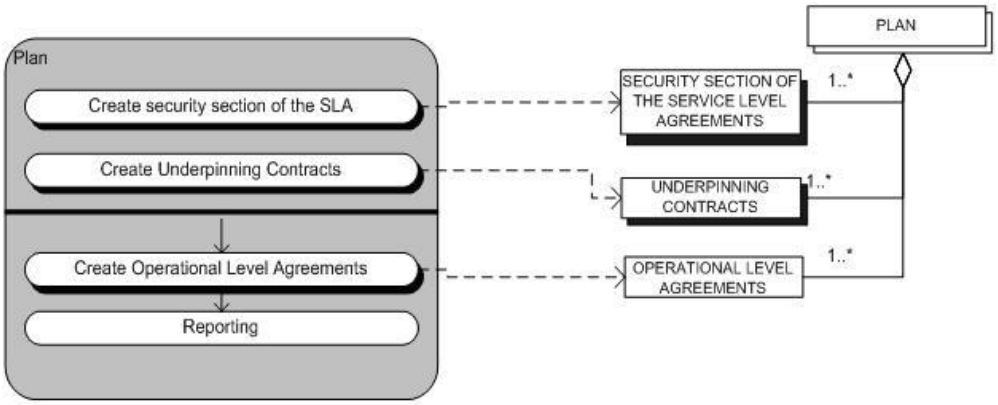

Figure 16 Process-data model Plan sub-process

9.1.2. Implementation

The Implementation sub-process makes sure that all measures, as specified in the plans, are properly implemented. During the Implementation sub-process no measures are defined nor changed. The definition or change of measures takes place in the Plan sub-process in cooperation with the Change Management Process.

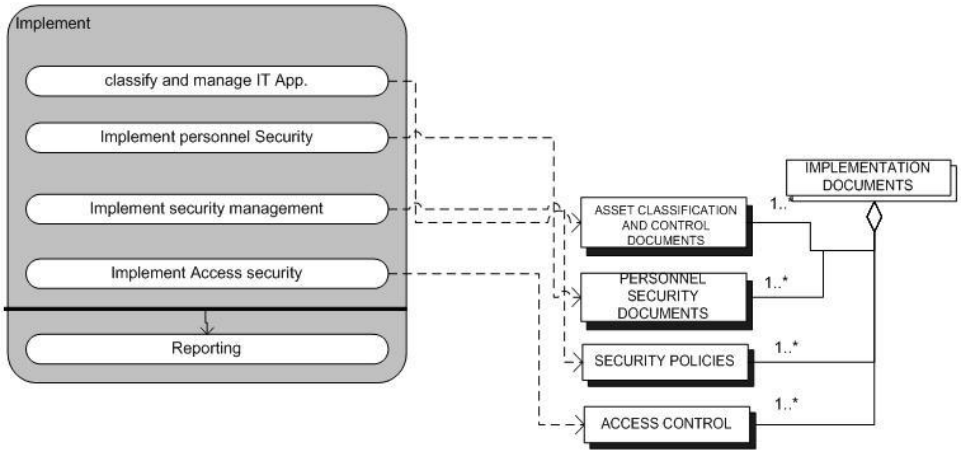

Figure 17 Process-data model Implementation sub-process

The left side of Figure 17 is the meta-process model of the Implementation phase. The four labels with a black shadow mean that these activities are closed concepts and they are not expanded in this context. No arrows connect these four activities, meaning that these activities are unordered and the reporting will be carried out after the completion of all four activities. During the implementation phase concepts are created and /or adjusted.

9.1.3. Evaluation

Evaluation is necessary to measure the success of the implementation and security plans. The evaluation is important for clients (and possibly third parties). The results of the Evaluation sub-process are used to maintain the agreed measures and the implementation. Evaluation results can

lead to new requirements and a corresponding Request for Change. The request for change is then defined and sent to Change Management.
The three sorts of evaluation are self-assessment, internal audit and external audit.

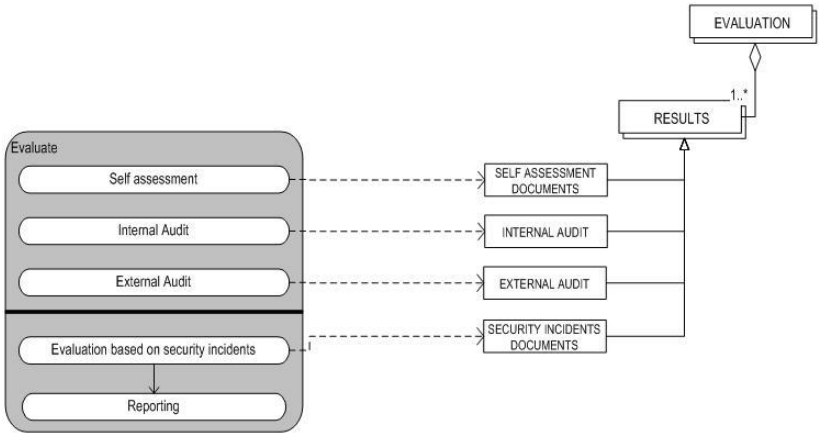

Figure 18 Process-data model Evaluation sub-process

The process-data diagram illustrated in the Figure 13 consists of a meta-process model and a meta-data model. The Evaluation sub-process was modelled using the meta-modelling technique. The dotted arrows running from the meta-process diagram (left) to the meta-data diagram (right) indicate which concepts are created/ adjusted in the corresponding activities. All of the activities in the evaluation phase are standard activities.

9.1.4. Maintanence

Because of organizational and IT-infrastructure changes, security risks change over time, requiring revisions to the security section of service level agreements and security plans.
Maintenance is based on the results of the Evaluation sub-process and insight in the changing risks. These activities will produce proposals.

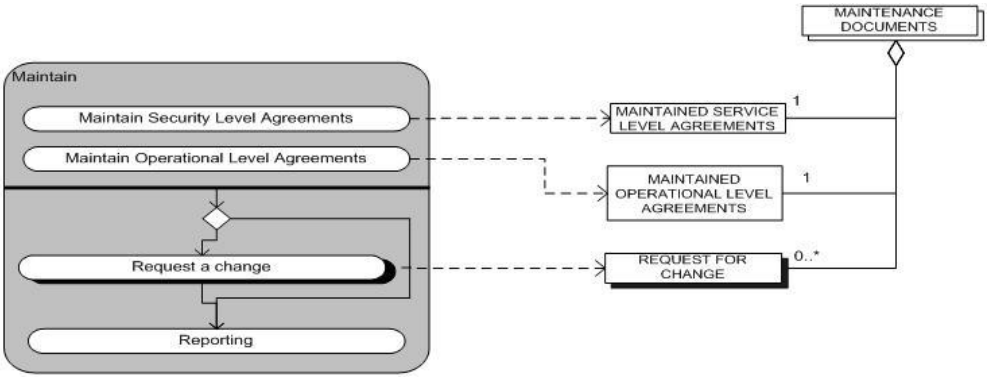

Figure 19 Process-data model maintanance sub-process

Errore. L'origine riferimento non è stata trovata.14 is the process-data diagram of the implementation sub-process. This picture shows the integration of the meta-process model (left) and

the meta-data model (right). The dotted arrows indicate which concepts are created or adjusted in the activities of the implementation phase. The maintenance sub-process starts with the maintenance of the service level agreements and the maintenance of the operational level agreements.

9.2.FINSEC Security Process Model

The proposed model is based on the ITIL Security Management Process and it has been extended to bring both cyber and physical into an overall model. It is designed to ensure that the confidentiality, integrity and availability of an organization's information, data and IT services. The complete process data model is below in Figure 20. It is based on three stages:

Implement:

This key element ensures that appropriate procedures, tools, and controls are in place to support the ITIL Information Security Management Policy. It also ensures that the security measures are implemented according to the defined plan.

Evaluation:

This phase is responsible for measuring the success of the security implementation. For doing this it carries out regular technical security audits of IT systems. It also checks the compliance of security implementation with IT security policy and security requirements defined in SLAs.

Maintain:

This phase takes the security evaluation results and suggests improvements on security implementation, and on security agreements as specified in, for example, SLAs and OLAs.
these phases are NOT one-time activity. These are continuous and cyclic activities.

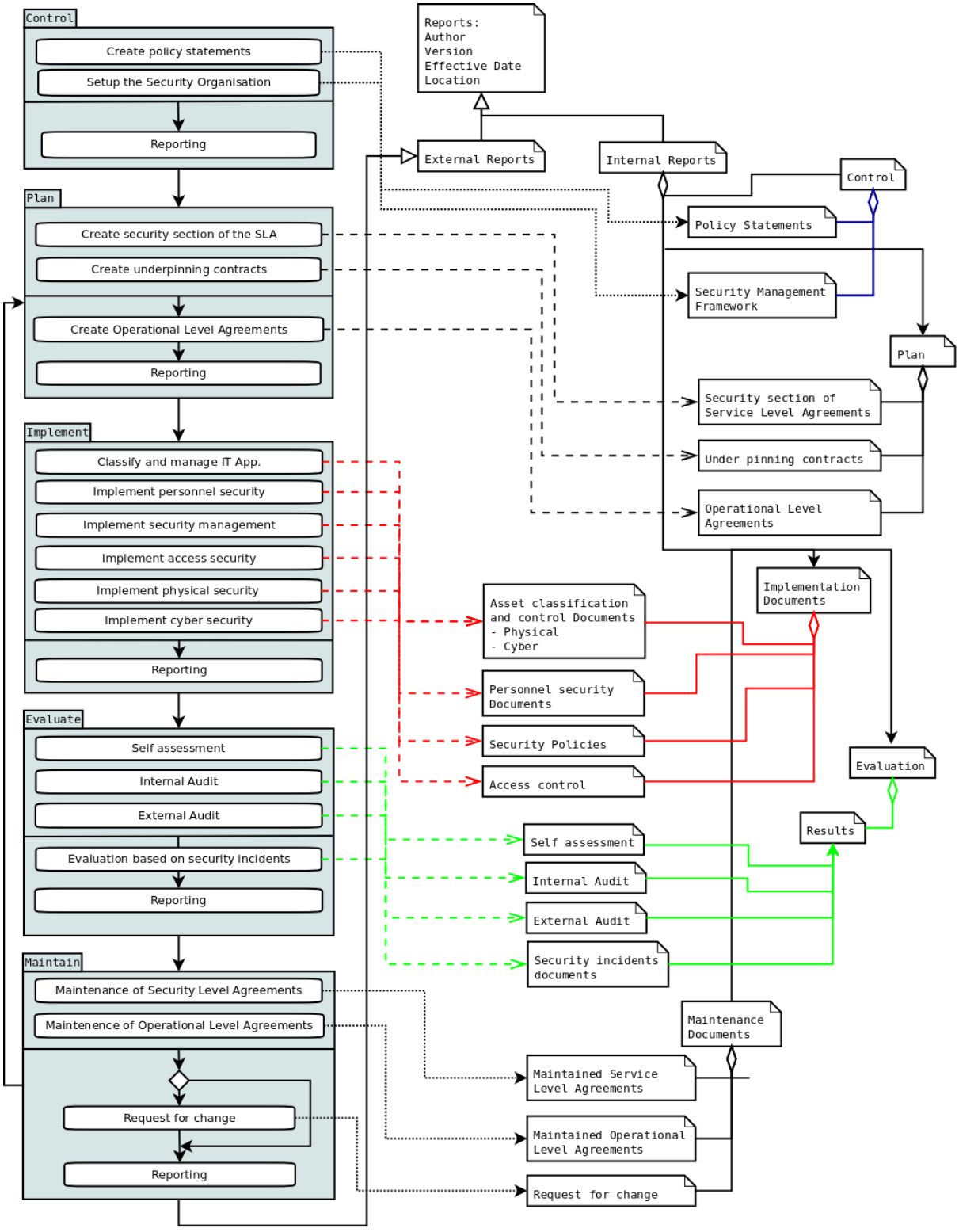

Figure 20 Security Process Model

10. FINSEC Risk Modelling Specifications

10.1. Standards-Based Risk Modelling Approaches

The initial specifications of FINSEC Risk modelling approach build on concepts and models presented in security risk management standards such as ISO 27001, whose process diagram is depicted in Figure 21.

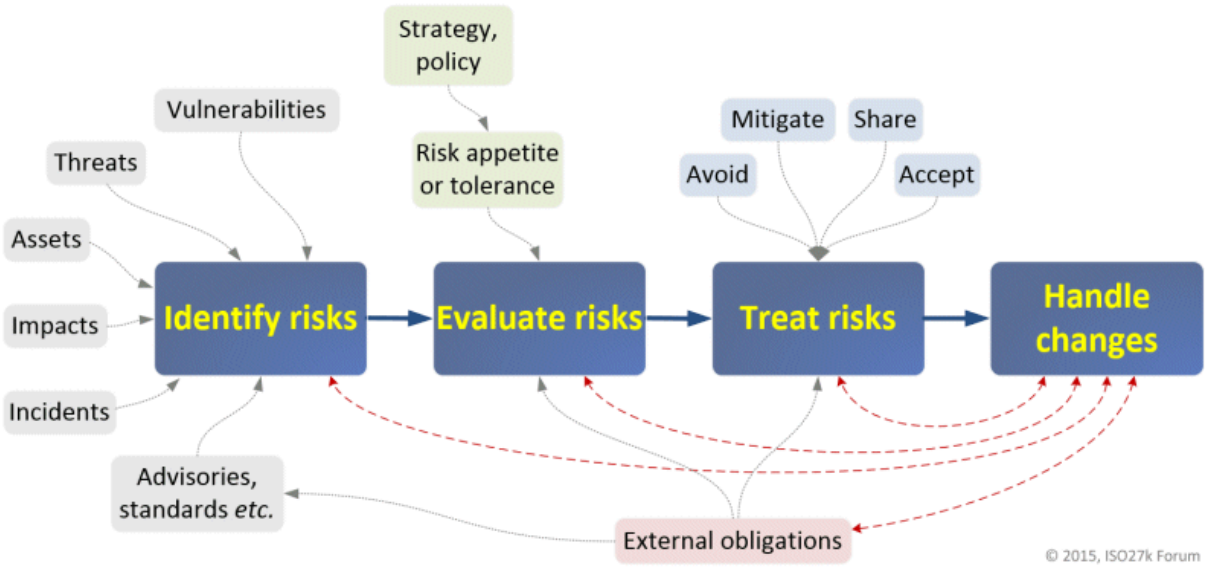

Figure 21 Information Security Risk Management Process Diagram (source ISO 27001 Forum)

The first stage of the process is to *Identify* potential information risks. Several factors or information sources feed-in to the *Identify* step, including: *Vulnerabilities; Threats*; *Assets; Impacts*; *Advisories; Evaluate risks;*

Treat risks means avoiding, mitigating, sharing and/or accepting them. This stage involves both deciding what to do and doing it (implementing the risk treatment decisions).

Handle changes might seem obvious, but it is called out on the diagram due to its importance. Information risks are constantly in flux, partly as a result of the risk treatments, partly due to various other factors both within and without the organization.

The organization often has to respond to *External obligations* such as compliance and market pressures or expectations.

To integrate risk management throughout an organization a three-tiered approach is adopted: (i) organization level; (ii) mission/business process level; and (iii) information system level. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization.

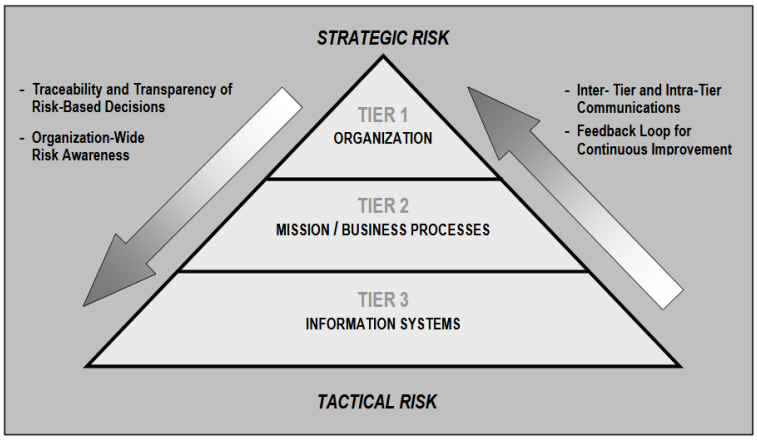

Figure 22 MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT (Source NIST SP 800—39)

Tier 1 addresses risk from an organizational perspective. Tier 1 implements the first component of risk management (i.e., risk framing), providing the context for all risk management activities carried out by organizations. Tier 1 risk management activities directly affect the activities carried out at Tiers 2 and 3. For example, the missions and business functions defined at Tier 1 influence the design and development of the mission/business processes created at Tier 2 to carry out those missions/business functions. Tier 1 provides a prioritization of missions/business functions which in turn drives investment strategies and funding decisions, thus, affecting the development of enterprise architecture (including embedded information security architecture) at Tier 2 and the allocations and deployment of management, operational, and technical security controls at Tier 3.

10.1.1. Models: Assets and Processes within an organisation

Within Financial Institutions currently the risk framework is developed at enterprise level and is composed of strategic, financial, compliance, reporting, reputation and operational risks.
It was developed following:

- the ECB's oversight framework and the supranational standards issued by the International Organization of Securities Commissions (the IOSCO Principles for financial markets infrastructures);
- the disposals coming from ECB (among them Circular no. 285 of December 17, 2013 "Disposal of oversight for banks") and other central banks dependent on legal jurisdictions;
- the Enterprise Risk Management COSO framework;
- the ISO 31000 standard.

The approach is based on the international standard ISO 31000:2018 and takes into account the relevant provisions of the respective central bank. The risk management process, is based on the following tasks:

Communication and consultation: the aim is to guarantee that the corporate bodies and the staff understand, adopt and implement the risk management process and have a shared knowledge and awareness base in order to make the correct decisions and implement the actions necessary for appropriate risk analysis and management.

Scope, context and criteria: the aim is to analyse, document, understand and assess the external and internal context in which the Company operates.

The aspects of the external context are:

- the social, cultural, political, legal, regulatory, financial, technological, economic and competitive environment in which the Company operates;
- the trends that may have an impact on the objectives of the Company;
- relations with and opinions of external parties involved.

The aspects of the internal context are:

- organisational structure, roles, responsibilities, relations, competences, resources, decision-making processes, corporate culture, policies, objectives and the strategies to achieve them;
- relations with and opinions of internal stakeholders;
- information systems, standards and guidelines adopted.

Risk assessment - risk identification: the aim is to identify the risks linked to significant events that may have a negative impact on the achievement of the objectives. The process:

- draws on the possible information sources which may identify risks and their impacts;
- ensures that risks are recorded in specific risk registers/catalogues;
- is performed in a continuous and selective manner on the corporate assets (e.g. services, projects, processes, technology architectures).

Risk assessment - risk analysis: the aim is to assess the risks identified and the notifications of potential risks. The activities provided for are as follows:

- collect the information related to the notification of the potential risk;
- identify the Risk Owner with whom to share the notification;
- assign a risk value based on the impacts and probability of occurrence, by calling on the experience of the experts or by giving a value to the incidents and operating losses incurred;
- validate the notification with the corporate bodies appointed.

Risk assessment - risk evaluation: the aim is to decide if and how to treat the risks. Based on the risk management process adopted, the activities provided for are as follows:

- identify the risk clearly and precisely;
- decide whether to treat and close the risk, on the basis of the delta compared to the risk appetite of the organisation and of other evaluations regarding merit and opportunity;
- define the priority of action.

Risk treatment: the aim is to define the actions in response to the risks, and plan and implement the activities defined. The activities provided for are as follows:

- define the risk response type;
- define the risk treatment plan;
- implement the activities identified;
- update the risk treatment plan.

Monitoring and review: the aim is to monitor the implementation of the activities undertaken and to determine, by means of indicators, the effectiveness and efficiency of the measures implemented. The monitoring phase permits:

- definition of closure of the risk, with a possible retroactive process to manage the residual risk (which produces a new risk notification);
- performance of a further evaluation of the risk, following results that are not in line with expectations;

- updating of the risk treatment plan.

Recording and reporting: the aim is to communicate risk management activities and outcomes across the Company, provide information for decision-making, improve risk management activities and assist interaction with stakeholders, including those with responsibility for risk management activities. Information management also takes into account the use, the information sensitivity and the external and internal context.
At corporate level, the risk management process includes:

- a set of predefined rules relating to the risk policy, roles and responsibilities, risk appetite and alerts;
- specific process inputs originating from customers, staff responsible for services/initiatives, staff responsible for operating processes/technologies, incidents and/or significant external events, staff responsible for the governance systems, internal/external audit activities and certifications;
- a method for the criteria used to assess the likelihood and impact of risks, and for the analysis of risks for services/products and initiatives;
- specific outputs represented by the risk records, reports and information notices.

10.1.2. Models: Assets and Processes within the financial supply chain

Financial Institutions are aware of their exposure to risks, which are heterogeneous and dynamic. They are also aware of the impact these risks may have on their operations, customers' operations, payment systems, financial community and citizens.
Typically, they have implemented a risk governance and internal control system through which they fight threats and vulnerabilities that may arise and threaten the delivery of their services.
The aim is to minimize the operating, financial, compliance and reputational risks. All institutions act on the business processes for the customers, cyber security, fraud management and business continuity. This is all done whilst fully taking into account the requirements and concerns of suppliers/ partners and to personal safety.

A lot of the mid-sized and large financial institutions have a CERT (Computer Emergency Response Team), a team made up of digital security experts that coordinate all the activities in response to a computer emergency. The mission is to coordinate all activities aimed at the prevention, detection and response to cyber security incidents within its constituency.

SIA, one of the partners in FINSEC, cooperates with the official Italian financial CERT promoted by The Bank of Italy via the Italian Banks association technical entity (ABILab) on Network and Card processing services through consultancy and information sharing in anonymous form. SIA leverages commercial information services (FS-ISAC) and others (e.g. OSINT).
Another example, in the case of a mid-sized bank operating in the jurisdiction of Spain, Liberbank, also in FINSEC project, establishes four categories for their providers based on the risk levels of the activities they are going to perform. These are:

- Low: Physical access with no interaction with information systems.
- Medium: Access to digital data for development of their functions. Access to client and banking operations data.
- High: Remote connection to internal infrastructure. Liberbank data is exposed via the Internet and is therefore at risk of being compromised
- Very High: Storing business and client data outside of Liberbank. Subcontracting critical services.

Each of these categories has some specific security requirements to mitigate and monitor the identified security risks:

- Low: establishing specific contractual clauses
- Medium: Self assessment of basic measures in the systems for the provider. Risk analysis of the initiative as a whole.
- High: Certification of the process to externalize.
- Very High: Restrictive security measures

10.2. FINSEC Risk Modelling Approach

The approach taken here combines the traditional approach taken by widely accepted mature international standards like ISO 27001, ISO 27005 and ISO 31000 and the incorporation of the three-tier model advocated in NIST SP-800-39. This means that the overall approach must be considered in a business context, and the inter-relationships with other business functions. It should also take into account the organisational risks and the policies for corporate governance. All this combined with the legal and regulatory drivers will provide the overall context for the proposed framework.

The first step will be the assessment of risks which will include the following activities:

- Assets identification
- Assets relevant legal and business requirements
- Assets valuation – taking into account the impacts of loss of confidentiality, integrity and availability
- Assets significant threats Identification
- Assessment of likelihood occurrence of those threats and vulnerabilities
- Risk calculation
- Risk evaluation.

This overall approach which is based on ISO 27001/ISO 3001 can then be transposed to the organisation model as indicated in NIST SP-800-39. This model is based on three tiers as indicated in section 10 above and is elaborated further below:

Tier 1

At Tier 1 all of the following have to be defined in order to 'frame the organisational risk' which would then provide the basis for the approaches taken in Tier 2 and 3 (including but not limited to):

1. Identify Risk Appetite
2. Overall Business Objectives
3. Organisational Legal and Regulatory Environment
4. Interested Parties Requirements (e.g. Regulatory Bodies, Customers, Law Enforcement, Shareholders)
5. Business Strategy
6. The risks that prevent the business objectives from being met.

Tier 2

The relevant business processes to deliver on the business objectives and strategy identified in Tier 1 should be elaborated and the risks associated with each of those processes should be identified. The following risks would typically arise at this level:

1. Loss of Productivity
2. Loss of Service
3. Loss of Cashflow

4. Loss of Customer Confidence
5. Loss of Profits
6. Legal Penalties, Fines and Liability Costs
7. Reputational damage to the business

As a result, some example business processes and related risks could also be:

8. Human Resources – Recruitment. Associated Risks might be loss of data (PII) and/or unauthorised access.
9. CRM – Systems not available when required which could cause reputational damage
10. Procurement – suppliers don't have appropriate corporate governance and compliance implemented
11. Finance – system is compromised jeopardising the privacy and integrity of PII and critical financial data that could result in monetary impact to the organisation.

Tier 3

Tier 3 is about the allocations and deployment of management, operational, and technical security controls based on the organizational perspective from Tier 1 and the business processes relating to that in Tier 2. Typical Risks and Controls at Tier 3 would be:

1. System Access Control
2. System Availability
3. Data Privacy
4. Network Intrusion
5. Weak Authentication
6. Lack of Software Controls
7. Breaking or unauthorized entry into buildings and officers
8. Social engineering
9. Theft of equipment or vandalism
10. Major System Failure

At each of these three tiers we will use the following approach based on ISO 27001:2013

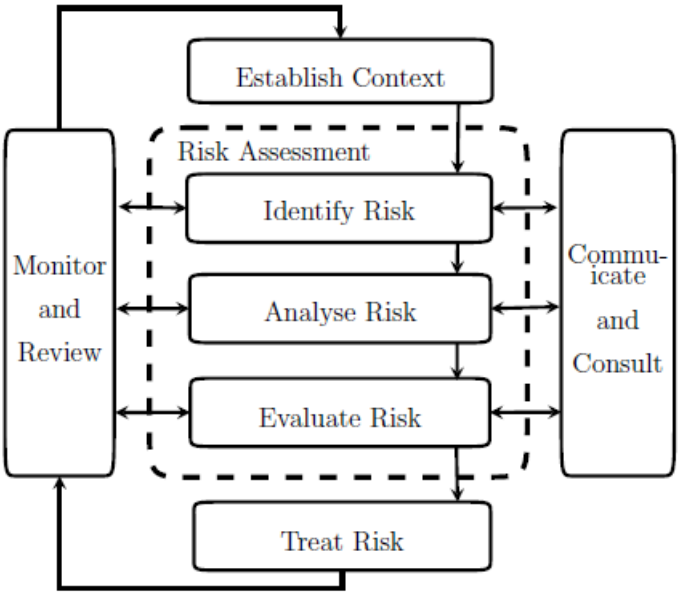

Figure 23 ISO 27001 Risk Management Process

The process above is done firstly at Tier 1 within the context of the overall organisational business and strategic objectives. At Tier 2 this same approach is carried out for each mission/business process which are all driven by the context as identified in Tier 1. At Tier 3 the same approach is taken for each operational system and technical security control. The resulting selection and implementation of risk controls at each of the three tiers will be based on the controls within Annex A of ISO 27001:2013.

11. Conclusions

Whilst the project addresses something that has proven challenging in the market, i.e. to deliver integrated protection for both cyber and physical infrastructures and for combined cyber and physical threats, considerable work has been done to address infrastructure and systems in their own right. The potential approaches available to FINSEC and its constituent components are presented in this deliverable including:

- The varied approaches and protocols for data modelling for both physical and cyber security.
- The standards based methods for assurance of Cyber Physical Systems.
- The different algorithmic approaches for predictive data analytics.
- The approaches to gathering security data, the probes and methods by which that data can most effectively analysed.
- The variety of standards, initiatives and protocols for information sharing of cyber incident intelligence within financial services and other domains within national critical infrastructure.
- An analysis of the pros and cons of loosely coupled and tightly coupled approaches with respect to the integration of systems.
- A review of the standards-based approaches for Security Process Modelling and Risk Management within the context of Financial Institutions for both the organisation and the complete supply chain.

Defining the data model is critical at this stage as all the components of the overall framework will rely on receiving consistent and usable data in order that they are able to deliver the required functionality. After a very comprehensive review of the different standards and protocols available it was clear that no one existing approach was adequate for FINSEC as it is, i.e. without enhancement or modification. FINSEC has proposed the use of STIX with specific enhancements that also take the physical infrastructure into account and also respects the existing data models for that physical infrastructure which are mainly based on PSIA. Section 3.2 details the proposed approach.

Assurance of Cyber Physical Systems has been primarily a standards based activity and significant work has gone on within International Standards Bodies. The state of the art is made up of standards like ISO 10746 and Common Criteria addressing architecture viewpoints and a means to establish consistent and internationally recognized evaluation regime for security products. The approach proposed in FINSEC builds on what is done in ISO 10746 and provides an approach that:

- Is based on international open standards as far as possible.
- Captures system specific properties (for example, functionality, timing, storage).
- Documents basic security concepts (for example, assets, threats, security requirements, and controls).
- Includes models that are appropriate and useful for security design as well as analysis and implementation and testing.
- Is technology neutral, that is, not assume specific technologies or products to be realized.

Section 4 details the approach taken for Assurance on the basis of modelling the system based on a number of viewpoints: Enterprise, Informational, Computational, Engineering and Technology (See Section 4.2)

Predictive Analytics using Machine Learning and Statistical Methods is an area that has been worked on for some time now and in more recent times has successfully been applied in the area of cyber security with some now very prominent products where these approaches are at the core for how they deliver the means by which to identify, assess, prevent and protect from threats. In Section 5 we

consider the different algorithmic approaches including deep learning, Bayesian inference, Classification, Clustering and so forth. It is the case that all the approaches prove to have advantages and limitations and that no one single solution is any sort of silver bullet. All of the algorithms are based on specific data requirements and have capabilities to provide certain specific types of output/answers.

It will be important to use algorithms (or combinations of) that are fast to deliver intelligence on anomalies and attacks with the sort of speed to maximise the value of that intelligence. The architecture for deploying and implementing the algorithmic approach will have to take into account the requirement to do big data treatment within seconds. The results of this analytics process will inform us if there is a suspicious attack in occurring or that an anomaly has been detected. For reinforcement of any output from the analytics process more data can be requested for analysis to confirm/or not the existence of the attack or anomaly.

Some Key Performance Indicators are listed in Section 5 that the predictive analytics approach and architecture should meet. They include six performance tactics, four accuracy tactics, two scalability tactics, three reliability tactics, and one security and usability tactic each. Performance and Scalability are critical. As such the mapping and deployment of the predictive analytics service is subject to some latency, bandwidth and storage constraints. Where very weak latencies are expected, components must be deployed on the fog or the in edge of the CPS. Otherwise, the data collection architecture will suffer from poor performance and scalability.

Security related data must be collected and analyzed in an intelligent, resilient, reliable, secure and timely manner fulfilling all the communication requirements and standards to detect attacks. To achieve this the FINSEC approach includes the design and deployment of the concept of adaptive multi-layer data collection by adapting different approaches. (See Section 6.5). Detection capability is greatly improved by correlating a wide-range of data sources and by multi-layer data collection and analytics.

The Security Knowledge Base will be an aggregation of threat intelligence from various public data/intelligence sources related to the typical cyber and physical infrastructure found in financial institutions. Its structure will be based on the asset types and their interactions as part of the overall critical infrastructure. The Knowledge Base will focus its collection of threat intelligence on these defined asset types. The Security Knowledge Base will be represented through the FINSEC DATA MODEL. Before being stored, all the information incoming from external sources will be translated by the FINSEC connectors into the FINSEC DATA MODEL. The Security Knowledge Base will expose a REST API to enable interactions with the other FINSEC services.

FINSEC will implement tools and techniques for sharing information across different security systems and stakeholders. This will provide a basis for implementing collaborative security in the financial sector supply chain, where security systems and critical infrastructures of multiple stakeholders are involved. The Data Exchange and Representation will be based on the FINSEC Data Model as defined in Section 3. A Blockchain approach is proposed (see section 8) which will provide a mean by which the data can be validated, and a smart contract can be used to provide alerts when new entries appear. Each Participant must agree to share information with other participants on the network however there are always likely to be conflicts of interest and confidentiality issues emerging which will require the appropriate granular access control within the network.

Security Process Models are generally standards based and generally follow a three-stage process: Implement, Evaluate and Maintain with a plethora of sub-processes. The proposed model for FINSEC is based on the ITIL Security Management Process and it has been extended to bring both cyber and physical into an overall model. It is designed to ensure that the confidentiality, integrity and availability of an organization's information, data and IT services. (See Section 9.3)

Finally managing risk in the organisation is a critical component of its approach to protection and mitigation. The approach taken here will combine the traditional approach taken by widely accepted mature international standards like ISO 27001, ISO 27005 and ISO 31000 and the incorporation of the three tier model advocated in NIST SP-800-39. This is in-line with the standards and approached already used and implemented by financial institutions but puts it within the context of the three tiers: 1. Organisation, 2. Mission/business processes, 3. Information Systems.

In summary Sections 3 to 10 of this report provide a basis for the definition of the reference architecture in Task 2.5 and for the subsequent workpackages, to define and implement the lower level components and services.

12. References

[Lin 2018] H. Lin, Z. Yan, Y. Chen and L. Zhang, "A Survey on Network Security-Related Data Collection Technologies," in IEEE Access, vol. 6, pp. 18345-18365, 2018. doi: 10.1109/ACCESS.2018.2817921

[NIST 1500-201] NIST Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0, June 2017

[NIST 1500-202] NIST Special Publication 1500-202, Framework for Cyber-Physical Systems: Volume 2, Working Group Reports, Version 1.0, June 2017

How Artificial Intelligence Will Secure the 21st Century, CYLANCE Whitepaper, 2017

Not All Machine Learning Is Created Equal, CYLANCE Whitepaper, 2017

Security Analytics: Using Deep Learning to Detect Cyber Attacks, Glenn M. Lambert II, University of North Florida, 2017

The Future of AI-Powered Autonomous Response, DarkTrace Whitepaper, 2018

Data Mining Clustering Techniques – A Review Shivangi Bhardwaj CSE,Amity University Haryana, India, JCSMC, Vol. 6 , Issue. 5, May 2017, pg.183 –186

Measuring Network Security Using Dynamic Bayesian Network, Marcel Frigault and Lingyu Wang

ACM 978-1-60558-321-1/08/10, 2008

[Soua 2013] A. Soua and H. Afifi, "Adaptive data collection protocol using reinforcement learning for VANETs," 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), Sardinia, 2013, pp. 1040-1045. doi: 10.1109/IWCMC.2013.6583700

[Erbacher 2008] Erbacher, Robert. (2008). Steps for Improving Data Comprehension for Digital Security and Forensics. Proceedings of the 2008 International Conference on Security and Management, SAM 2008. 318-326.

[Lin 2019] Huaqing Lin, Zheng Yan, Yulong Fu, Adaptive security-related data collection with context awareness, Journal of Network and Computer Applications, Volume 126, 2019, Pages 88-103, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.11.002

[Jing 2018] X.Y. Jing, Z. Yan*, W. Pedrycz, “Security Data Collection and Data Analytics in the Internet: A Survey”, IEEE Communications Surveys and Tutorials, 2018. Doi: 10.1109/COMST.2018.2863942 (IF: 20.23)

[Zhou 2018] D.H. Zhou, Z. Yan*, Y.L. Fu, Z. Yao, “A Survey on Network Data Collection”, Journal of Network and Computer Applications, 2018. Doi: 10.1016/j.jnca.2018.05.004 (IF: 3.5)

[Lin 2018] H.Q. Lin, Z. Yan*, Y. Chen, L.F. Zhang, “A Survey on Network Security-Related Data Collection Technologies”, IEEE Access, vol. 6, issue 1, pp. 18345-18365, Dec. 2018. Doi: 10.1109/ACCESS.2018.2817921 (IF: 3.224)

[Li 2018] G.Q. Li, Z. Yan, Y.L. Fu*, H.L. Chen, “Data Fusion for Network Intrusion Detection: A review", Security and Communication Networks, 2018. vol. 2018, Article ID 8210614, 16 pages, 2018. https://doi.org/10.1155/2018/8210614/.

[Liu 2018] G. Liu, Z. Yan*, W. Pedryczc, “Data Collection for Attack Detection and Security Measurement in Mobile Ad Hoc Networks: A Survey”, Journal of Network and Computer Applications, Vol. 105, pp. 105-122, march 2018. Doi: https://doi.org/10.1016/j.jnca.2018.01.004 (IF: 3.500)

[He 2018] L.M. He, Z. Yan*, M. Atiquzzaman, “LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey”, IEEE Access, Vol. 6, Issue 1, pp. 4220-4242, 2018. Doi: 10.1109/ACCESS.2018.2792534

[Ullah 2018] Ullah, F., and Babar, M.A (2018) 'Architectural Tactics for Big Data Cybersecurity Analytic Systems: A Review'

[Bonelli 2011] N. Bonelli, A. DiPietro, S. Giordano, G. Procissi, and F. Vitucci, “Towards Smarter Probes: In-Network Traffic Capturing and Processing,” in Trustworthy Internet, L. Salgarelli, G. Bianchi, and N. Blefari-Melazzi, Eds. Milano: Springer Milan, 2011, pp. 289–301.

[Schroeder 2016] Schroeder, J. et al. Adaptive Data Collection Mechanisms for Smart Monitoring of Distribution Grids. arXiv 1608, 06510v1 (2016).

[Blefari-Melazzi 2011] Nicola Blefari-Melazzi, Giuseppe Bianchi, & Luca Salgarelli, Editors: Trustworthy Internet, Springer-Verlag Italia Srl 2011,

[Habib 2016] C. Habib, A. Makhoul, R. Darazi and C. Salim, "Self-Adaptive Data Collection and Fusion for Health Monitoring Based on Body Sensor Networks," in IEEE Transactions on Industrial Informatics, vol. 12, no. 6, pp. 2342-2352, Dec. 2016. doi: 10.1109/TII.2016.2575800

[Kemal 2016] M. S. Kemal and R. L. Olsen, Adaptive Data Collection Mechanisms for Smart Monitoring of Distribution Grids, arXiv:1608.06510v1 [cs.SY] 22 Aug 2016

[Ji 2009] Z. Ji, Z. Kuang and H. Ni, "A Novel Two-Dimension Adaptive Data Collection Method for Network Management," 2009 WRI International Conference on Communications and Mobile Computing, Yunnan, 2009, pp. 237-241. doi: 10.1109/CMC.2009.10

[Tang 2008] X. Tang and J. Xu, "Adaptive Data Collection Strategies for Lifetime-Constrained Wireless Sensor Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 6, pp. 721-734, June 2008. doi: 10.1109/TPDS.2008.27

[Al-Qurabat 2017] Ali Al-Qurabat and Ali Idrees (2017). Adaptive Data Collection protocol for Extending Lifetime of Periodic Sensor Networks. Qalaai Zanist Scientific Journal. 2. 10.25212/lfu.qzj.2.2.11.

[Laiymani 2013] D. Laiymani and A. Makhoul, "Adaptive data collection approach for periodic sensor networks," 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), Sardinia, 2013, pp. 1448-1453. doi: 10.1109/IWCMC.2013.6583769

[Androulaki18] Elli Androulaki et. Al. “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”, Proceedings of the Thirteenth EuroSys Conference (EuroSys '18), Article No. 30, Porto, Portugal — April 23 - 26, 2018.

[Brown16] Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn, «Corda: An Introduction», Corda/R3 Whitepaper, August, 2016.

[Babich16] Babich, Volodymyr and Hilary, Gilles, Blockchain and Other Distributed Ledger Technologies in Operations (July 16, 2018). Available at SSRN: https://ssrn.com/abstract=3232977

13. Annexes

ANNEX A

The Figure Below shows a worked through example of the FINSEC Data Model SDOs as described in Section 3.2. It shows the basic flow of data for a cyber attack on an ATM Machine. It demonstrates the use of the following SDOs:

1. Organisation SDO
2. Asset SDO
3. Probe SDO
4. Probe Configuration SDO
5. Threat SDO

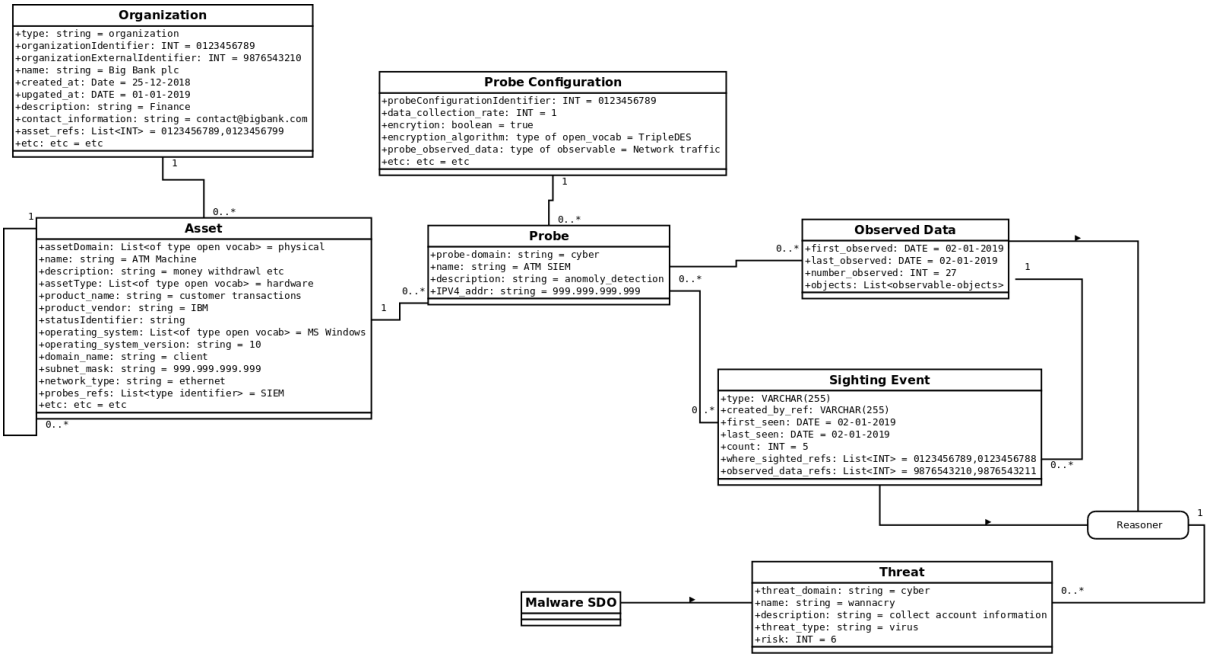

Figure 24 Example Threat Representation with the FINSEC data model

The Probe SDO outputs observed data and Sightings (events) as described in Section 3.2. The outputs from both of these will be analysed, (depicted in Figure 19 by the Reasoner), with the results going into the Threat SDO.