Integrated Framework for Predictive and Collaborative Security

of Financial Infrastructures

Start Date of Project: 2018-05-01

Duration: 36 months

D7.1 Market Platform Architecture and Technical Specifications

Deliverable Details	
Deliverable Number	D7.1
Deliverable Title	Market Platform Architecture and Technical Specifications
Revision Number	1.0
Author(s)	INNOV
Due Date	31/01/2019
Delivered Date	31/01/2019
Reviewed by	AS
Dissemination Level	PU
EC Project Officer	Christoph CASTEX

Contributing Partners	
1.	INNOV (responsible)
2.	GFT
3.	SIA
4.	JRC
5.	NEXI
6.	AS
7.	Z&P
8.	CCA

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

Document Status

☒ draft
☒ WP leader accepted
☒ Consortium reviewed
☒ Project coordinator accepted

Revision History

Version	By	Date	Changes
0.1	INNOV	10/12/2018	Initial ToC, indicative items, List of Contributors
0.12	INNOV	14/12/2018	Introduction (Section 1) and initial list of services and their description (Section 3)
0.20	INNOV	21/12/2018	Information Architecture (Section 3) – Updates in the technical specifications (Section 4)
0.25	INNOV, SiLO	15/01/2019	First version of the Technical Architecture
0.30	INNOV	17/01/2019	Analysis of Relevant platforms in Section 2
0.31	Z&P	24/01/2019	Inputs on Dissemination and Quality Control of the Document
0.35	INNOV	24/01/2019	Updates in Section 2
0.40	INNOV	25/01/2019	Authoring of Executive Summary and Conclusions
0.50	INNOV	28/01/2019	Preparation of version for the latest round of quality control
0.60	FUJITSU, AS	29/01/2019	Quality and Peer Review of the deliverable
1.0	INNOV	29/01/2019	Version addressing review comments

Abbreviations

B2B	Business to Business
CEI	Critical Energy Infrastructures
CDN	Content Delivery Network
CSV	Comma Separated Values
CVE	Common. Vulnerabilities and Exposures
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information Communication Technologies
IA	Innovation Action
JSON	JavaScript Object Notation
MSP	Multi-Sided Platform
NIST	National Institute of Standards and Technology
RAE	Risk Assessment Engine
SECaaS	Security as a Service
SME	Small Medium Enterprise
SOA	Service Oriented Architecture
URL	Uniform Resource Locator
USM	Unified Security Management
XML	eXtensible Markup Language

Executive Summary

FINSEC's main goal is to introduce and validate a novel, integrated approach to the security of the critical infrastructures of the financial sector, which shall combine cybersecurity and physical security processes in a common, integrated security center. The project is already working towards a wide range of scientific and technical results, in the areas security monitoring and predictive security analytics for the infrastructures of the finance sector towards providing security officers within financial institutions with services like risk assessment, compliance auditing and security alerts.

One of the main objectives of the FINSEC project is to promote and make widely available these results through a public cloud platform, while at the same time creating a stakeholders' community around it. This platform is conveniently called market platform of the FINSEC platform and is designed and implemented as a multi-sided market platform that will bring together the supply and demand sides for security solutions in the financial sector. The present deliverable is devoted to the description of the architecture of the market platform and of its technical specifications.

The architecture of the market platform is described in terms of the technical components that will enable its implementation, but also in terms of the structuring principles that will drive their integration. On the other hand, the specifications of the platform are manifold and include:

- Specification of the platform's functionalities, notably common functionalities of multi-sided platforms such as user registration, services registration, service rating, services search and more.
- Specification of the platforms content, including blog posts, presentations, simulation services, services description texts and more.
- Specification of the architecture of the information elements of the platform, notably in terms of the main elements of the portal that will serve as a single entry point to the services that are going to be provided.

One of the main and most important parts of the deliverable is devoted to an initial description of the services that are going to be provided through it, including:

- Simulation and demonstration of SECaaS Services, i.e. of services that will be delivered based on a security-as-a-service modality. This service will provide a simulated demonstration of FINSEC security services based on sample data.
- Risk assessment services, provided as a B2B ,(Business-to-Business), service to interested parties
- Access to parts of the project's security knowledge base.
- Training presentations and seminars, notably focusing on security for digital finance services.
- Security consulting services targeted to financial sector stakeholders.
- Demonstrators of the project's security probes, such as the CCTV probe for supporting physical security.
- A forum for discussing standards and regulation.
- Integration services to be provided in a B2B fashion.
- Access to open datasets for security services in the finance sector.
- Access to the entire FINSEC platform or selected parts of it (e.g., microservices) as a service.

For each of the above services, a description along with use case scenarios and a list of potential contributors to each of the services is provided. Note however that the delivery of the services and the nature of their integration in the platform (e.g., as simple description, as a simulated service or as an on-line service) will depend on the evolution of the project's results. To this end, an update of this specification document will be provided in M18 of the project, along with the initial launch of the platform, which is one of the main targets of work package WP7.

TABLE OF CONTENTS

List of Tables

List of figures

1. Introduction

1.1. Scope and Purpose of the Deliverable

FINSEC is developing a platform and solutions for integrated (cyber/physical) security in the finance sector. The project will produce a wide range of technical results ranging from simple security monitoring probes, to integrated security platforms and solutions for target sector. One of the main objectives of FINSEC is to provide a market platform for the project's solutions and services for integrated security in the finance sector are aggregated, listed and made available to relevant communities including: academics, security experts, integrators of security solutions, as well as stakeholders of the finance sector. This market platform will boost the project's dissemination and exploitation strategy, through serving as a vehicle for raising awareness and promoting the main results of FINSEC. In this context, WP7 of the project is devoted to the specification, development, launch and operation of this market platform.

As a first step to specifying and implementing the market platform, the present deliverable is dealing with its architecture and technical specifications. In particular, the deliverable specifies the services that the market platform will comprise, how they will be structured in the platform, as well as the main technical guidelines and specifications that will drive their integration within the platform. Special emphasis is paid on identifying and describing the contents of the market platform, given that they will be its main assets. Indeed, as evident in following sections, the technical implementation of the platform does not represent the core innovation of WP7 in general and the market platform in particular. Rather, the main source of WP7's innovation lies in the services that will be provided through the platform, the way they will be offered and promoted and ultimately the community that will be developed around them.

1.2. FINSEC Market Platform: Main Objectives

In most EC funded projects (including H2020 projects and project's supported by structural funds) their website serves also as a main repository of the project's results. The FINSEC DoA foresees however, the development of an additional market-oriented repository of results (i.e. the FINSEC market platform) that aims at serving multiple purposes in-line with the project's innovation and exploitation objectives. In particular, the market platform of the project will be used as a main channel for following purposes:

- **Dissemination and Communication of FINSEC results**: The market platform will make accessible the most important project's results from a single-entry point, which will boost the project's dissemination and communication targets. In practice, the market platform will provide the means for communicating about FINSEC results with a market outlook.
- **Promotion of FINSEC results**: The platform will provide opportunities for generating and distributing promotional material about specific results of the project, including video demonstrations, market-oriented presentations, whitepapers and more.
- **Sales and distribution**: The platform will serve as a channel for future sales and distribution of the project's results. To this end, all results of the project with commercial relevance will be listed along with relevant contact points for additional information, including sales related information. Note that our planning does not foresee the implementation of sales transaction functionalities as part of the market platform, as commercial sales is out of the scope of FINSEC. Nevertheless, the inclusion of such functionalities for selected outcomes of the project in the market platform is likely to be considered as future work as part of the exploitation phase of FINSEC.
- **Joint Exploitation Activities**: The platform will provide a forum where all FINSEC partners will be able to collaborate for the exploitation of the project's results. It will allow partners to offer services in-line with their individual exploitation strategies. However, it will also greatly boost the

project's joint exploitation strategy, since it will become the place where joint foreground could be promoted and exploited by the FINSEC partners.

- **Community Building Mechanism**: A single entry point to the project's results that comprises easy to understand promotional material will provide a sound basis for attracting interested parties and building a community around the project's results. In this context, the market platform could play an instrumental role in realizing and maximizing the project's impact.

Note that serving the above listed purposes is essential for an Innovation Action (IA) like FINSEC, which is destined to produce results with a market outlook, while also pursuing the substantiation of this outlook.

1.3. Methodology

The development of the architecture and the technical specifications of the market platform is a joint effort of the FINSEC partners, which engaged not only the partners that participate in WP7 of the project, but actually all FINSEC beneficiaries and stakeholders. The collaboration of the partners on the market platform took place in the scope of the project's meetings, but also through teleconferences. Overall, the deliverable has been developed based on the following methods and activities:

- **Definition of the scope of the market platform, which took place during M1-M4 of the project**: This activity aimed at specifying the purpose of developing and sustaining the market platform, including the dissemination, promotion and exploitation goals that it is destined to serve. This included the identification of the main contents of the platform and the services that it should offer to interested parties and stakeholders. Moreover, it identified relevant stakeholders (e.g., security experts, financial institutions, security services integrators) which should engage in the platform as part of the FINSEC community. Note that the scoping of the platform took into account a review of the state-of-the-art of similar platform in the financial services industry, and in the security services area. This state of the art review served also as a market analysis linked to the project's market platform.
- **Specify the main functionalities and services of the platform, which took place during M3-M7**: The FINSEC partners have intensively collaborated towards specifying the services that could be offered in the platform. They have created lists of relevant services, which were refined based on the partners' research strategies and business interests. The goal was to reach consensus on the services that can be offered in a professional and sustainable way through the platform. In principle, the partners will offer a mix of training presentations, and services' demonstrations, along with a set of technical components and services. Each of the above items will be sustained and updated by different, (and dedicated), partners of the consortium. Note that the specification of the platform's functionalities included also a set of horizontal (service independent) services, which are typically part of most multi-sided market platforms [1] like the FINSEC marketplace.
- Detail the technical architecture of the market platform, including the structuring of its main **components and services, which took place during M6-M9**: The last part of the development period of this deliverable focused on the technical specifications of the market platform that will drive its actual implementation as part of subsequent WP7 deliverables. It also specified the way the different services will be structured and presented in the scope of the ecosystem portal of the project i.e. the so-called "information architecture" of the platform.

The following figure illustrates the above outlined activities, which are described in subsequent sections of the deliverable. Note that along with the platform architecture and specifications, the present deliverable identified relevant communities for collaboration and dissemination, as part of the marketing and promotion strategy for the project's market platform and overall ecosystem. Moreover, a high-level plan for the launch of the platform is presented as well.

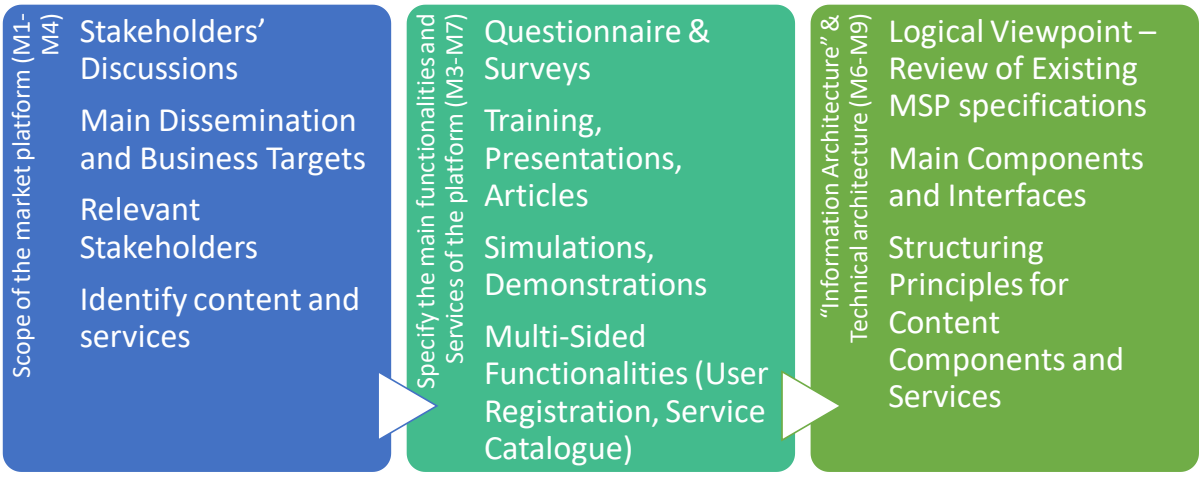

Figure 1: Main Elements of the Activities and Methodology for the deliverable

1.4. Structure and Contents of the Deliverable

Following this introductory section, the deliverable is structured as follows:

- Section 2 presents the review of the state of the art that emphasized on pertinent financial services and cybersecurity services platforms and ecosystems.
- Section 3 specifies the architecture of the market platform in terms of the services that it comprises and how they are structured, but also in terms of the technical specifications of the platform.
- Section 4 presents technical specifications for the FINSEC platform, including technical specifications associated with its multi-side functionalities.
- Section 5 is devoted to the marketing and the plan for launching the platform. It identifies relevant communities and initiatives, with which FINSEC will pursue synergies towards promoting the platform and broadening the project's community.
- Section 6 is the final and concluding sections of the deliverable.

2. Relevant Market Platforms and Ecosystems

2.1. Security as a Service (SECaaS) and Managed Security Solutions Markets

This subsection aims to provide an overview of some relevant services i.e. SECaaS and managed security services [2], [3]. It lists some solutions that are available in the market and analyzes their relevance to FINSEC's platform. A good understanding of the solutions available in the market is valuable for the FINSEC project: It has been taken into account in specifying and designing the project's market platform. Given that the amount of Security as a Service services that are dedicated to the financial sector is limited, this subsection also includes Security as a Service services that could be used by several industries, including in the financial industry.

2.1.1. AlienVault Unified Security Management

2.1.1.1. Overview

The AlienVault Unified Security Management (USM) Anywhere product[1], enables organisations to detect threats from a single cloud platform. The service enables banks and credit unions identify threats and address compliance issues through an all-in-one platform. As a prominent example, the service offers cyber threat detection. It also continuously monitors the network, users and assets to identify suspicious and malicious activity and is capable of automatically detecting new assets and vulnerable systems before attackers can target them. It is also able to conduct threat prioritization by correlating and analysing security incidents from built-in data sources and legacy tools. Through its threat prioritization approach, it is able to focus on the most critical assets and minimize the risk of security breaches and data jeopardization. The product also includesintegrated threat intelligence such that it minimizes the need for having dedicated security analysts that are in charge of researching threats and compliance misalignments in the financial sector. This product is targeted mainly to financial services organisations of small size.

2.1.1.2. Relevance to FINSEC

AlienVault Unified Security Management (USM), emphasizes on threat detection. Although the product is also targeted towards the financial sector, it only focuses on identifying and detecting threats and compliance issues. FINSEC's toolbox alongside other features it will also encapsulate features such as anomaly detection and compliance, based on a more integrated (cyber and physical security) approach. However, the USM product provides a very good example of how FINSEC services could be delivered and could be demonstrated in the market platform. Moreover, USM focuses on Small Medium Enterprises (SMEs), which is an interesting market for FINSEC as well as it can directly benefit from a managed security or SECaaS modality that does not require in-house infrastructure for the delivery.

2.1.2. Oracle Cloud Access Security Broker (Former Pallera)

2.1.2.1. Overview

Oracle's Cloud Access Security Broker (CASB)[2], provides a sophisticated security service to organizations interested in securing their entire clod footprint. The service encapsulates a variety of features including cloud usage, data security, user behavior analytics, and security configuration and

[1] https://www.alienvault.com/products
[2] https://www.oracle.com/cloud/paas/casb-cloud-service.html

automated incident responses. The organization has the capacity to configure the service's settings based on its practices to customize the service with respect to its needs. The service includes data security protection with respect to data visibility (e.g. whether data was accessed, moved, copied etc.), data accessibility (monitors the access rights to information and logs who has used those access rights), and data inspection (integrates with data inspection tools available from cloud service providers to ensure data inspection is conducted where data is stored). Also, regarding cloud infrastructure, the service goes beyond the security issues arising by shadow IT and offers protection for the organization's entire cloud footprint, including all the IaaS, PaaS, SaaS services used by the organization. The service delivers a holistic view of the organization's cloud environment regarding all users and devices. Threat detection is based on user behavior analytics also integral part of the service. CASB builds a baseline of typical user behavior such that it is able to detect when and how users deviate from that baseline. The service also combines predictive analytics to assist the organization to detect and stop an incident before it occurs. In this way, the service allows the organization to detect rapidly threats across multiple cloud services in order to immediately respond and take corrective action.

2.1.2.2. Relevance to FINSEC

The framework to be delivered by the FINSEC project will encapsulate a predictive approach to the security of critical financial infrastructures. Understanding the features offered by Oracles' Cloud Access Security Brokerage regarding the use of predictive analytics for threat prediction assist the requirements elicitation to be used for the design of the Market Platform Architecture. Along the same lines, the fact that predictive analytics features are also detected in other relevant services in the market highlight the need of a variety of industries, including the financial industry, to use this feature in their security services.

2.1.3. Okta

2.1.3.1. Overview

Okta[3] offers authentication services that are relevant to a variety of sectors. To offer enhanced security in user authentication, Okta offers a single sign-on service for users regarding all their web and mobile applications. Its Adaptive Multi-Factor Authentication service is particularly relevant to sectors for which the misuse of authentication mechanisms may pose important threats such as the financial services sector. The service provides secure access to the businesses systems and infrastructure through the use of secure authentication services that are deploy and maintained by the organisations IT administrators. The service, beyond the use of more mainstream authentication mechanisms such as passwords, it also offers the option to use biometric authentication factors (e.g. fingerprints). Overall, the service's features aim to ease employee experience while at the same time ensuring that authentication is presumed securely.

2.1.3.2. Relevance to FINSEC

The secure authentication of employees of financial organisations is particularly important in the financial services sector. However, FINSEC focuses on security monitoring for risk assessment and compliance, rather than user authentication. However, Okta is another paradigm of managed security and SECaaS that will be consulted by FINSEC in order to design the delivery of its services and their promotion through the market platform.

[3] https://www.okta.com/

2.1.4. Qualys

2.1.4.1. Overview

Qualys[4] network security offers prevention, detection and protection on network attacks. It offers an automated network audits such that potential attacks can be detected. In particular, the product performs on-going and always-on assessment of the network, such that it is able to identify irregularities and provide relevant alerts. The system is able to provide tailored alerts with respect to the conditions impacting the organisation's systems, certificates, ports, software etc. The product is also capable of providing insights regarding the network's status in a graphical representation form such that the spotting of anomalies is eased. The platform is accessible directly in a browser allowing the IT managers to gain a complete and continuously updated view of the security status of their IT assets.

2.1.4.2. Relevance to FINSEC

Qualys provides a pool of SECaaS services for IT assets. FINSEC will offer physical security services concerning the protection of the physical infrastructure as well. However, the delivery model of Qualys and its marketing can be taken into account by FINSEC.

2.1.5. WhiteHat Dynamic Application Security Testing

2.1.5.1. Overview

WhiteHat's Dynamic Application Security Testing[5] assists organisations in detecting and fixing the security vulnerabilities of the organisation's website. The service continuously scans an organisation's websites for thigs like code changes which are then automatically detected and assessed. In this way, information about new vulnerabilities that may arise are collected and relevant alerts are issued. The tool is capable of validating vulnerabilities detected. It also offers real time analysis of the security status of all the websites of the organisations such that IT managers can monitor it and take action in cases that security breaches arise.

2.1.5.2. Relevance to FINSEC

WhiteHat's services provide a concrete example of managed services that can protect website and other IT servers of an organization. It offers a notion of plug-ins that boost modality. This modularity concept will be considered in the design, demonstration, promotion and (in few cases) offering of the various modules of the FINSEC platform as plug-ins.

2.2. Relevant Communities Linked to the Project's Partners

In addition to integrating and offering services in the project's market platform, FINSEC will aim at developing an ecosystem of relevant stakeholders around it. In the following paragraphs we outline some communities directly linked to the project, which can serve as a basis for bootstrapping the development and the expansion of the project's community. These communities are affiliated to the project's partners, while being relevant to security and/or financial services. Note also that members of these communities may participate as both demand-side and supply-side participants in the market platform i.e. using/accessing and offering/providing services respectively.

[4] https://www.qualys.com/
[5] https://www.whitehatsec.com/

2.2.1. Finance Innovation[6]

2.2.1.1. Overview

Finance Innovation (FI) is an innovation cluster for the French financial sector. It was founded in 2007 by the French Public Authorities, and has ever since undertaken a wide range of projects that address economic, societal and environmental challenges in the service of growth and employment. FI has 500 members, including innovative SMEs, bank and insurance corporations, universities, research labs and public authorities. FI's mission is to key barriers and opportunities in the financial ecosystem i.e.: (i) Promote and support the French Fintech ecosystem locally and internationally, while building bridges with the other Fintech hubs; (ii) Advocate for a democratic and inclusive financial services industry; (iii) Support SMEs of the territory in their search for capital and funding; (iv) Attract greater investment.

2.2.1.2. Links to FINSEC Consortium

ORT is closely collaborating with FI in several projects. Hence, it will facilitate liaisons with FI towards promoting the FINSEC services and its result to FI's members. Initial discussions have focused on the delivery of courses of the Digital Finance Academy on security/cybersecurity to FI members and affiliated stakeholders. Moreover, joint dissemination efforts such as stakeholders' workshops where the FINSEC market platform can be promoted will be also planned.

2.2.2. Digital Finance Innovation Lab and Code-n[7]

2.2.2.1. Overview

GFT has a leading role in two innovation initiatives that provide opportunities for synergies associated with the FINSEC market platform. These two innovation initiatives include: (i) The Digital Finance Innovation Lab (DFiL), which is joined by a consortium of research centres, banks and financial institutions in Italy with GFT in a leading role; (ii) CODE_n, which is a leading cross-industry innovation hub for entrepreneurs, ambitious business founders, and established companies. GFT is the founder of CODE_n, which provides a stage for new business models and digital trends, enriched by an international network of startups and corporations (see: https://www.gft.com/int/en/index/discovery/innovation/code-n/).

2.2.2.2. Links to FINSEC Consortium

FINSEC will leverage its collaborative links to these two innovation initiatives in the following directions: (i) Joint organizations of courses, workshops and other dissemination activities; (ii) Promotion of the FINSEC services to DFiL participants for further development, deployment and commercialization in the scope of real-life cases.

2.2.3. Hellenic Blockchain Association[8]

2.2.3.1. Overview

Members of the FINSEC team are participants to the Hellenic Blockchain Association that is destined to promote blockchain adoption and foster the development of the blockchain ecosystem in Greece.

[6] https://finance-innovation.org
[7] https://www.code-n.org/
[8] http://blockchain.org.gr/home/

2.2.3.2. Links to FINSEC Consortium

FINSEC will collaborate with the Hellenic Blockchain Association towards promoting its blockchain related products and services, notably the blockchain developments for sharing security data across different banks and financial institutions.

3. Market Platform Architecture

3.1. Solutions and Services

In following paragraphs we provide an overview of the services that will be listed in the market platform catalogue and/or integrated in the platform. At this stage these services are based on some reasonable assumptions about the nature and the functionalities of the FINSEC services that are under development. Moreover, the initial exploitation and dissemination intentions of the partners have been considered in terms of their interest to promote, support and sustain these services. Nevertheless, most services are currently under development and therefore their final integration of in the FINSEC platform might deviate from the specifications given in this section. Likewise, the list of services is preliminary as more services are likely to be included and others could be removed as well during the actual development, launch and evolution of the market platform. Furthermore, the lists of participating and contributing partners are likely to be enhanced or revised in the next version of this deliverable.

3.1.1. SECaaS Simulation and Demonstration

This service is a data-driven demonstrator of SECaaS services that will be integrated in the FINSEC platform. The purpose of the demonstrator will be to illustrate and to showcase the security analytics algorithms of the project. The operation of these algorithms could be based on sample simulated security datasets about one or more assets of a financial organization [4]. The service is illustrated in the following table.

Service Parameters	Description
Description	On-line demonstrator of the security analytics capabilities of the FINSEC platform based on selected data analytics algorithms (e.g., machine learning algorithms).
Stakeholders' Involved	Security Experts & Consultants, End-Users (Financial Institutions)
Indicative Use Scenario	1. A Security expert or consultant uploads (simulated) security data about one or more assets (e.g., machines, access gates, ATM) of a financial institution. The data can for example be available in a text file (e.g., CSV or XLS formatted) unless the data analytics algorithms of the next step involves processing of multimedia data. 2. A FINSEC data analytics algorithm processes this data and extracts security related information about the asset (e.g., a vulnerability or risk). 3. The extracted information is visualized in a simple dashboard, which allows user to see the operation of the SECaaS through a simple example.
Consortium Partners Involved	GFT, CNR, ORT, UTI, LIB
Related WPs	WP3 (where algorithms are developed) and WP5 (where algorithms are integrated in the FINSEC platform and SECaaS services)

Table 1: Overview of the SECaaS Demonstrator Service

3.1.2. Video Demonstration of FINSEC Security Services

Video demonstrators of the FINSEC services (i.e. the SECaaS services) will be integrated in the FINSEC market platform for the purpose of promoting the project's results and illustrating their use in a financial services context. The following table provides information about the video demonstrators to be included in the market platform.

Service Parameters	Description
Description	A series of videos demonstrating one or more SECaaS services of the FINSEC project.
Stakeholders' Involved	Security Solution Integrators, Financial Institutions and Financial Organizations
Indicative Use Scenario	Security experts within a financial institution or bank access video demonstrations of a risk assessment services in order to understand its operation and capabilities.
Consortium Partners Involved	Z&P, GFT
Related WPs	WP7/WP8 (as the videos can be classified as dissemination materials)

Table 2: Video Demonstrators of FINSEC SECaaS Services

3.1.3. Risk Assessment Services

This service will be based on the risk assessment functionalities that will be developed in the scope of work packages WP4 and WP5 of the project, over the FINSEC data collection and based on one or more existing risk assessment engines of the partners (such as the IBM's and ATOS' RAE services). The risk assessment services will be accessible based on a SECaaS modality. Within the FINSEC market platform a description of the service will be provided along with information about its availability and accessibility. This is illustrated in the following table.

Service Parameters	Description
Description	A description of the FINSEC Risk Assessment Services, including information about assets that can be assessed, the different levels of risk that will be produced by each assessment, as well as the list of relevant/applicable actions to be considered.
Stakeholders' Involved	Security Experts, Security Solution Integrators, Financial Institutions and Financial Organizations
Indicative Use Scenario	An organization provides datasets to a service in the FINSEC market platform based on a specified format. The platform provides a textual or visual output comprising an assessment of the risk of assets contained in the dataset.
Consortium Partners Involved	ATOS, IBM

Related WPs	WP4 / WP5 (where the risk assessment services are developed and integrated based on the SECaaS modality).

Table 3: Overview of the FINSEC Risk Assessment Services

3.1.4. Security Knowledge Base

One of the main results of the project will be the creation of a security knowledge base that will comprise information and knowledge about security threats in the finance sector. This database will be based on existing databases such as the NIST/CVE database, yet it will also contain additional value-added information for use in the finance sector. In the scope of the FINSEC market platform, information about this knowledge base will be provided, including the possibility of accessing some of its elements/files. The concept is illustrated in the following table.

Service Parameters	Description
Description	A description of the FINSEC Security Knowledge Base, including information about its purpose, contents and use, but also access to various feeds (e.g., vulnerabilities feeds) in popular formats (like JSON and XML).
Stakeholders' Involved	Security Experts, Security Solution Integrators, Financial Institutions and Financial Organizations
Indicative Use Scenario	A security solutions integrator wants to leverage information from the FINSEC security knowledge base in its service. The integrator can visit the FINSEC market platform in order to access information about the security knowledge base, including files and documentation for integrating it in his/her application.
Consortium Partners Involved	CINI
Related WPs	WP3 (where the security knowledge base is developed)S

Table 4: Overview of the Security Knowledge Base Service in the FINSEC Market Place

3.1.5. Training ("Digital Finance Academy for Security")

FINSEC will develop and make available training materials (e.g., presentations, webinars) for security in the finance sector, covering cybersecurity, physical security, relevant regulations, as well as illustration of the FINSEC results. Some of these training materials will be made available with a public licence in order to form a freely available course for stakeholders in the finance sector. Moreover, the consortium will consider the development of additional course material and courses as a paid business-to-business service. All relevant courses and materials will be streamlined with existing efforts and activities of some partners (notably GFT, ORT and INNOV) towards the establishment of a digital finance academy (DFA). In this context, security courses for finance will be offered in conjunction with other courses covering digital finance/banking and FinTech. FINSEC will therefore offer the security part of the partners' on-going DFA project, which can be conveniently characterized as a "Digital Finance Academy for Security". The following table provides an overview of the training services that are envisaged to be offered as part of the FINSEC market platform.

Service Parameters	Description

Description	On-line Training materials structured into courses concerning security for digital finance critical infrastructures
Stakeholders' Involved	Security Experts, Financial Institutions (end-users), Security Solutions Integrators, Researchers'/Academics (all as either providers of training materials or trainees/users of the courses)
Indicative Use Scenario	Employees of a security integrator register with FINSEC market platform and access the training services / courses of the "Digital Finance Academy Training on Security".
Consortium Partners Involved	ORT, GFT, INNOV
Related WPs	WP7 & WP8 where training materials will be developed to support the project's training activities.

Table 5: Overview of the Training Services in the FINSEC Market Platform

3.1.6. Security Consulting Services

FINSEC will provide consulting services to financial institutions and/or integrators of security solutions that have an interest in implementing and fully leveraging integrated security based on the technologies and solutions implemented in the project. The consulting services will be therefore centered round the FINSEC solutions and technologies as added-value outcomes for enhancing the security of the critical infrastructures of the finance sector. The following table illustrates the nature and envisaged content of the consulting services of the project.

Service Parameters	Description
Description	Consulting services associated with the implementation/integration of solutions that protect both physical and cyber assets. These services will span the areas of solution design, integrated information modelling, design/delivery of risk assessment functionalities, identification of applicable laws and regulations for the infrastructures at hand, as well as techno-economic evaluation of integrated security solutions. The above list of consulting services is not exhaustive.
Stakeholders' Involved	Financial Institutions, Banks, Security Solutions Integrators
Indicative Use Scenario	A financial institution is interested in breaking its technical and organizations silos associated with physical and cyber security. It resorts to partners of the FINSEC consortium through the FINSEC market platform, as providers/designers of cost-effective and robust integrated security solutions. As part of the latter, consulting on the architecture of the solution and integrated modelling of assets and threats is provided.
Consortium Partners Involved	GFT, HPE, Z&P, UTI

Related WPs	WP7/WP8 as it is implemented for integration in the market platform (WP7) and as part of the exploitation strategy of the project (WP8).

Table 6: Overview of the Consulting Services provided/listed in the scope of the FINSEC Market Platform

3.1.7. Probe Demonstrator

FINSEC will implement and provide a number of probes that will delivery security information about cyber and physical assets to the FINSEC platform. The consortium will endeavor to provide on-line and/or off-line demonstrators as part of the FINSEC market platform. Relevant information about these demonstrators is provided in the following table.

Service Parameters	Description
Description	On-line (cloud-based) demonstration of a probe and/or off-line demonstrator based on video or animation. The demonstrator will illustrate how information about assets is delivered, including the semantics of the information of the probes
Stakeholders' Involved	Probes Providers (e.g., FUJITSU), Financial Institutions / End-Users, Security Solutions Integrators
Indicative Use Scenario	A financial institution (e.g., bank) access the demonstrator of a probe (e.g.., CCTV) in order to raise its awareness about the operation of the probe and in order to assess it appropriateness for the organization's needs
Consortium Partners Involved	UTI, FUJITSU, ATOS, LIB
Related WPs	WP4 (where Probes are implemented)

Table 7: Information about Probe Demonstrators

3.1.8. Standards and Regulatory Support Forum

Standards and regulations play a key role in the design and implementation of security services for the financial sector. As part of the market platform of the project, the consortium will stress the importance of standards and regulations for the integration, deployment and operation of the FINSEC technologies. To this end, a forum for discussion and consultation on regulatory issues and standards will be established and integrated in the market platform, as illustrated in the following table.

Service Parameters	Description
Description	A forum for discussion and consultation on the compliance of security systems for the finance sector to standards and regulations.
Stakeholders' Involved	Regulatory Experts, Security Experts, Financial Organizations
Indicative Use Scenario	Participants to the market platform ask questions about the adherence to a specific standard or regulation (e.g., GDPR) in the scope of FINSEC solutions. The questions are posted in the forum and are answered by other participants or regulatory experts.

Consortium Partners Involved	GFT, Z&P, INNOV
Related WPs	WP2 (where an initial analysis of applicable regulations and standards has taken place i.e. in D2.2), WP7

Table 8: Information about the FINSEC Regulatory Support Forum

3.1.9. Integration Services

As an exploitation measure, the consortium will offer integration services for the FINSEC technologies. They will be advertised through the market platform of the project, as outlined in the following table.

Service Parameters	Description
Description	The consortium will offer integration services to financial institutions and solution integrators that would like to benefit from FINSEC components and technologies such as probes, data analytics algorithms and SECaaS services.
Stakeholders' Involved	Financial Organizations (End-Users), Integrators of Security Solutions for the Financial Sector
Indicative Use Scenario	A financial organization is able to access information about the integration services provided by FINSEC partners. This information will be accessible through the "services" section of the FINSEC market platform.
Consortium Partners Involved	GFT, HPE, UTI, SiLO
Related WPs	WP5 (which is the integration workpackage of the project), WP7

Table 9: Integration Services in the FINSEC Market Platform

3.1.10. Open Datasets for Financial Services Security

The FINSEC market platform will provide datasets that will facilitate researchers, academics, data scientists and integrators of security solutions to experiment with data analytics and machine learning algorithms for security applications. The following table illustrates the use of these datasets.

Service Parameters	Description
Description	Datasets of cyber and/or physical security information for assets of financial organizations will be integrated and made available through the market platform based on a public/open license and in popular formats (e.g., XML, CSV, JSON).
Stakeholders' Involved	Financial Organizations, Data Scientists, Academics/Researchers, Security solution integrators etc.
Indicative Use Scenario	A researcher intends to experiment with data analytics and machine learning models for security in critical infrastructures. He/she is able to download relevant datasets from the FINSEC market platform based on a public/open license.

Consortium Partners Involved	SIA, WIRE, ALPHA, NEXI, HDI, LIB
Related WPs	WP6 (where data will be provided for the FINSEC pilots), WP7

Table 10: FINSEC Open Datasets

3.1.11. FINSEC Platform as a Product

The ultimate integrated foreground results of the project will be the FINSEC platform. The market platform of the project will provide information about the FINSEC platform as a whole and the modules that it will comprise. This information will aim at acquainting the community with the components of the platform and how these can be used/deployed in the scope of a turnkey solution. The following table provides more information about this service of the market platform.

Service Parameters	Description
Description	A detailed presentation of the FINSEC Platform as product, including most of its features and functionalities, also with links to video demonstrators
Stakeholders' Involved	Security Integrators, FINSEC Components/Technologies Providers, Financial Organizations (End-Users of FINSEC Solutions)
Indicative Use Scenario	A security integrator access the market platform in order to find information about the structure, the deployment configuration and the components of the FISNEC platform.
Consortium Partners Involved	GFT, UTI, HP
Related WPs	WP5 (where the FINSEC platform is integrated), WP7

Table 11: FINSEC Platform as a Product

3.2. Information Architecture

Given the above listed services, the FINSEC market platform will comprise a portal that will serve as a single-entry point to any of the services. The information on the portal will be structured in a simple and intuitive way that will facilitate navigation and use of the services. As a minimum, the portal will comprise the following sections:

- **Home Page**: This is the initial landing page of the portal, which shall provide general information about the purpose and scope of the market platform, including information about its linking to the H2020 FINSEC project and the consortium.
- **About FINSEC**: This section will provide more details about the FINSEC project and its results, including links to the project web site, information about its objectives and sustainability plan.
- **Solutions**: This section will comprise information about the solutions of the project, such as the FISNEC platform and the FINSEC risk assessment solutions.
- **Services**: This section will provide information about accompanying services offered by the consortium, including for example consulting and integration services.
- **Demonstrations**: This section will provide access to the various demonstrators that will be integrated in the market platform such as demonstration of probes and video demonstrations of SECaaS Services.

- **Training**: This section will be devoted to the training services of the project, including the "Digital Finance Academy for Security". It will provide access to courses and their materials.
- **Blog/News**: This section will provide access to blog posts and other news items, including news associated with the FINSEC ecosystem (e.g., participation to events and exhibitions).
- **User/Login**: This section will manage user registrations to the FISNEC market platform, as well as the login process for registered users. It will be an important section for community building, which will be boosted by the fact that several of the project's solutions and services will be accessible to registered users only. The latter is expected to support the community building efforts of the project's partners.

The structure of the information that will comprise the above-listed sections is depicted in the following figure. It will serve as a basis for specifying the site map of the FINSEC portal, which will drive the development of front end of the market platform.

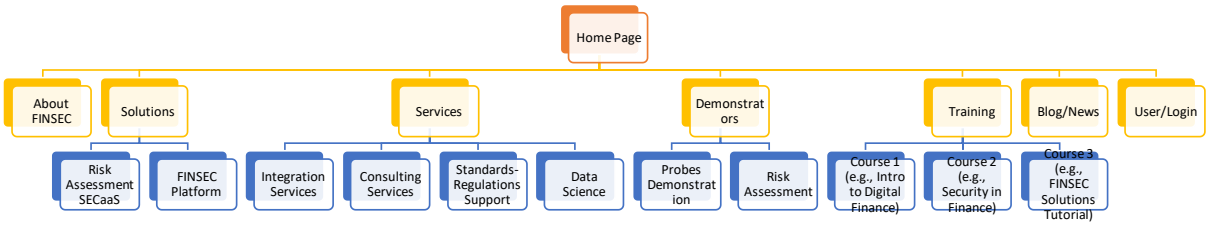

Figure 2: FINSEC Market Platform Portal Site Map

3.3. Technical Architecture

The marketplace platform will be architected and implemented using a dynamic web-based application. It will be accessible through a web browser. The server will process independently each request from the users and generate the corresponding response each time. For the needs of the application, a database will be used in order to store user-specific content and dynamic content. The marketplace will communicate to a cloud API in order to dynamically request demo applications deployment and provide platform specific data.

The technical architecture will be based on a standard multi-tier (i.e. three-tier) architecture with some extensions.

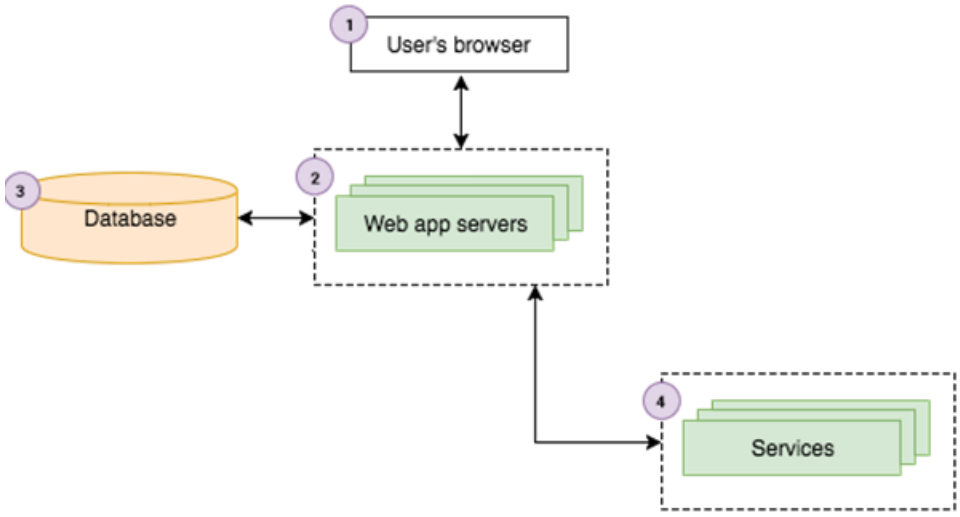

Figure 3: High Level Overview of the Technical Architecture of the FINSEC Market Platform

The components of this architecture are:

1. The Presentation Tier – Frontend Application

This part of the application is responsible for the graphical representation of the backend-generated content into the web browser of the end user.

2. The Application Tier – Backend Application

This application is responsible for the processing of the request and the generation of user-specific content.

3. The Database Tier – DB

The database is responsible to store any dynamic content (containing user accounts, blog posts, provided services etc.)

There also will be a communication with external services (most likely to a FINSEC Cloud platform i.e. a cloud platform used by the project) in order to provide content and services. The latter will be able to support both demonstration services, but also pre-production (e.g., beta operation) services, in case the latter is deemed necessary.

The actual technical architecture in the production environment will have some addition in order to give performance and reliability to the marketplace platform.

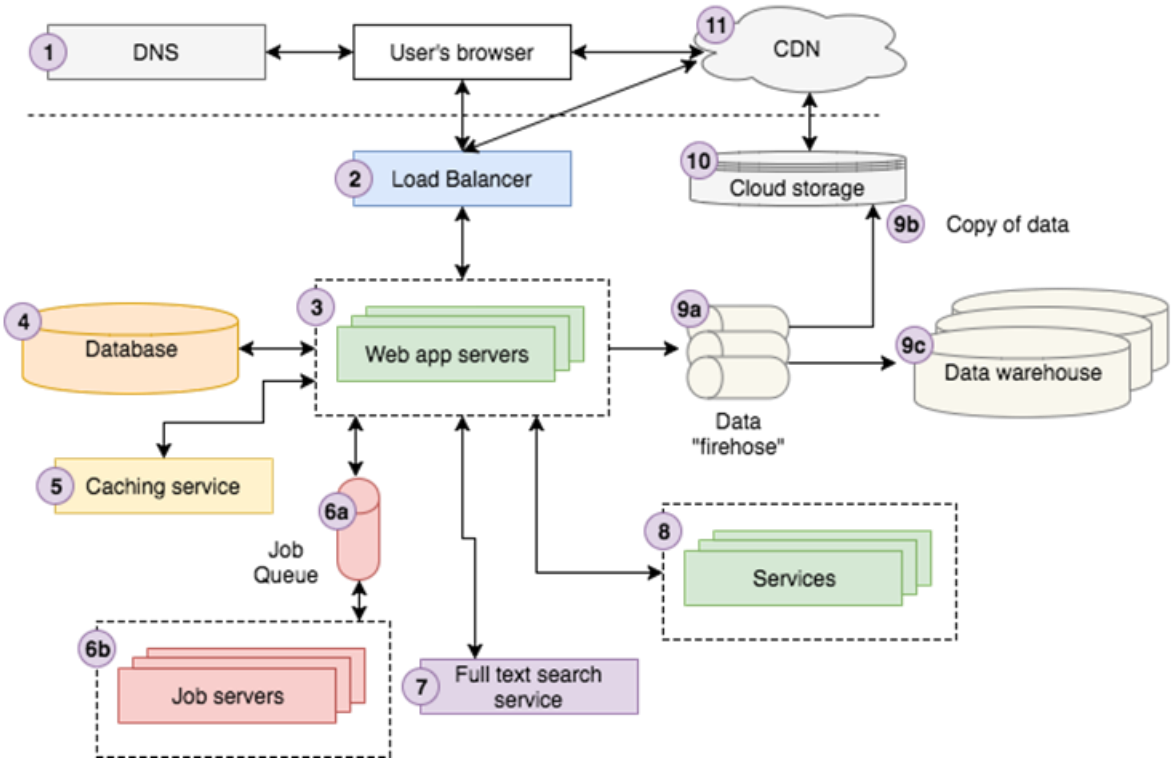

Figure 4: More Detailed Logical View Level Overview of the Technical Architecture of the FINSEC Market Platform

Figure 4 depicts some additional architectural components and describes a complete communication flow within the marketplace platform. Below is a short description of the components:

- **Public DNS Server**: This is the network discovery service of the client, which enables it to get access to the application.
- **Load Balancer**: This service handles all the requests and forwards them to appropriate servers thus allowing scaling of the performance of the marketplace and the applications that are supported by it.

- **Backend Application**: This service (part of the Web apps in the figure) handles all the "business logic" processing and communicates with all of the rest architecture components.
- **Database**: The database is responsible to store any dynamic content (e.g., containing user accounts, blog posts, provided services etc.).
- **Caching**: This service provides a caching mechanism in order to keep an index of pre-calculated data and it gives a significant increase in performance.
- **Jobs Scheduling**: This comprises two components/services, namely:
    - **Job Queue**: The Queue allows an asynchronous execution of the jobs, allowing first-available/first-serve in order to efficient utilize as much available resources as it can.
    - **Job Servers**: The separation of the job servers allows on the one hand the independence of the running jobs and in the other hand allows to resource limit and scale vertical the performance.
- **Search Service**: This service is responsible to implement searching algorithms within the available context. It could be part of the pool of services that is labelled as the eighth component in the figure.
- **External Services**: The external services provide access to the FINSEC services that need them.
- **Data Services**: Data services include:
    - **Data Streaming**: This service allows the production and the consumption of the data in a transparent and efficient way.
    - **Data Replicas**: This service allows the distribution of the data to multiple destinations of storage.
    - **Data warehouse**: The data warehouse is a data vault with a copy of the platform data.
- **Cloud Storage**: This component handles the data and the distribution and makes them available to the users (through the CDS network).
- **Content Delivery Network (CDN)**: This component allows the efficient access of the platform data provides multi-regional/high-available storage networks.

The technical architecture is developed in line with the microservices approach [5]. Hence, it will be able to be deployed in a container and in-line with Service Oriented Architecture (SOA) principles. The scaling of all the architecture components will be possible both vertically and horizontally for each one of its components i.e. it supports scale-up and scale-out at the component level. Note also that the major public Cloud providers provide most of the architecture's components, which allows transparent deployment/scaling functionalities without any service interruptions. Moreover, the architecture will provide support for a combination of public cloud services – such as Amazon RDS, Elastic Load Balancing, Amazon ElastiCache, Route 53, and Amazon Simple Storage Service from Amazon or Azure SQL Database, Content Delivery Network, Azure DNS, Load Balancer, Storage and Azure Search from Microsoft Azure. Hence, most of its application components will be provided as a service.

The above-listed technical specifications ensure:

- Support for the deployment of all the services that are listed in the previous paragraphs, as well as of their content.
- Scalability of the architecture as needed in order to support access to the market platform by a large number of users.
- Integration with third party cloud services, which will provide flexibility for all providers of components and services. In particular, component and services providers will have the opportunity to deploy their service in a public cloud services provider and accordingly integrate it seamlessly to the FINSEC market platform.

4. Technical Specifications

4.1. Multi-Sided Platform Overview

In-line with the DoA the FINSEC market platform is destined to be a multi-sided platform (MSP) i.e. a platform that will bring together multiple stakeholders from both the demand (i.e. end-users of security solutions) and the supply (i.e. providers of security solutions) sides. As such, the FINSEC market platform will provide a range of functionalities that are standard in multi-sided market platforms. On top of these functionalities we will integrate the content and tools that comprise the services and solutions listed in the previous section.

4.2. User Registration and Management

The FINSEC MSP should offer user registration functionalities. Several of the FINSEC solutions and services will be accessible to registered users only. To this end, the platform should offer user registration functionalities, as well as functionalities for managing users. The user registration and management shall be subject to the following specifications:

- The User Registration process should collect basic information about registered users including first name, surname, job function, affiliation and e-mail.
- Alternative one-click ways for user registration (e.g., register via LinkedIn, register via Google Account) should be supported to ease the registration process.
- Information collection and management should be in-line with the GDPR regulation. User's consent should be solicited for all communications with the users of the MSP.

4.3. Services Catalogue

The FINSEC MSP should offer a catalogue of the various solutions and services. This is a typical feature of the market platform. In the scope of FINSEC the term service includes also the solutions and training modules that will be accessible. In particular:

- The MSP shall include a database of services, including a full description of the service offering using text and media (e.g., images, video).
- The MSP shall provide functionalities for managing the service catalogue, including additions and updates to the information of a service,
- The services catalogue shall be managed by an administrator/authorized user/role.

4.4. Third-Party Services Management

In the early stages of the market platform's development and launch, members of the FINSEC consortium will provide the content and services of the FINSEC platform. In latter stages, the project will enable third-parties to participate in the platform as supply-side stakeholders i.e. providers of services such as training services or security analytics components. To this end, the MSP should support:

- Authorization of third-parties to update the service catalogue.
- A workflow of review and approval of third-party services by authorized consortium members. This will differentiate the inclusion of services from third-parties from the inclusion of services from consortium members.

4.5. Service Reviews and Ratings - Localization

As part of the service management and the service catalogue, the MSP should support the review and rating of the services. However, reviews and ratings shall be optional i.e. it should be possible to have services/solutions that cannot be rated or reviewed in the scope of the MSP. Note also that the MSP shall provide support for an international environment through appropriate localization of the services including currency and language support.

5. Plan for Marketing, Promotion and Ecosystem Building

5.1. Streamlining with Dissemination and Communication Activities

The promotion and marketing of the FINSEC marketplace will take advantage of the project's dissemination and communication activities. In particular, we will make sure that the marketplace's URL and content items will be communicated as part of the project's communication activities and channels, including newsletters, social media posts, stakeholders workshops, presentations in conferences and workshops, publications and more. A detailed presentation of the project's dissemination activities and plans is beyond the scope of this document, as this presentation can be found in WP8 deliverables. As part of this detailed presentation the project will also identify the marketplace-related content to be published in each of the different channels, along with the frequency of the relevant promotions.

5.2. On-Line Channels

The FINSEC marketplace will be promoted through on-line channels, including social media and social networks like YouTube (through a video) and LinkedIn through posts. In particular:

- **Regular LinkedIn posts will be published,** in all occasions when new content will be added to the FINSEC market platform.
- **All videos and video demonstrations of services in the market platform** will be regularly disseminated via the social media channels of the project including LinkedIn and Twitter.

The promotion of the FINSEC market platform through social media and other on-line channels will be performed in the scope of the dissemination and communication activities of the project, as the latter activities are described in the DoA and the WP8 deliverables.

5.3. Stakeholders' Workshops

In order to build a community around the FINSEC market platform, the project intends to organize several stakeholders' workshops where the FINSEC results and the market platform will be presented and promoted towards stakeholders including financial institutions, security experts, integrators of security solutions and more. A minimum of one workshop is planned in each of the countries of the consortium partners. Note that stakeholders' workshops may serve additional purposes, also providing a basis for further research activities. To advertise these workshops, promotion material will be produced, as it will be detailed in deliverable D8.1 of the project.

5.4. Liaisons with other ecosystems and communities

5.4.1. Other H2020 Projects on the Security of Critical Infrastructures

FINSEC will streamline its promotion and dissemination efforts through the MSP based on synergies with other H2020 projects dealing with integrated security of critical infrastructures, notably synergies with projects awarded in the scope of the same call[9] such as:

- **H2020 DEFENDER (Grant agreement ID: 740898)[10]**, that deals with integrated security in CEI (Critical Energy Infrastructures).

[9] CIP-01-2016-2017 - Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.
[10] http://defender-project.eu/

- **H2020 SAFECARE (Grant agreement ID: 787002),** that provider integrated security solutions for healthcare infrastructures, notably solutions that improve both physical and cyber security in a seamless and cost-effective way.
- **H2020 STOP-IT (Grant agreement ID: 740610)[11],** which emphasizes on the protection of critical water infrastructures, including both their cyber and physical assets and relevant processes.

Based on synergies with the above projects, FINSEC will attempt to expand its ecosystem in terms of both demand and supply chain stakeholders. To this end, it will exploit the common ground with these projects in terms of the provision of integrated cyber-physical solutions.

5.4.2. European Cyber Security Organization[12]

Based on liaisons with ECSO FINSEC will attempt to broaden participation in its MSP, given that some of its results (e.g., knowledge base, training materials) are likely to be of interest to ECSO members. The FINSEC consortium includes partners that participate to ECSO as members and will therefore facilitate relevant liaisons.

[11] https://stop-it-project.eu/
[12] https://ecs-org.eu/cppp

6. Conclusions

This deliverable provided the initial specifications of the FINSEC market platform, including specification of the content of the platform, the services that it will offer and promote and the technical architecture that will drive its implementation. It has also outlined the consortium's initial plans for building a stakeholders' community around the market platform, which are streamlined with the project's dissemination, communication and premarketing activities. Special emphasis has been paid in providing a comprehensive description of the contents of the platform, which will include services descriptions, services simulations, video demonstration of services, forum for discussion of standards and regulations, access to open datasets and more. These services are of diverse nature and could therefore provide risk diversification, which will subsequently increase the chances of success for the market platform. In particular, based on the provision of a rich and diverse set of services, the possibility of attracting a critical mass of interested stakeholders becomes more likely.

Key to the success of the platform will be early launch of the platform and its aggressive dissemination in conjunction with the activities of the dissemination and communication workpackage of the project (i.e. WP8). This was also the main motivation behind specifying the services of the market platform prior to their actual implementation, given that currently their implementation is on-going as part of the technical workpackages of the project. Nevertheless, it is the project's intention to refine the given description of the services in order to ensure that the services to be integrated in the platform match the ambition and the quality of their actual implementation. To this end, a second version of this deliverable will be released along with the initial launch of the platform in M18. Note however that the project will launch the platform based on an initial set of content and services described in Section 3 of this deliverable. Additional services will be integrated as they become available.

Overall, the FINSEC market platform represents a golden opportunity for the project to promote and exploit its results, while at the same time building a community of interested parties around them. This opportunity will be substantiated in other tasks of WP7, notably the platform implementation and the community building tasks.

7. References

1. Hagiu, Andrei and Wright, Julian, Multi-Sided Platforms (March 19, 2015). International Journal of Industrial Organization, Vol. 43, 2015. Available at SSRN: https://ssrn.com/abstract=2794582 or http://dx.doi.org/10.2139/ssrn.2794582
2. Furfaro, A.; Garro, A.; Tundis, A. (2014-10-01). "Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing". 2014 International Carnahan Conference on Security Technology (ICCST): 1–6.
3. Thomas W. Edgar and David O. Manz. 2017. Research Methods for Cyber Security (1st ed.). Syngress Publishing.
4. M. E. Kuhl, M. Sudit, J. Kistner and K. Costantini, "Cyber attack modeling and simulation for network security analysis," 2007 Winter Simulation Conference, Washington, DC, 2007, pp. 1180-1188. doi: 10.1109/WSC.2007.4419720
5. P. D. Francesco, I. Malavolta and P. Lago, "Research on Architecting Microservices: Trends, Focus, and Potential for Industrial Adoption," 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, 2017, pp. 21-30. doi: 10.1109/ICSA.2017.24.