Chapter 5

Information Sharing and Stakeholders' Collaboration for Stronger Security in Financial Sector Supply Chains: A Blockchain Approach

By Ioannis Karagiannis, Konstantinos Mavrogiannis, John Soldatos, Dimitris Drakoulis, Ernesto Troiano and Ariana Polyviou

DOI: 10.1561/9781680836875.ch5

Published in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures* by John Soldatos, James Philpot and Gabriele Giunta (eds.). 2020. ISBN 978-1-68083-686-8. E-ISBN 978-1-68083-687-5.

Suggested citation: Ioannis Karagiannis *et al.* 2020. "Information Sharing and Stakeholders' Collaboration for Stronger Security in Financial Sector Supply Chains: A Blockchain Approach" in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 76–93. Now Publishers. DOI: 10.1561/9781680836875.ch5.

now
the essence of knowledge

Security incidents in the finance sector highlight the need for sharing security information across financial institutions, as a means of mitigating risks and boosting the early preparedness against attacks. To address this issue and enhance the security and trust in the information sharing process, a blockchain-based solution for sharing security information in a decentralized way can be employed. Our earlier research work has reflected on this approach and proposed a reference architecture that incorporated a blockchain-based sharing of security information for critical infrastructures of the finance sector. In this Chapter, we extend this reference architecture by enhancing its collaborative risk assessment approach and a security knowledge database. We then employ an example to provide a demo of the dashboard that has been implemented.

5.1 Introduction

In recent years, we have witnessed a steady rise of cybersecurity incidents against infrastructures of the financial sector, such as phishing, ransomware, and DDoS (Distributed Denial of Service) attacks. These incidents include notorious attacks, which have resulted in significant economic damage, while decreasing trust in financial institutions and questioning their social value. As discussed extensively in the Chapter of this book which introduces the security challenges of the financial sector, the critical infrastructures of financial institutions are vulnerable. Some of the reasons of their vulnerability is the integration between physical and cybersecurity and the connectivity between the different systems and infrastructures. First, there is currently limited integration between physical and cybersecurity. This is because data-driven systems for the security of the finance sector are mainly addressing cybersecurity and ignore physical security systems. As a result, vulnerability assessment, threat analysis, risk mitigation, and response activities are fragmented. However, holistic approaches could assist financial institutions in better addressing security incidents involving both cyber and physical assets of their critical infrastructures. Second, as financial infrastructures are more connected than ever before, attacks are likely to impact other infrastructures and systems in the financial chain [1]. Thus, stakeholder collaboration could largely contribute identifying and alleviating such issues more effectively.

The exchange of security information across collaborating stakeholders of the financial services value chain can be a foundation for security collaboration in the relevant supply chain. In the scope of an integrated security approach, information for both cyber and physical security should be exchanged. This Chapter draws on [2] to extend the proposed blockchain-based system for collaborative security in the finance sector that includes an enhanced collaborative risk assessment approach and the incorporation of a security knowledge database.

5.2 Related Work

Collaboration is considered as one of the key activities in a plethora of European national cybersecurity strategies. Collaboration refers to the enhancement of cybersecurity at different levels so as to encapsulate threats sharing, risk assessment, and awareness raising. This is also reflected in the establishment of formal structures such as Information Sharing and Analysis Centers (ISAC) and Public Private Partnerships (PPP) [3]. In the finance sector, the Financial Services Information Sharing and Analysis Center (FS-ISAC) [4] was also established, as an industry forum for sharing data about critical cybersecurity threats in the financial services industry. ISAC centers support information sharing across stakeholders and assist the related

collaborative workflows, such as those implemented in other sectors of the economy (e.g., the maritime [5] and transport sectors [6]). Collaborative security and information sharing options have been proposed in the literature (e.g., [7]), in order to support and complement conventional risk assessment techniques (e.g., [8, 9]). The rationale of information sharing is to trigger security processes like risk assessment and threat analysis, based on information received from other parties that join the collaborative security infrastructures. Trustworthiness and the security of the information sharing process are the two main obstacles in leveraging collaboration. This is because the use of a centralized database for sharing data involves disadvantages such as the requirement for a trusted third party (TTP) that will assume the ownership and will guarantee the integrity of the shared information. Additionally, it is susceptible to security attacks, which can compromise the shared data.

Financial organizations are overall reluctant to share information and thus avoid to share any information that lies beyond their compliance with regulations. Thus, a decentralized approach could provide solutions for addressing this issue. In particular, the use of blockchain technology could enable financial organizations to share information in a shared distributed ledger in a secure and decentralized way and hence in this way provides distributed trust. Alternative technologies that could be employed include STIX (Structured Threat Information Expression) [10], a protocol developed by OASIS to model cyber threat intelligence. TAXII (Trusted Automated Exchange of Intelligence Information) [11] refers to the application-layer protocol developed by OASIS to exchange STIX data. TAXII runs on top of HTTP and can provide secure connections over SSL (Secure Sockets Layer) if needed. But, TAXII is mainly a communication protocol, and thus, it does not provide storing capabilities. Hence, although it supports both publish-subscribe and client-server topologies, compared to blockchain, it lacks the guaranteed degree of confidentiality. Along the same lines, the alternative of pure P2P networks [12] could not provide a viable solution for sharing financial data. This is because the lack of solid authorization techniques could lead in information compromise, bad connections could possibly produce big network latency, while malicious files or messages can be easily implanted and consumed by other peers. For these reasons, information sharing is nowadays one of the most prominent blockchain use cases in the financial sector [13]. Existing literature provides a thorough analysis on the benefits arising by the use of blockchain technology in the financial sector [14, 15].

5.3 Collaborative Risk Assessment

In the proposed architecture, risks are calculated using specific metrics. These metrics include the vulnerability level, the impact level, and the threat level. Both vulnerability and impact levels were derived from the CVSS scores of the assets'

vulnerabilities detected. The threat level is now a result of events occurring inside the organization and historical information. As a result, the calculations are more precise and are based on the current state of each organization.

Risk configuration is an object that follows the FINSTIX format (see Chapter 3) defined to make the risk calculation process easily adaptable to the needs of each organization allowing them to easily edit calculation triggers, add or remove events from the calculation scope, and, in general terms, enable customization. Essentially, through this object an officer can map events to threats and define trigger thresholds for the risk calculation.

5.3.1 Services

The first step to initialize a risk calculation suite is the creation of a Service. Services are stored in the FINSEC data-tier; hence, the communication with it is critical. In the current platform state, the data tier is protected using basic authentication. To protect the credentials, the username and password are provided as environment variables during the container initialization.

The form creation involves the asset selection as well as the vulnerability definition for each asset. The latter is now leveraged by the introduction of the Security Knowledge Base.

Important information related to a service includes:

- Name—which identifies the service along with the id;
- Description—which provides extra information for the security officers;
- Criticality—which defines the level of importance of the service. This information is important because mitigation actions are sometimes urgent and should be handled immediately;
- Subtype—which identifies the level of exposure (e.g., if the service is part of a supply chain, the subtype value will be "public");
- Service references—which lists the dependency of the current service to other services, either inside or outside the borders of the organization.

5.3.2 Threats

While Services provide the ability to group assets inside the organization, it could be impossible to calculate a risk on them without the detection of threats that may target the service. Likewise, a list of events should be defined. These events affect the level of the threat in real time. Threats are associated with the Service using the risk configuration object. Threat objects must be stored in the Security Knowledge Base. Therefore, the form endpoint of the Collaborative Risk Assessment GUI

(Graphical User Interface) will send a POST request to the deployed FINSEC KB (Knowledge Base).

The key properties of a Threat are:

- Name—identification of the threat;
- Description—details of the threat;
- Domain—cyber or physical;
- Subtype—related to the subtype. Example may be "natural disaster" in case of "physical subtype";
- Impact description—What may happen if the threat if realized;
- Likelihood.

5.3.3 Events

As mentioned before, events play a significant role in the risk calculation process. First, a security officer needs to define event models and then map them to a predefined threat. For instance, an "invalid login attempt" is related to a "SWIFT compromise threat." Consequently, when a probe produces an instance of this model, the Collaborative Risk Assessment platform detects it, and if the trigger value is reached for this specific event, the overall risk of the related threat is re-calculated.

Event details must include the following values:

- Name—identifies the event;
- Description—provides more information about the event;
- Domain—cyber or physical;
- Subtype—main or sub (in case the event is of subtype sub, it means that it is dependent of another parent event);
- Probe reference – defines the probe that produced the event;
- Coordinates—only for event instances;
- Observed references—provide the whole observation (may be pointing to an observable like IP address, binary file, etc.).

5.3.4 Triggers

A key consideration is the conditions that trigger the calculation process. In our approach, the calculation can be triggered in three ways:

- Manually;
- Vulnerabilities of the assets involved have changed;
- Event Instances reach a specified threshold.

The threshold is defined during the risk configuration by the security officer. It is an integer value which currently refers to the detections per day. Thus, when set to the number 3, the risk computation will run after the third detection of the specific event. The same event model may be associated with other threats, with a lighter or more sensitive bound. The threshold value is stored inside the Collaborative Risk Assessment platform's local storage (internally).

5.3.5 Risk Calculations

Figure 5.1 presents a high-level overview of the risk calculation process. For the service to function properly, certain preconditions need to apply. These include the service definition, the threat to event mapping, and the probe to be up and running.

As soon as a probe produces a new event, it is forwarded through the data collector to the FINSEC data layer. The Collaboration Service is connected to the data layer and is "listening" for event instances. After the event detection, the Collaborative Risk Assessment Engine:

- Examines all the Services of the organization;
- For each service, it checks the corresponding risk configuration;
- If the risk configuration does not define a relation of the current service to the event detected, the process is terminated;
- If the risk configuration defines a relation of the current service to the event detected, The Collaborative Risk Assessment Platform fetches the threats related to the event instance as well as all the vulnerabilities of the service (through its assets);
- The vulnerability, impact, and threat levels are calculated internally;
- A new FINSTIX risk object is created and sent to the data layer;
- The object is also displayed in the Dashboard;

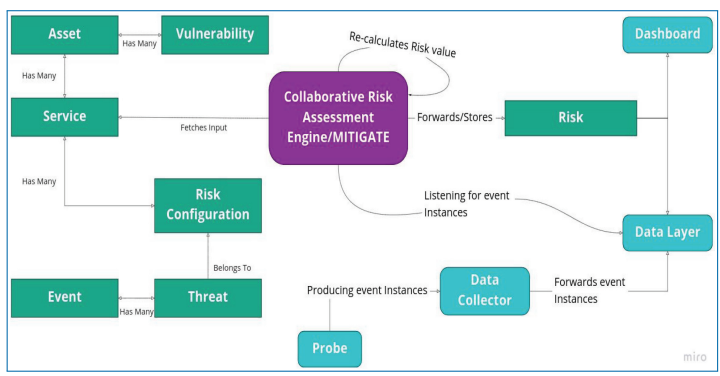

Figure 5.1. Collaborative risk assessment inputs/outputs.

- The logged in security officer checks the new risk calculation details;
- The officer can either approve or decline sharing the object with other stakeholders.

Note that the Collaborative Risk Assessment Engine is developed and customized based on the risk assessment platform of the H2020 MITIGATE project[1].

5.4 Information Sharing Architecture

5.4.1 FINSEC Platform Overview

Aiming to elevate security collaboration in the financial services supply chain, this Chapter extends the proposed information sharing architecture included in [2]. The proposed architecture (Figure 5.2) regards wider platform for financial infrastructures security developed in the frame of the FINSEC H2020 research project. The implementation of the FINSEC platform is based on a state-of-the-art microservices architecture. The platform encapsulates a Big Data system for security analytics, which provides the means for collecting security-related information from physical and cybersecurity systems. The platform can be viewed as a n-tier architecture, with a lower layer (i.e., the edge layer) that interfaces with the actual physical and logical infrastructures. Moreover, it includes several cross-cutting services, which are not confined to providing support to a single tier, but rather support functionalities that may reside in any of the layers of the architecture.

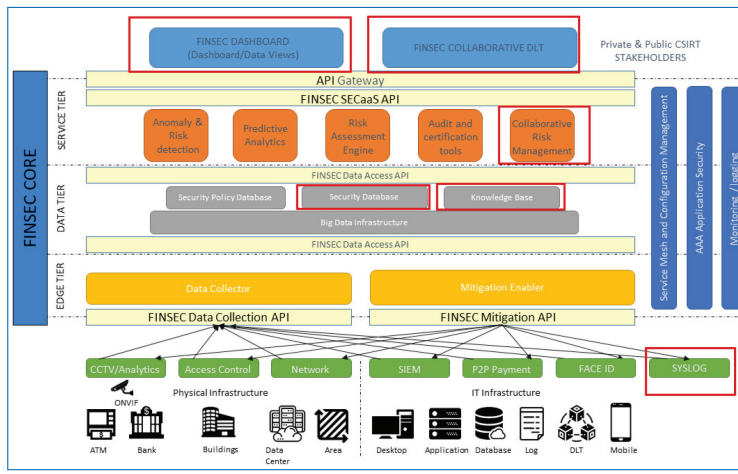

Figure 5.2. Main tiers of the FINSEC platform architecture.

1. https://cordis.europa.eu/project/id/653212

The main tiers of the architecture enable the implementation of the previously presented building blocks and are as follows: (i) The Field Tier is the lower level and includes the probes and their APIs, whose role is extracting raw data from the physical and logical assets to be protected against threats; (ii) The Edge Tier contains the Actuation Enabler and a Data Collection module, which is needed to filter information as it flows towards the upper levels; (iii) The Data Tier is the logical layer where information is stored and organized into three different storage infrastructures, providing consisting data access APIs to all other modules; (iv) The Service Tier is where the kernel applications and the security toolbox will be running (i.e., the security kernel of the platform), able to be used by external applications via proper APIs; (v) The Business Client Applications tier is the layer where end users and business applications may actually get benefits from the platform capabilities. The FINSEC dashboard enables the end users to visually monitor in real time the data and assets managed by the platform, while the (Supply Chain) collaboration module enables the sharing of information with other instances of the platform, including instances deployed in different business organizations.

The core platform encapsulates three tiers: the Edge, Data, and Service tiers, which interact with the external environment with two main interfaces, northbound API and southbound API. (i) The northbound API towards higher level applications (e.g., end-user/business applications) called SECaaS (Security as a Service) API. It represents a consistent and unified view of the individual APIs exposed by the service tier high-level services that represent the "major intelligence" of the platform. The SECaaS API is exposed, and the API Gateway, which is the single-entry point to the system for external clients. Among other capabilities, the API Gateway provides and supports Authentication, Authorization, and Accounting (AAA) services, which conceptually are part of the two cross-cutting vertical modules on the right of the figure (Application Security and Monitoring/logging). (ii) The southbound API interface, consisting of an "Event API" and a "Probe API", allows communication between the Edge Tier and physical and cybersecurity probes.

The SECaaS API is leveraged and invoked by external (north end) Business Client Applications (upper side of the figure). They are outside of the core platform and interact with it only through the SECaaS REST API. Typical examples of business client applications include: (i) The Dashboard application, a web-based GUI used by the profiled end users of the platform; (ii) The Collaboration application, which enables the collaboration of multiple platform instances (data sharing etc.); (iii) Third parties' applications that exploit the capabilities of the platform, such as risk assessment and regulatory compliance applications. The Collaboration application is illustrated in following paragraphs, as it is based on the sharing of data in a blockchain infrastructure.

The Service Tier defines the high-level services that represent the "major intelligence" of the platform. The Service Tier services communicate with each other in three (3) possible ways: (i) Synchronous communications through their REST APIs. In this case, being the services internal to the platform, it is not necessary to use AAA functionalities; (ii) Asynchronous communications via an MQ bus; (iii) Asynchronous communications through the Database Infrastructure.

The collaborative module refers to a FINSEC service aims to provide a collaboration platform on top of a blockchain ledger. The module is deployed as a FINSEC service and provides endpoints to produce and consume FINSTIX messages across organizations. It was originally built to support the Ethereum blockchain; however, efforts are in progress for supporting Hyperledger Fabric. The Open API provided is not expected to change drastically, so the already available endpoints are used to push/pull messages from the blockchain. New capabilities, trust model definition and so on will not pose further issues, and the integration will be seamless. The integration with the collaborative module was rather simple. Instead of the MITIGATE UI, now the information sharing functionality is embedded inside the FINSEC Dashboard.

The security knowledge base essentially utilizes external sources of attacks and vulnerabilities. The most popular of which are NIST NVD and ATT&CK. In case a new asset is stored inside the data tier, it is automatically associated (based on product name and version) with all its known vulnerabilities. This fact eliminates the need of manually importing cyber vulnerabilities for each new asset. Only physical vulnerabilities should now be imported by a security officer. Figure 5.3 presents the Security Knowledge Base architecture.

Additionally, the introduction of the security KB ensures that the vulnerabilities are up to date and updated when necessary. Integrating with the KB required the utilization of its endpoints to persist and fetch information related to threats

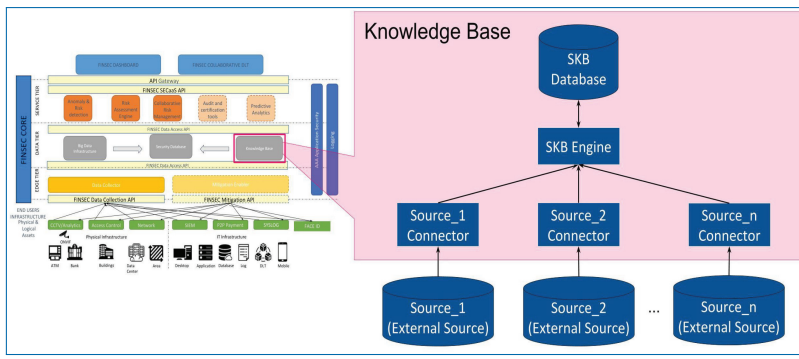

Figure 5.3. Security knowledge base—external sources.

and vulnerabilities. The communication was RESTful, and the authentication was achieved using basic authentication[2] just as the data-layer case.

5.5 Implementation

5.5.1 CRUD Operations—User Interface

Collaborative Security Tools are encapsulated in the FINSEC Dashboard. Thus, all the forms needed are generated through the JSON schemas defined as a FINSTIX domain object. As a result, form validation coupled with form inputs needed for each object are provided for assets, threats, vulnerabilities, services, events and services. Association of domain objects lies on the security officer drag and drop actions, while notifications are still provided to the end user. The efforts were basically to update the FINSTIX schemas, align the Angular versions, code refactoring, so the forms can be automatically generated and other code adjustments on the Dashboard end to enable the full MITIGATE frontend operations.

Figure 5.4 presents the new form layout embedded in the FINSEC Dashboard. Both the validation errors and the input fields are auto-generated from a FINSTIX schema. Figure 5.5 illustrates the association functionality which is achieved with a dual filterable list box. Finally, 5 displays the sharing prompt as realized in the Dashboard.

Figure 5.4. Form layout—dashboard integration.

2. Basic Access Authentication requires a client to provide a username and a password during the HTTP message exchange. https://en.wikipedia.org/wiki/Basic_access_authentication

Figure 5.5. Server room asset creation.

5.6 Demonstrator

Drawing on an example of the behavior of a logged in security officer, in this Section we provide a demo of the proposed approach.

5.6.1 Initialization

As a first step, the security officer logs in and navigates to the Assets page. By clicking the button "Add New," the tool displays a form which must be filled and submitted to generate the new Asset. Figure 5.5 illustrates the generation of the first Asset detected.

Next up, the security officer navigates to the Events page and creates the event models which will be considered for the risk calculations of the current demonstrator (Figure 5.6).

Soon after the event model definitions, the security officer must introduce a Threat. The operation is illustrated in Figure 5.7. Additionally, Figure 5.8 sketches the mapping of the Threat created with the appropriate event models. This step is crucial for the dynamic risk calculations. Note that threats are stored inside the Security Knowledge Base.

Figure 5.6. Invalid Signon event model creation.

Figure 5.7. SWIFT compromise threat creation.

Figure 5.8. SWIFT compromise threat mapping to relevant events.

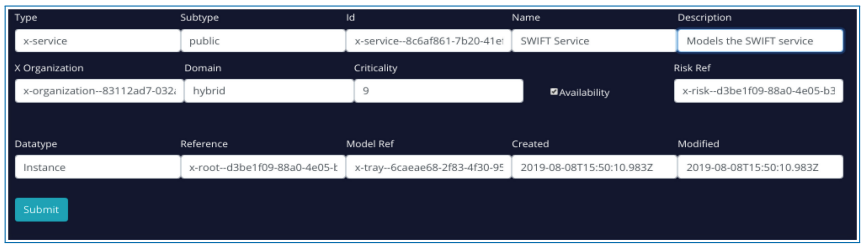

Figure 5.9. SWIFT service creation.

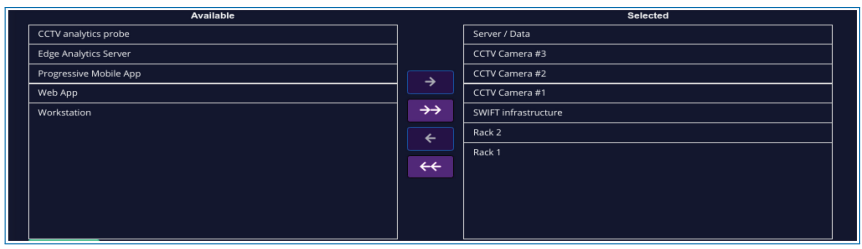

Figure 5.10. SWIFT service asset attachment.

At this stage, the security officer is ready to create the SWIFT service. The pure service information is initially provided. Consequently, the threats are associated with the service, and finally, a risk calculation object is being filled in to define risk triggering conditions. Figures 5.9 and 5.10 illustrate the steps followed.

Inputs/Outputs

All the FINSTIX objects created via the FINSEC Dashboard. These objects will serve as input for the MITIGATE tool. The objects cover both the use cases defined in the SWIFT Service pilot and include the Assets detected, the Event models, the

Threats identified, the Service, and finally the Risk Configuration Object. Additionally, the MITIGATE will listen for Probe events, and thus, these events are also considered input for the Collaborative Risk Assessment Service. Vulnerabilities detected for every asset are used in the risk calculations. They are the building blocks for calculating the Vulnerability and Impact metrics. Using the aforementioned inputs, the MITIGATE platform will produce a risk object which will be available for sharing with other stakeholders. The risk object essentially constitutes the output of the Collaborative Risk Assessment Service.

Demonstrator

As soon as all the necessary input is provided by the Security Officer, the vulnerability constitution is available in the FINSEC Dashboard home page. Figure 5.11 illustrates the vulnerabilities for the SWIFT service pilot, categorized by their domain (cyber/physical).

Figure 5.12 displays the auto-imported vulnerabilities from the Security Knowledge Base, while Figures 5.13 and 5.14 compose a proof that the vulnerabilities detected for the NodeJS server are also defined in the external source (CVE).

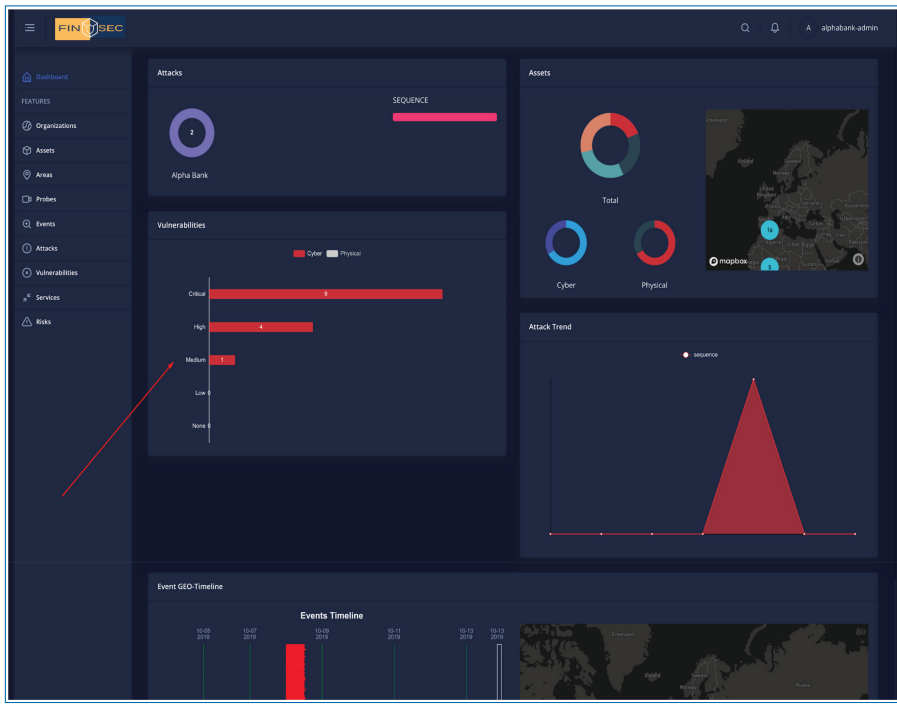

Figure 5.11. FINSEC Dashboard homepage—vulnerability categorization.

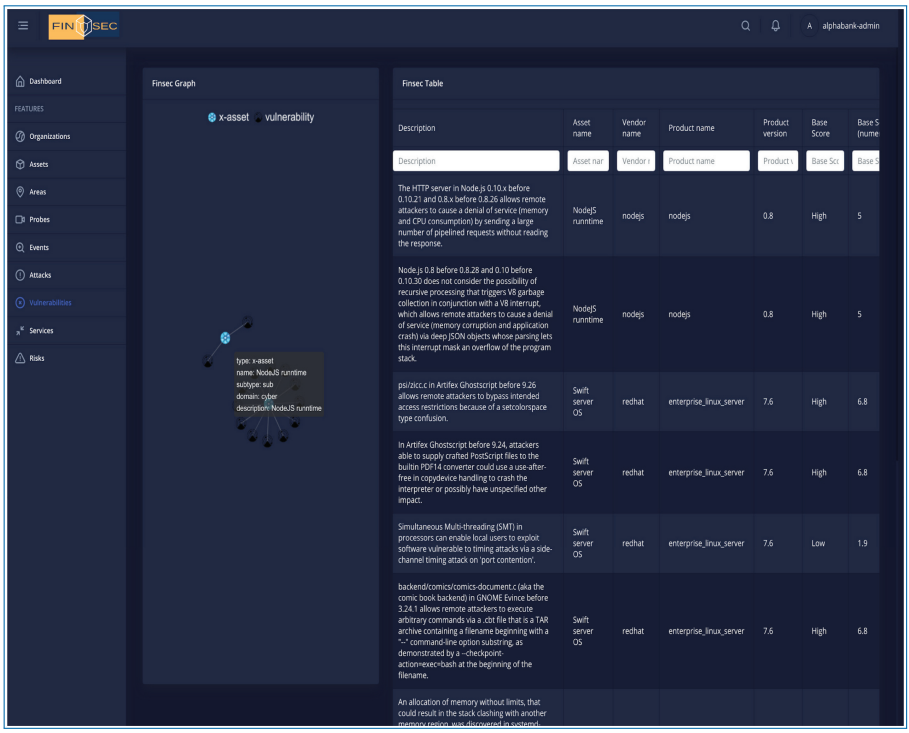

Figure 5.12. Vulnerabilities—auto-imported from the security knowledge base.

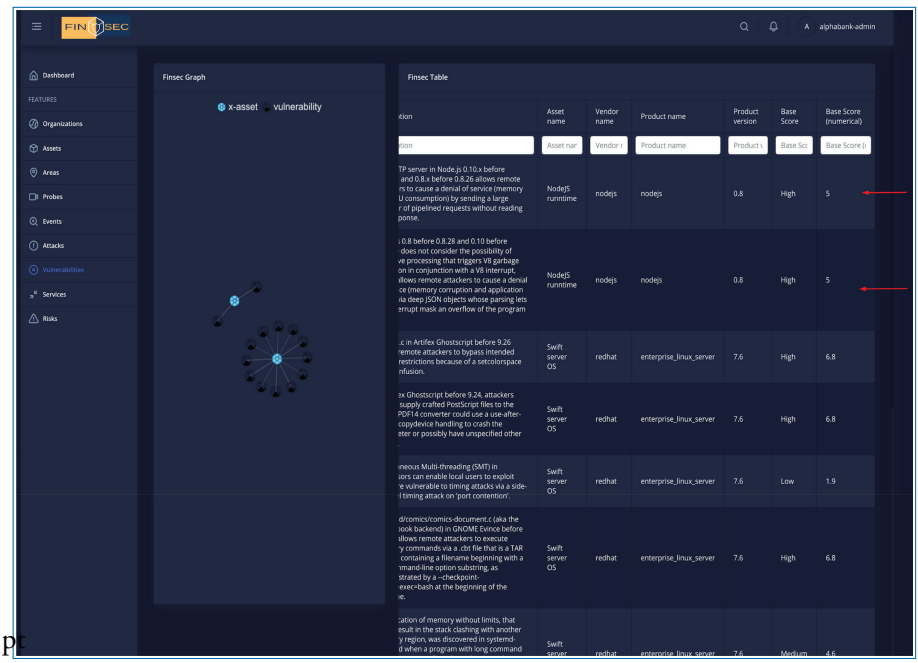

Figure 5.13. NodeJS vulnerabilities detected.

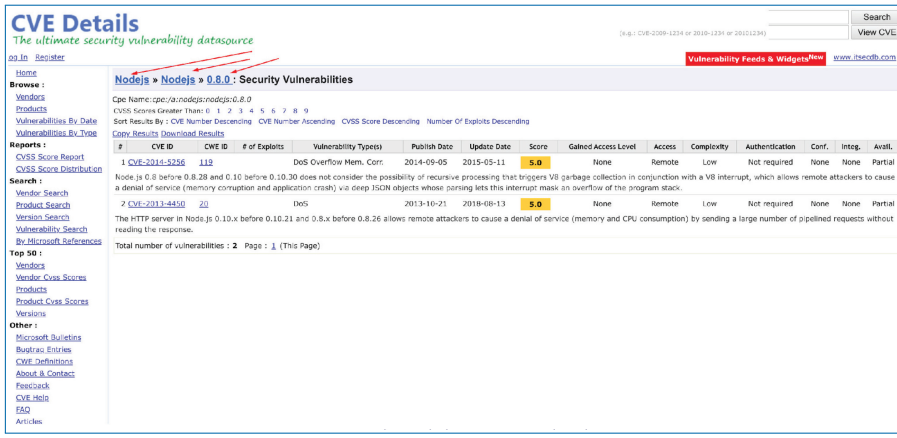

Figure 5.14. CVE vulnerabilities cross check.

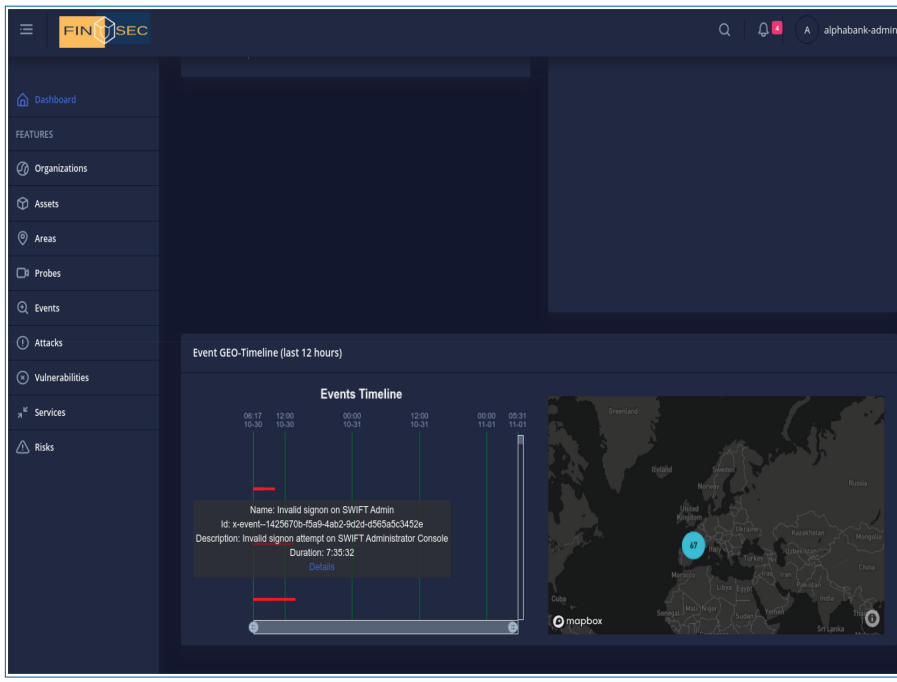

Figure 5.15. Probe events detected.

Figure 5.15 illustrates the Probe events detected. For the specific SWIFT service scenario, they are both the "Invalid Signon Attempt" and the "Submission of SWIFT messages outside working hours."

One notification is displayed on the upper right corner as soon as a risk value is changed. The risk value calculated for the SWIFT service and especially the SWIFT

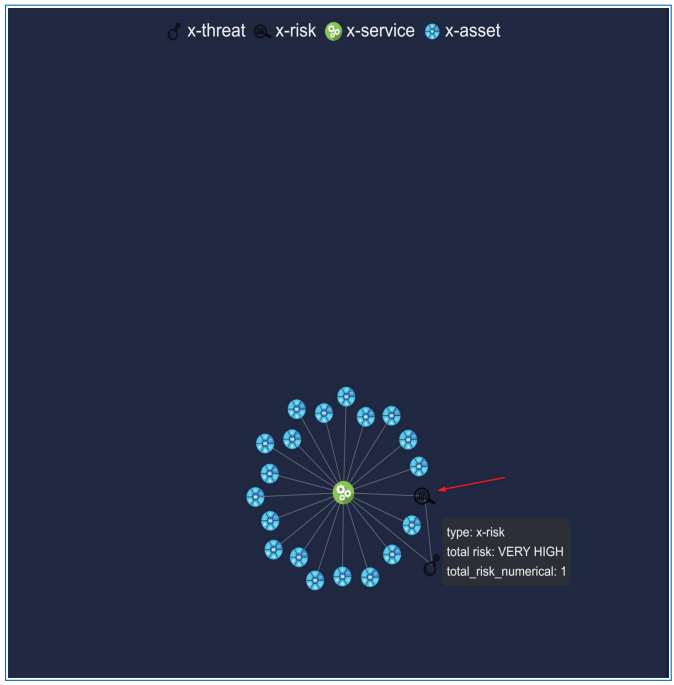

Figure 5.16. Risk results—graphical representation of the service generated.

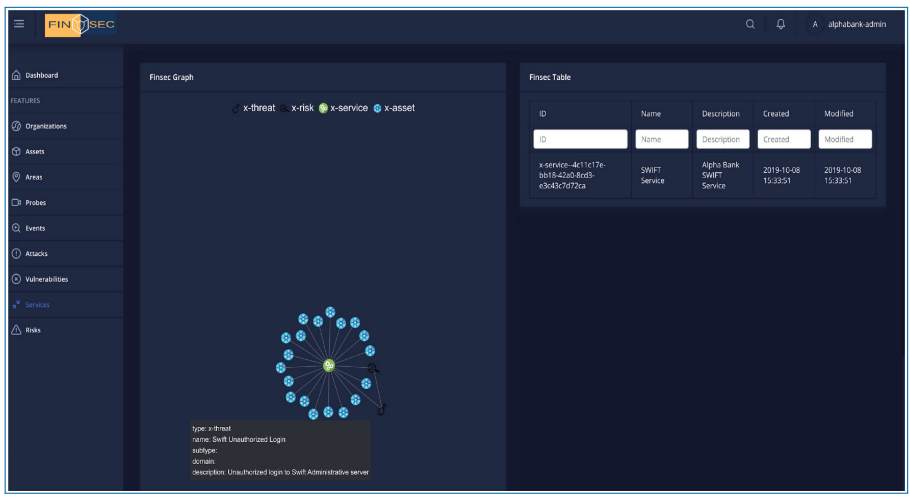

Figure 5.17. Threat identified for the SWIFT service.

Service Compromise Threat due to "Invalid Signon Attempt" events produced by the Syslog Probe is provided in Figure 5.16.

SWIFT Service details are illustrated in Figure 5.17. Both a table detail view and a relation graph are available.

The incidents related to the Compromise of the SWIFT service were successfully detected for both use cases without providing false positives.

5.7 Conclusions

This Chapter extended the approach introduced in [2] for sharing security information across financial organizations, towards enabling collaborative security in the financial services supply chain. In particular, it described a blockchain infrastructure, as a means of leveraging the advantages of auditability, security, and distributed trust offered by distributed ledger technologies. The blockchain infrastructure is appropriately integrated to a wider platform for financial services security, which is destined to protect both cyber and physical assets. In particular, this Chapter has introduced the extended collaborative risk assessment functionalities of the platform as well as the platform's security knowledge base. Then, drawing an example of the behavior of a logged in security officer, it has demonstrated the functionality of the user interface and dashboard.

Acknowledgments

Part of this work has been carried out in the scope of the FINSEC project (contract number 786727), which is co-funded by the European Commission in the scope of its H2020 program. The authors acknowledge valuable help and contributions from all partners of the project.

References

[1] Rinaldi, S.M., Peerenboom, J.P., and Kelly, T.K., Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, 11–25 (2001).

[2] Karagiannis I., Mavrogiannis K., Soldatos J., Drakoulis D., Troiano E., and Polyviou A. Blockchain Based Sharing of Security Information for Critical Infrastructures of the Finance Sector. In: Fournaris A. *et al.* (eds.) Computer Security. IOSEC 2019, MSTEC 2019, FINSEC 2019. Lecture Notes in Computer Science, vol. 11981. Springer, Cham, (2020).

[3] Maurer, T., Levite, A., and Perkovich, G. Toward a global norm against manipulating the integrity of financial data. Economics Discussion Papers, 38, Kiel Institute for the World Economy, Kiel, Germany (2017).

[4] Hussain, K. and Prieto, E. Big Data in the Finance and Insurance Sectors. In: Cavanillas J., Curry E., Wahlster W. (eds.) New Horizons for a Data-Driven Economy. Springer, Cham. (2016).
[5] European Union Agency for Network and Information Security. Safeguarding the Global Financial System by Reducing Cyber-Risk, Heraklion, Greece (2016).
[6] Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/, last accessed 2019/07/09.
[7] Ntouskas, T. and Polemi, N. A Secure, Collaborative Environment for the Security Management of Port Information Systems. 5th International Conference on the Internet and Web Applications and Services, pp. 374–379, IEEE Press, Barcelona, Spain, (2010).
[8] Theoharidou, M., Kandias, M., and Gritzalis, D. Securing Transportation-Critical Infrastructures: Trends and Perspectives. 7th IEEE International Conference in Global Security, Safety and Sustainability, pp. 171–178, Springer, Greece, (2011).
[9] Kampanakis, P. Security Automation and Threat Information-Sharing Options. IEEE Security & Privacy, 12(5), 42–51, (2014).
[10] European Network and Information Security Agency. Inventory of Risk Management/Risk Assessment Methods. rm-inv.enisa.europa.eu/rm_ra_methods.html, last accessed 2019/07/09.
[11] Ekelhart, A., Neubauer, T., and Fenz, S. Automated Risk and Utility Management, In: 6th International Conference on Information Technology: New Generations, IEEE Computer Society, 393–398, Las Vegas, NV, USA (2009).
[12] Jordan, B., Piazza, R., and Wunder, B. Stix Core Concepts. https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html, last accessed 2019/07/09.
[13] Wunder, J., Davidson, M., and Jordan, B. TAXII™ Version 2.0. Retrieved from https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/edit, last accessed 2019/07/09.
[14] Parameswaran, M., Susarla, A., and Whinston, A.B. P2P Networking: An Information-Sharing Alternative, Computer, 34(7), 31–38, 2001.
[15] Bosco, F., Croce, V., and Raveduto G. Blockchain Technology for Financial Services Facilitation in RES Investments. In: 4th International Forum on Research and Technology for Society and Industry (RTSI), pp. 1–5, IEEE Italy Section, Palermo, Italy, (2018).