electronics

MDPI

Article

Cybersecurity in Supply Chain Systems: The Farm-to-Fork Use Case

Helen C. Leligou [1], Alexandra Lakka [1], Panagiotis A. Karkazis [1,*], Joao Pita Costa [2], Eva Marin Tordera [3], Henrique Manuel Dinis Santos [4] and Antonio Alvarez Romero [5]

[1] Synelixis Solutions S.A., 34100 Chalkida, Greece; nleligou@synelixis.com (H.C.L.); lakka@synelixis.com (A.L.)
[2] XLAB, SI-1000 Ljubljana, Slovenia; joao.pitacosta@xlab.si
[3] X Lab, Universidad Politecnica de Catalunya, 08034 Barcelona, Spain; eva.marin@upc.edu
[4] ALGORITMI R&D Centre, University of Minho, 4710-057 Braga, Portugal; hsantos@dsi.uminho.pt
[5] Eviden, 28037 Madrid, Spain; antonio.alvarez@eviden.com
* Correspondence: pkarkazis@synelixis.com; Tel.: +30-6973249129

Abstract: Modern supply chains comprise an increasing number of actors which deploy different information technology systems that capture information of a diverse nature and diverse sources (from sensors to order information). While the benefits of the automatic exchange of information between these systems have been recognized and have led to their interconnection, protecting the whole supply chain from potential attacks is a challenging issue given the attack proliferation reported in the literature. In this paper, we present the FISHY platform, which anticipates protecting the whole supply chain from potential attacks by (a) adopting novel technologies and approaches including machine learning-based tools to detect security threats and recommend mitigation policies and (b) employing blockchain-based tools to provide evidence of the captured events and suggested policies. This platform is also easily expandable to protect against additional attacks in the future. We experiment with this platform in the farm-to-fork supply chain to prove its operation and capabilities. The results show that the FISHY platform can effectively be used to protect the supply chain and offers high flexibility to its users.

Keywords: cybersecurity; supply chain systems; blockchain; validation; security monitoring; attack mitigation

Citation: Leligou, H.C.; Lakka, A.; Karkazis, P.A.; Costa, J.P.; Tordera, E.M.; Santos, H.M.D.; Romero, A.A. Cybersecurity in Supply Chain Systems: The Farm-to-Fork Use Case. *Electronics* **2024**, *13*, 215. https://doi.org/10.3390/electronics13010215

Academic Editors: Dariusz Rzońca and Tomasz Rak

Received: 9 October 2023
Revised: 15 December 2023
Accepted: 20 December 2023
Published: 3 January 2024

1. Introduction

Supply chains today have become more and more complex, involving many different businesses and consumers that deploy and use diverse IT systems and applications. These IT systems usually involve IoT-based islands, robots or other smart devices next to sensors, servers and end-devices serving their users, as also happens in other sectors like health [1]. Examining cybersecurity in such a complex environment involving solutions of different types from different software companies is a very challenging problem. Today, platforms that target enhanced network security (like TERAFLOW, described in [2]) or Digital Single Market's E-Commerce Ecosystem (like ENSURESEC, described in [3]) or cloud level security are being developed. However, they target protection against a subset of the security threats applicable in the supply chains. Additionally, quantum computing has provided very promising results with respect (and not limited) to digital signatures (see [4–6]) this technology is not yet mature for being applied to the supply chain complex environment.

Should examining be challenging, ensuring protection is far more so, especially considering that the attacks targeting supply chains proliferate every day, as reported in [7]. Cybersecurity in supply chains has been recognized not only as a challenging task but as a very important task because it does not only affect a single entity (business or individual/consumer), but a series of actors in the chain. The intricacy of the supply chain attack is that it affects multiple actors at the same time, as clearly pointed out in [7]. For example,

succeeding in inserting fake information in the information system of an actor in a supply chain may affect all its downstream counterparts. Such a security breach may put at risk food safety when the supply chain under consideration is the farm-to-fork supply chain.

The "farm-to-fork" (F2F) supply chain includes all the actors that contribute to the cultivation (farmer), to the transportation (transporter), to the storage (warehouse operator), to the wholesaler and to the retailer of the vegetables that the end consumer will purchase and consume with their forks. The security challenges and requirements of such a supply chain (as reported in [8]) primarily include (a) the need for end-to-end solutions for vulnerabilities and risks management, (b) the lack of evidence-based metrics for security assurance and trust guarantees, and (c) the cumbersome coordination in multi-actor and multi-vendor supply chains of ICT systems. These have been identified for the F2F supply chain, but they are common to other supply chains as well as in, e.g., smart factories. *The problem* (research question) in this environment is "how to ensure the security of the whole supply chain and not only of isolated IT systems when these systems can significantly differ in the types of security vulnerabilities they suffer from". Another research question is this: "could a platform that answers the above question be expandable to emerging threats?". *The challenge* is to design and deliver a platform/solution that can address multiple types of vulnerability while most security-oriented solutions today target specific vulnerabilities like IoT/edge or blockchain or network security aspects.

In this paper, we present a *platform that aims* at protecting the IT systems of supply chains from multiple types of attacks including blockchain-oriented, network-oriented and web application-oriented attacks by detecting them and then recommending and possibly enforcing mitigation policies in an automated way. We validate this approach in the farm-to-fork supply chain that uses state-of-the-art IT systems. The presented platform anticipates being (a) capable of detecting a variety of attacks, (b) flexible and configurable so as to protect diverse IT systems taking into consideration their internal organization, (c) able to recommend and capable of enforcing mitigation policies and (d) flexibly deployable on premise or on cloud.

For the evaluation of such a platform, it is imperative to perform the following:

(a) Carefully consider user interface aspects: for this reason, in the piloting round, we recruited people outside the FISHY teams for carrying out the evaluation of the UI and used the prepared user manual to do so.
(b) Examine and ensure that the functionality and value of all the FISHY components is validated.
(c) Check the extensibility of the FISHY platform to address additional attacks that may be considered in the future as important for the FISHY supply chains. To examine this possibility, we have used the MITRE ATT&CK framework [9]. This has also allowed us to ensure that FISHY employs techniques that are aligned with the state of the art (reflected in MITRE ATT&CK) and that the techniques we use in FISHY enable the detection of a wide set of additional attacks in the future.

2. A Cross-Solution Security Platform—The FISHY Platform

The FISHY platform is a coordinated framework for cyber-resilient supply chain systems. Its goal is to protect diverse IT systems towards enhancing the trust among the actors of the supply chain.

FISHY platform consists of multiple functional components which can either be deployed in the same premises as the IT systems under protection or can be deployed in a different cloud infrastructure. In the latter case, a minimal set of components needs to be deployed on the same premises as the IT system under protection to enable the flow of status information (e.g., logs) from the system under protection to the FISHY platform and vice versa.

The FISHY architecture (an initial version of which can be found in [10]) is shown in Figure 1. It consists of the following set of building modules: (1) Intent-based Resilience Orchestrator and Dashboard (IRO), (2) Security Assurance and Certification Manager

(SACM), (3) Trust and Incident Manager (TIM), (4) Enforcement and Dynamic Configuration (EDC), (5) Security and Privacy Data Space Infrastructure (SPI) and (6) Secure Infrastructure Abstraction (SIA).

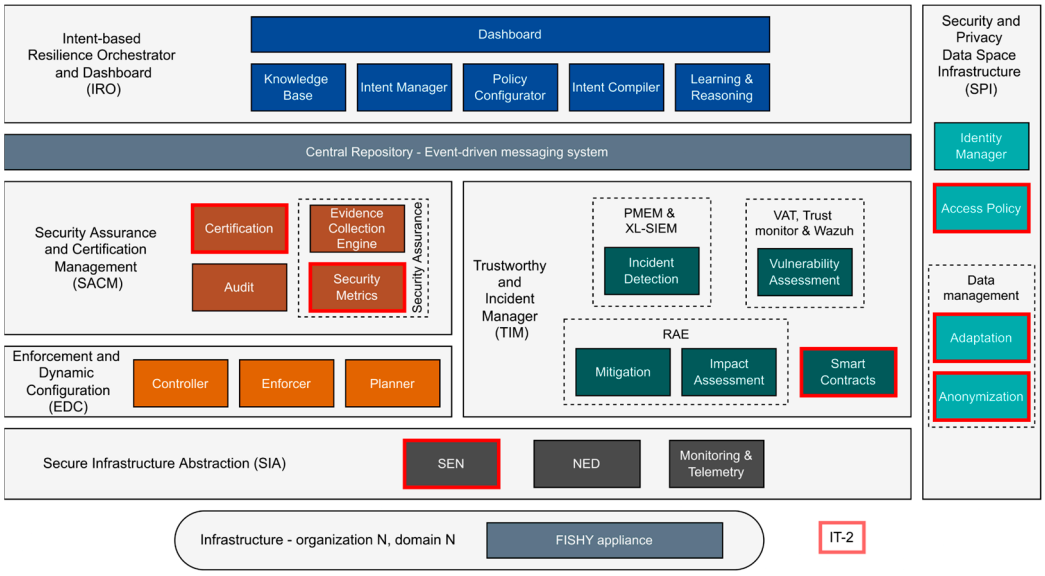


Figure 1. The architecture of the FISHY platform.

Next, we give an overview of each one of the major FISHY modules:

1. The IRO is in charge of interfacing with the security personnel/administrators of the IT systems to be protected (through the dashboard) to receive their security requirements and translate them within the FISHY platform into intents and, in turn, corresponding security workflows and policies. To be more specific, an intent is the set of data which describes the action a user can perform, for example, banning a malicious IP address [11]. It is through the IRO dashboard that the inspection of the detected security events and security control (e.g., enforcement of security policies as a response to a detected security attack) is made possible as well as the performance monitoring.
2. The SACM coordinates the monitoring process, the automated evidence-based security reporting and the certification towards ensuring that the required security policies are correctly implemented [12].
3. The TIM includes tools, such as incident detection, vulnerability and risk estimation, along with incident detection and management, with a goal of developing mechanisms, which ensure security assessment of the stakeholder's supply chains. These tools may also include machine learning-based mechanisms like those presented in with a comparison being presented in [13].
4. The EDC is in charge of security policies enforcement and configuring the specific infrastructure and network security functions (NSF) to ensure resilience. Automated remediation is thus made possible, as discussed in [12,14].
5. The SPI is in charge of identity management, access policy and data management procedures including several activities, such as access control, definition and enforcement of policies, and anonymization of the data and the tools for assessing the security of the stakeholder's devices [15].
6. The SIA module enables secure connectivity among different infrastructures (IoT, edge, cloud) and the FISHY platform, controlling connectivity and providing telemetry of the network, in order to adapt the received data to formats that the FISHY other modules can use [15].

Apart from the previously described modules, a central repository which also includes an event-driven messaging system is included, which is used to store and access information written by the FISHY components.

It is worth stressing that in this revised version of the architecture designed in the final year of the project, FISHY consortium realized that it would be beneficial of its exploitation and sustainability plans to adopt an architecture that would allow for easy integration of additional components (which we name "tools") detecting additional attacks or performing additional functionalities in the future [10]. The evolution of the architecture and further details of the workflow of the platform are provided in [10].

3. The F2F Systems under Consideration

Food security attracts continuously growing attention, as we all want to know the practices and conditions under which the food we consume has been cultivated in the farms, has been transported, has been stored and finally exposed to the shelves of the retailers. In the farm-to-fork (F2F) pilot, we distinguish the following five actors:

- The actor in the farm (user/administrator of the IoT island that is deployed in the farm);
- The actor of the transportation company which associates the products with the conditions under which the products are transported (captured by the IoT island deployed in the vehicle);
- The actor in the warehouse where the products are stored and associates the conditions under which the products are kept up to the point they are purchased by a consumer;
- The consumer who purchases the product and, based on the RFID tag attached to the product, can inspect the full history of the product;
- The administrator of the platform that gathers the information from all IoT islands and delivers it to the consumer.

In real life, there are additional actors of the same type (e.g., transportation and supermarket actors) who perform the same activities as the transporter and the warehouse manager. Each of the above represents a node in this supply chain and can be supplier and customer at the same time. For example, the actor from the transportation company represents a consumer for the farmer and a supplier for the actor of the warehouse.

We now briefly describe the F2F platform from a technical point of view. Such a system consists of multiple Internet of Things (IoT) islands registering data in different repositories and deploying different business logics. In the following figure, such an example system is presented on the left-hand side of the figure. For our study, we have selected a system that has already employed traditional authentication and authorization techniques along with state-of-the-art blockchain technology to offer a secure solution [16]. The IoT islands (shown at the bottom of Figure 2) inject traffic through the so-called federation adapters (FA) which are then responsible for storing the information in the consortium ledger. Once the product arrives at the supermarket shelves, the hashes of all relevant information are used to create a unique entry in the public distributed ledger technology (DLT) which is, in our implementation, the public Ethereum network with its hash stored in a third blockchain named KSI, which is a commercial blockchain solution. To provide an interface for the users to interact with the underlying platform, a supervisor web server has been implemented.

To protect any F2F platform, the security officers of/people responsible for the F2F platform must define the specific points they are interested in monitoring and protecting and facilitate the creation of "security probes". In our example, we have implemented the components that deliver to the FISHY platform information from four distinct points of the deployed F2F platform, as shown in the figure. The aforementioned F2F platform has been studied and from the specified distinct points we have identified four types of attacks of major interest. For each type of attack, we also specify the data that should be monitored in order to detect such an attack. The attack types and the relevant "metadata" follow:

- Type 1: Unauthorised device—wallet ID level. Metadata: {Attacker wallet ID, Expected Legitimate Wallet ID, Device name}.

- Type 2: Unauthorised device—Decentralised Identifier (DID) level (with DID characterizing the device). Metadata: {Attacker DID, Device name, Jwt}.
- Type 3: Unauthorised user. Metadata: {username, IP}.
- Type 4: Attack to Blockchain node. Metadata: {IP, port, incident type}.

The "security probes" in our example are points where logs are collected and passed to the FISHY platform so that it can analyse them to detect attacks and propose countermeasures and remediations. For example, entry points 1 and 2 are relevant to the registration of information in the farm, transportation and warehouse steps of the supply chain during which the information is stored in the ledger maintained per step. Entry point 3 is relevant to the consumer or administrator of platform and entry points 4a and 4b are relevant to the consortium level operations. The logs from these "security probes" are sent to the FISHY platform through the SIA module in the form of a JSON object which will include the following fields: Unique Universal ID (UUID), Timestamp (UTC timestamp), Type, Metadata.

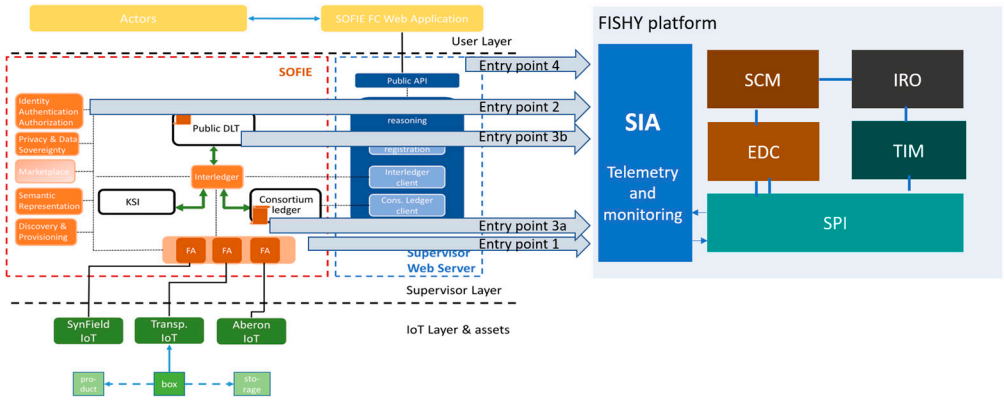


Figure 2. The F2F platform and its interconnection with the FISHY platform.

We have also discussed with other partners and decided to protect the F2F platform against additional attacks to extend the protection against additional attacks, if this is feasible and what extra actions are needed.

4. Evaluation and Discussion

Our aim is to evaluate FISHY platform from multiple perspectives ranging from technical to more commercial exploitation-oriented ones. For each of them, a different validation methodology has been adopted as will be explained in the next subsection. The aspects our evaluation has focus on include:

(a) Technical validation: We have validated that FISHY platform protects the considered platform in the defined attack scenarios (implementing or emulating the attack which is the typical methodology in attack detection, e.g., used in [17]). In this technical validation, the validation scenarios were selected based on the following criteria: (a) Attacks of interest to our customers. DDos attacks affect availability, and wallet or DID level attacks affect data integrity and privacy. These are the most important concerns in the farm-to-fork use cases. (b) Attacks of significant variety including "traditional" attacks (like DDoS attack and brute force attacks) and technology specific (blockchain specific) attacks.

(b) Additional attack detection capability with the existing tools (relevant to commercial exploitation): we studied whether the FISHY platform can protect against additional attacks outside those reported above using the currently deployed tools, which is closely related to the expandability of the platform;

(c) Commercial exploitation in diverse supply chain instances: we explored the value of offering multiple deployment options;

(d) Expandability with respect to the number and type of threat detection: we adopted the MITRE ATT@ACK framework to check how far such a platform could go in the number of attack types it can handle based on the "security probes" types we have adopted.

4.1. Evaluation of FISHY for Wallet ID Level-Oriented Attack

To carry out the technical validation for all attacks, i.e., to check whether FISHY platform efficiently detects the attacks under consideration in the farm-to-fork use case, the methodology we adopted was the following: we deployed the farm-to-fork platform in a dedicated infrastructure and developed code performing the considered attacks. The "reaction" of FISHY in the attempted attacks was monitored as well as the result in the farm-to-fork platform.

The aim is to confirm that the FISHY platform detects the attacks of type 1 titled "unauthorized device—wallet ID level". This is an attack that could occur in any of the IoT islands as, for example, the one deployed in the farm. For example, a malicious actor uses an unauthorized device and attempts to enter "fake" information in the F2F platform. In this platform, the IoT devices (through the so-called federation adapter—FA) register information about the fresh products, and in this registration, they use a wallet ID.

Assuming a malicious user intends to push to the platform fake information, they would use a device which has not been registered in the F2F platform. The information about data registration and the corresponding wallet IDs are passed to the FISHY TIM module through the security probes and the SIA deployed in the F2F platform premises. The F2F platform operator has appropriately configured the FISHY and more specifically the SACM module so that it recognizes which wallet IDs are legible or not. Thus, when the malicious user uses an unregistered wallet ID, SACM will detect this and will report a security event. In the following figure, the dashboard of the FISHY platform is shown in Figure 3. The instance presented here shows the events (one per row) detected by FISHY and their details as well as whether this event has been registered in the FISHY blockchain network (indicated by the green (check mark) symbol on the right-hand side of the event). This will trigger the IRO so that the relevant intent is identified, and a policy is suggested to the F2F platform operator. Once (s)he confirms (s)he agrees for the enforcement of the policy, the EDC undertakes its translation into a low-level policy, and it is passed to the F2F platform.

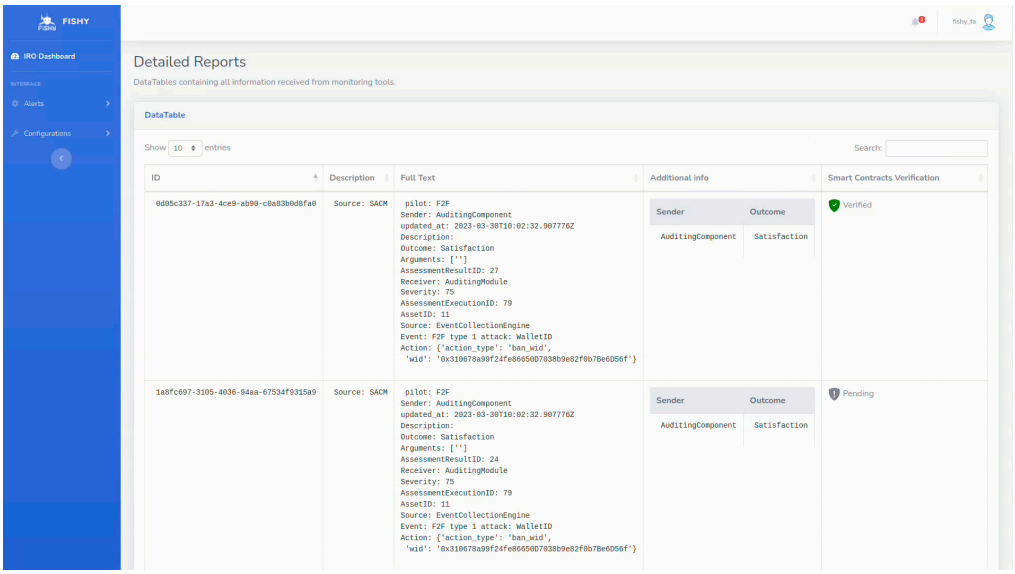


Figure 3. The FISHY dashboard presenting the detected event.

Now, the F2F platform will no longer communicate with the malicious federation adapter. Instead, the F2F platform displays a message to the attacker that the information (s)he tries to register is not accepted (as shown in the red box in the Figure 4).

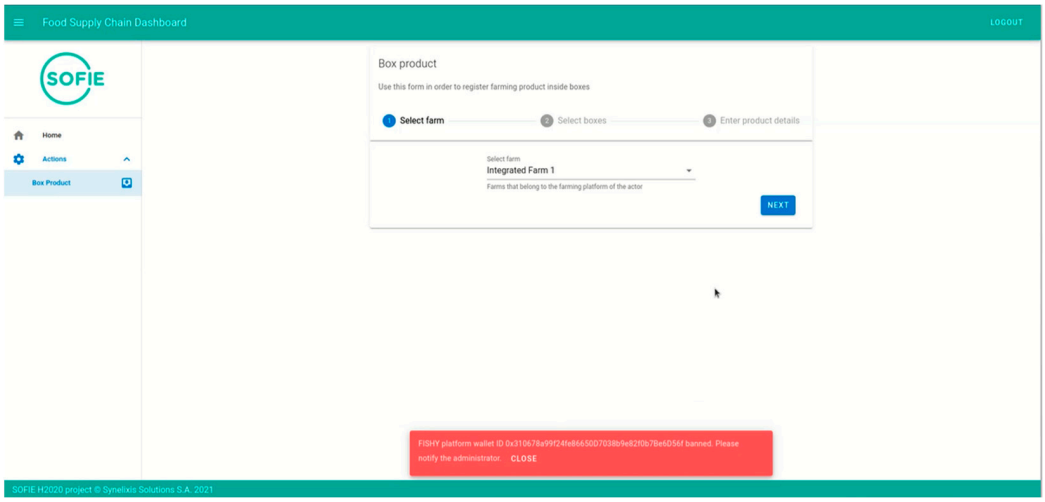


Figure 4. Screenshot from the F2F platform where the inability of the malicious user to enter information is shown.

4.2. Evaluation of FISHY for Attack to Blockchain Node

The aim in this section is to demonstrate that the FISHY platform detects the attacks of type 4, titled "Attack to blockchain node". This is an attack more likely to occur from a knowledgeable person to insert fake information in the blockchain used by the F2F platform. Let us assume the attacker tries to compromise the blockchain node, trying to connect to the blockchain node from a device with an IP address that is not whitelisted for the F2F premises.

The malicious actor could try to construct a request to the F2F blockchain, to try to insert fake information, for example, an unauthorized "Farm" platform, as depicted in Figure 5. The adversary, in order to prepare for the attack, can attempt to gain information on the nodes of the F2F blockchain network by exploiting the Tessera transaction manager of the nodes. Figure 6 shows the results of the exploitation of the Tessera endpoints. The user gains knowledge of the public keys of the nodes, which (s)he can use to sign their transaction and send to the blockchain.

```
        FOOD_CHAIN_ABI_RAW = \
"""...

        public_key = "fZsrQpqSy9xScXIgEUGXy2vokXJsxdAP18RgjxB9QCo="

        arguments = ["0xc5707BdcD820694303496B74d56895902a009943",
                     "My farming platform",
                     0,
                     '']


        FOOD_CHAIN_ABI = json.loads(FOOD_CHAIN_ABI_RAW)

        status, tx_hash, tx_revert_reason = self.transact_quorum("http://192.168.1.238:32232",
                                            "0xc3d09235621Ec77C51C0615b164a96403e82467d",
                                            public_key.split(),
                                            "0x716Ae3752487b70a7BD529d7De718c6096550fdD",
                                            "register_platform",
                                            arguments,
                                            FOOD_CHAIN_ABI,
                                            1000)
```

Figure 5. The adversary attempts to register fake information to the blockchain.

Should an external connection from an unknown IP occur, then the FISHY platform and more specifically SACM tool is notified as shown in Figure 7. In this validation, SIA, SPI, TIM and IRO were involved.

```
→ curl http://192.168.248.11:9001/partyinfo | jq '.'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   635  100   635    0     0  42333      0 --:--:-- --:--:-- --:--:-- 42333
{
  "url": "http://quorum-node2.fishy-sc:9001/",
  "peers": [
    {
      "url": "http://quorum-node1.fishy-sc:9001/"
    },
    {
      "url": "http://quorum-node2.fishy-sc:9001/"
    },
    {
      "url": "http://quorum-node3.fishy-sc:9001/"
    },
    {
      "url": "http://quorum-node4.fishy-sc:9001/"
    }
  ],
  "keys": [
    {
      "key": "E5SY6IBNuyesnXpjXhnrlfFq/H4NH+xzOTRkCz4Q2gM=",
      "url": "http://quorum-node4.fishy-sc:9001/"
    },
    {
      "key": "MHFxTeY8fS1aU+DdhpQvseYBSN20YREYH2levMyqhw8=",
      "url": "http://quorum-node3.fishy-sc:9001/"
    },
    {
      "key": "XvEGjW5CvngN8vVNpqWm3fD0g02cj/6AblOry6RSMTg=",
      "url": "http://quorum-node1.fishy-sc:9001/"
    },
    {
      "key": "fZsrQpqSy9xScXIgEUGXy2vokXJsxdAP18RgjxB9QCo=",
      "url": "http://quorum-node2.fishy-sc:9001/"
    }
  ]
}
```

Figure 6. The adversary exploits the endpoints of the Tessera transaction manager of the nodes to find their public keys.


```
{"device_product": "AuditingComponent",
 "device_version": "1.0",
 "pilot": "F2F",
 "event_name": "F2F type 4 attack: Attack to Blockchain Node",
 "device_event_class_id": "32",
 "severity": "75",
 "extensions_list": '{"pilot": "F2F",
 "Sender": "AuditingComponent",
 "updated_at": "2023-03-30T10:02:32.907776Z",
 "Description": "",
 "Outcome": "Satisfaction",
 "Arguments": [""],
 "AssessmentResultID": 32,
 "Receiver": "AuditingModule",
 "Severity": 75, "AssessmentExecutionID": 79, "AssetID": 11, "Source": "EventCollectionEngine",
 "Event": "F2F type 4 attack: Attack to Blockchain Node", "Action": {"action_type": "ban_ip", "ip": "163.23.164.166"}}'
}
```


Figure 7. SACM monitors the IPs being connected to the blockchain node and checks whether these are whitelisted IP addresses.

Next, FISHY platform proposes a policy to be enforced. This policy is a ban-IP policy and is generated in IRO and turned to a low-level policy by EDC which then enforces it in the F2F use case, as shown in Figure 8. The end result is that the connection of the adversary node is terminated.

```
→  nc -v 192.168.1.236 32232
nc: connect to 192.168.1.236 port 32232 (tcp) failed: Connection refused
```

Figure 8. The malicious user can no longer connect to the blockchain node.

4.3. Evaluation of FISHY for DDoS Attack

The aim in this section is to demonstrate that the FISHY platform detects distributed denial of service (DDoS) attacks. For the F2F platform, the availability of the services is extremely important, due to the economic loss to the actors that rely on the F2F platform (e.g., retailers that use the platform to guarantee the safety of the supply chain) that can be caused by downtimes. Therefore, it is important for FISHY to be able to protect the platform against this type of attack.

To do this, the real-time network traffic is captured from the platform and then it is sent continuously to the PMEM tool [3] in the FISHY control services (Figure 9). As observed in the figure below, the captured flows contain normal traffic which is sent to the PMEM, and different traffic statistics are shown.

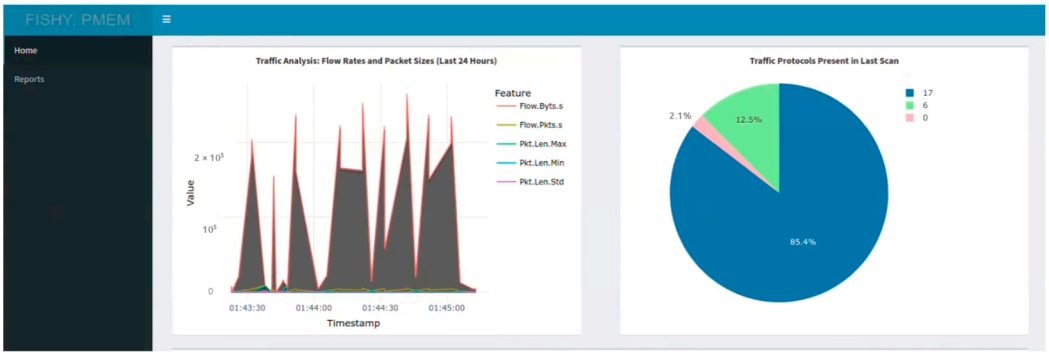


Figure 9. The PMEM dashboard showing the traffic of the system under examination.

PMEM gives information about the different flows in the network as well as different useful statistics about traffic share and severity of the attacks. To test the capability of PMEM to detect a DDoS attack, we intentionally simulate the scenario on the F2F platform. This malicious traffic along with the normal traffic is captured and sent to the PMEM tool. The traffic analysis shows that something abnormal is happening in the network (Figure 10).

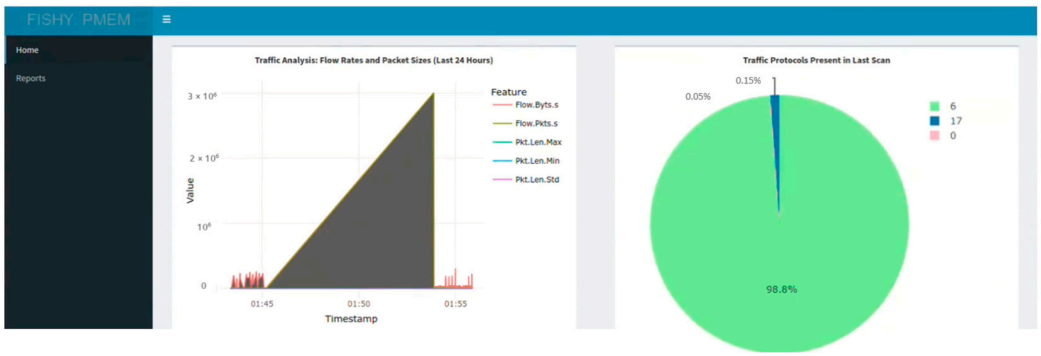
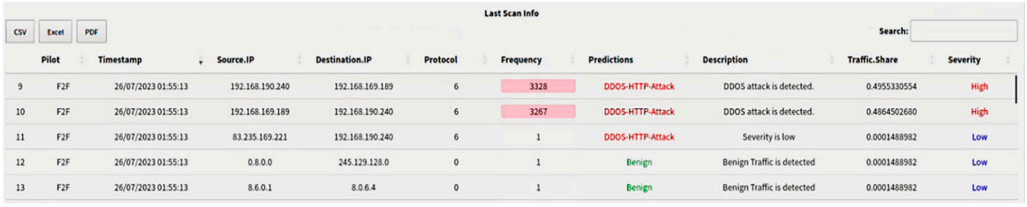


Figure 10. PMEM dashboard showing the statistics which show the results of the machine learning model (which classifies the traffic in benign and suspicious).

The prediction result of the PMEM for the network flows are presented in Figure 11:



	Pilot	Timestamp	Source.IP	Destination.IP	Protocol	Frequency	Predictions	Description	Traffic.Share	Severity
9	F2F	26/07/2023 01:55:13	192.168.190.240	192.168.169.189	6	3328	DDOS-HTTP-Attack	DDOS attack is detected.	0.4955330554	High
10	F2F	26/07/2023 01:55:13	192.168.169.189	192.168.190.240	6	3267	DDOS-HTTP-Attack	DDOS attack is detected.	0.4864502680	High
11	F2F	26/07/2023 01:55:13	83.235.169.221	192.168.190.240	6	1	DDOS-HTTP-Attack	Severity is low	0.0001488982	Low
12	F2F	26/07/2023 01:55:13	0.8.0.0	245.129.128.0	0	1	Benign	Benign Traffic is detected	0.0001488982	Low
13	F2F	26/07/2023 01:55:13	8.6.0.1	8.0.6.4	0	1	Benign	Benign Traffic is detected	0.0001488982	Low

Figure 11. Details of the PMEM prediction results as shown in the PMEM dashboard.

The PMEM has detected the IP addresses which are trying to perform a DDOS attack, also including the frequency of the specific combination of source IP and destination IP. The severity of the attack is related to its computed frequency. The system shows, for instance, that the 3rd row in the table is considered a DDoS attack with low severity because the frequency is only 1, whereas the two first rows are considered real DDoS attacks because the frequencies are higher than a specific threshold.

4.4. Evaluation of FISHY for Detection of Brute Force Attacks

The aim in this section is to demonstrate that FISHY platform detects brute force attacks or in other words prevent an "unauthorized user" that possibly uses a machine to check all potential passwords to access the farm-to-fork platform. We assume that the attacker uses the wrong password or issues a brute force attack to gain access and potentially alter information relevant to specific products either to create a mesh or to diminish the value of specific brands. The attacker tries different combinations of username and password to enter the F2F platform. The F2F platform operator sets a rule in FISHY to check unsuccessful logic attempts from the same IP address and when these exceed a predefined threshold that he/she sets, FISHY notifies the F2F platform operator and suggests the banning of this IP.

In more detail, the FISHY platform detects this event (attack) as shown in Figure 12 through the Wazuh tool.

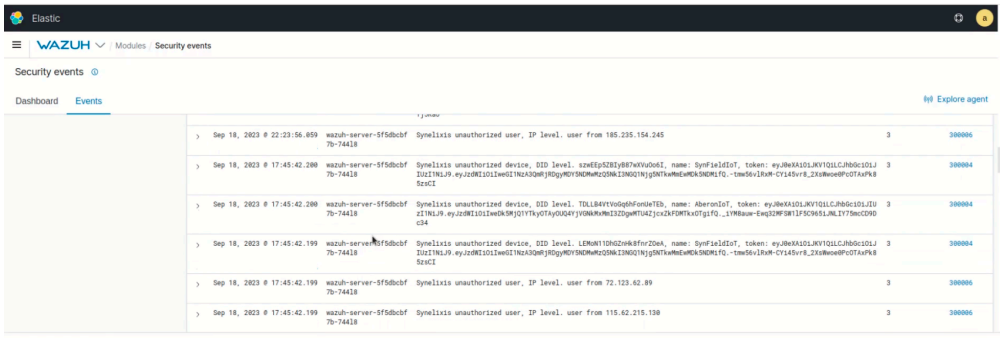


Figure 12. Screenshot from the dashboard of Wazuh that detects the brute force attack.

Next, to the detection, the FISHY platform proposes a ban-IP policy to be enforced. This policy is generated in IRO and turned to low-level policy by EDC which then enforces it in the F2F use case. Finally, the F2F platform displays a message to the attacker that the information he/she tries to register is not accepted.

4.5. Benchmarking FISHY to MITRE ATT&CK Framework

To assess the expandability of the FISHY platform, we use the MITRE ATT&CK framework and we proceed to logical implications to reach useful conclusions. To elaborate, during our research in the area of security attacks, we realized that the MITRE ATT&CK framework [9] plays a vital role. First, we must clarify that ATT&CK stands for adversarial tactics, techniques and common knowledge, and these are what the framework and accompanying ATT&CK knowledge base consist of. This framework aims at addressing the gap left by traditional models which are very focused on the study of attacks rather

than their role in risk analysis, where the concern is not how the attack is executed but more on the effects and exploitation opportunities that can impact the system. This is of particular interest in the supply chain environments where the attacks to one of the interconnected IoT islands directly affect other actors in the chain. An additional reason to study this framework is that MITRE table is enriched by the open community that supports it. Thus, regularly inspecting this table can help us (a) continuously upgrade FISHY so that it protects against an ever-increasing set of attack types it handles and (b) verify that the techniques addressed are those reported in this open "literature".

In the farm-to-fork use case, the attacks we identified have been proposed to be detected using logs. To verify our decision, we select as the "control element" the log in the MITRE navigator, and we see the set of attacks that can be detected using logs, shown in green colour in Figure 13. All the attacks shown in green in this figure can be detected based on logs. This implies that should a platform owner be interested in detecting all these attacks, he/she should take care of providing the FISHY platform with the relevant logs in real time (i.e., ensure the provisioning of the relevant information).

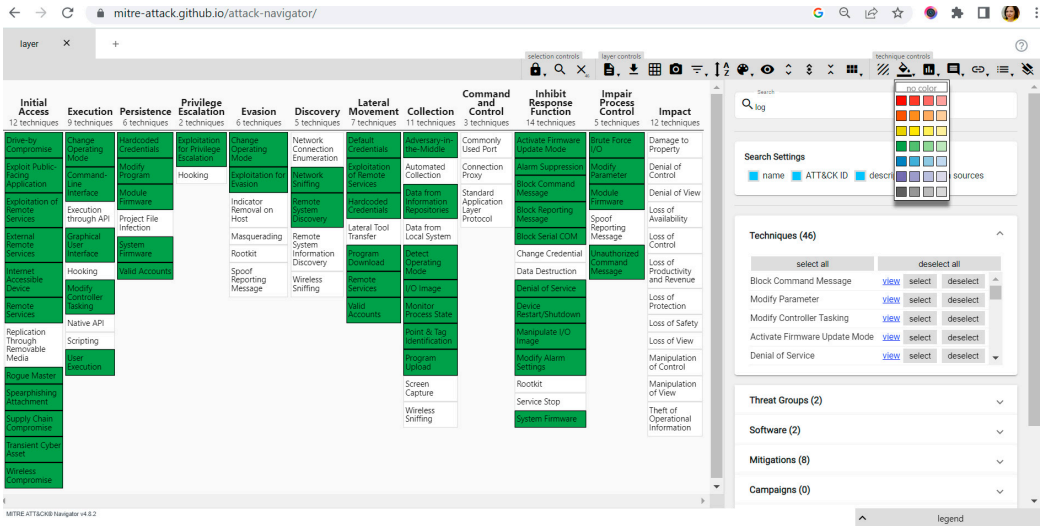


Figure 13. The attacks that can be detected based on logs shown/highlighted in green.

From the green boxes highlighted in the figure, we then select one-by-one the threat most relevant to our system. For example, the "default credentials" attack and the "denial of service" attack. Then, selecting the attack, the MITRE ATT&CK navigator displays all the procedures that an adversary may follow to issue such an attack that have been registered in the framework, the mitigation measures identified so far and the detection alternatives. Then, we check for the cells of interest whether FISHY platform implements a detection technique and whether the mitigation identified (and recommended and/or enforced) in FISHY is aligned with the one suggested by MITRE table. This way we have confirmed that FISHY platform adopts mitigation strategies well recognized in the market.

Another way to use the MITRE ATT&CK framework is the following: to check what can be detected based on specific controls. The rationale behind this choice is the following: in the farm-to-fork system, FISHY is capable of detecting threats based on logs and based on traffic analysis. So, in the MITRE ATT@CK navigator, we first selected "log" and then "traffic analysis", and the result is shown in Figure 14. The attacks that can be detected based on traffic analysis are marked in orange colour while those that can be detected using logs and not on traffic analysis are marked in green colour. (A subset of the orange-coloured threats are also detected using logs as was shown in the previous figure.) Again, as mentioned for the attacks detected based on logs, similarly, for the attacks detected based on traffic analysis information, the security officers of any platform interested in protecting their platform using FISHY, they should only ensure that the appropriate traffic analysis

data are passed to the FISHY platform. Then, FISHY integrates all the necessary tools for detecting, recommending and potentially enforcing the mitigation policies.

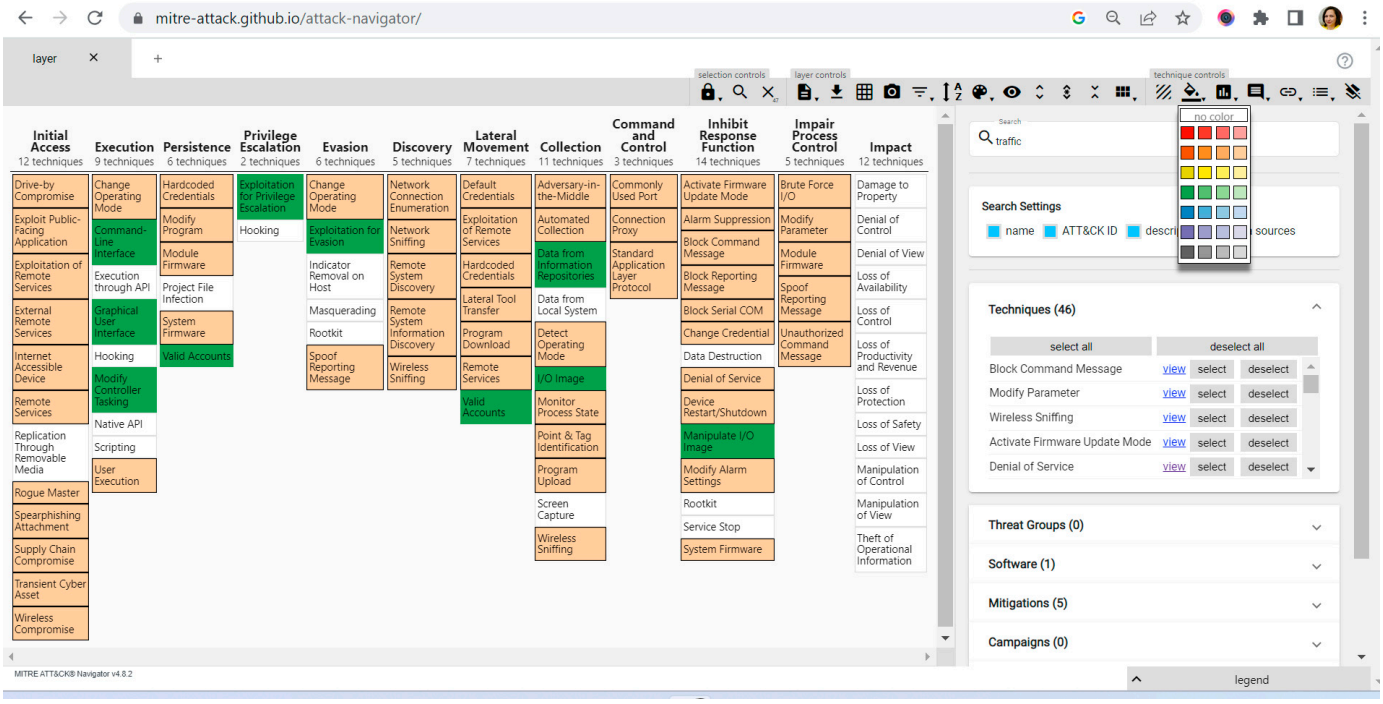


Figure 14. The threats that can be detected based on logs and traffic analysis information are coloured.

This has an important logical implication for FISHY: FISHY components can detect the majority of the identified threats which shows that FISHY is a flexible platform that can be exploited to detect the proliferating attacks that supply chain systems suffer today. With regard to mitigation, the flexible FISHY user interface allows for easy registration of multiple mitigation rules which could be drawn from a MITRE ATT&CK table.

4.6. FISHY-Enabled Security Enhancement in F2F Supply Chain

As has been shown in the previous sections, with the integration of the F2F IT system with FISHY, a set of interesting (to the actors) and important attacks are detected and mitigated. Additionally, we have realised that the different components of the FISHY platform can detect more attacks than those presented above: generating additional security probes, FISHY platform can detect attacks to additional points in the supply chain IT platform based on SACM and also, analysing traffic at different network levels or network islands, based on PMEM additional parts of the supply chain system can be protected. Analysing log information and performing machine learning-based traffic analysis enables the detection of a variety of attacks.

To assess the FISHY platform as objectively as possible, we presented the platform and asked colleagues outside the project teams to experiment with the features of the platform during a workshop that we held with seven people. The alpha version of the FISHY platform was released to the select group of testers from the consortium partners for evaluation and feedback. This process focused on identifying fundamental issues such as bugs, glitches and major functionality gaps, ensuring that the core features of the software were operational, and collecting feedback on performance and stability. The feedback collected during the workshop served as a valuable resource for refining the software before progressing to more extensive testing, where a larger and more diverse user base will be involved. Although this is not a large and statistically representative sample, due to the high expertise of the participants we consider their opinion valuable, carrying their extensive experience in the farm-to-fork sector and more specifically from the

IT system vendors. During this workshop, the user group answered/commented on the following topics:

- Easiness to use and user friendliness: the Average rating was 4.1 (using a five-point Likert scale), which was considered very good for a platform resulting from a research project.
- Security improvement: The question we asked was this: "what would you say if you were to quantify how much more secure is now the platform?". From the discussion that was raised, the answers converged towards the following key points:
    - The platform seems to efficiently detect the main attacks of interest.
    - The flexibility provided by the dashboard makes the operators feel they control what happens in the platform they operate.
    - The flexibility in detection offered by the different tools make the operators feel they can defend a wide range of attacks.
    - The FISHY dashboard with its clear presentation of events leaves time to the operator to focus on configuring the platform to detect additional attacks.
    - The immutability of the events guaranteed by the introduction of the blockchain technology and the registration of events in the blockchain network open the door to IoT vendors to persuade IT platform vendors to consider integrating IoT devices by less popular vendors, thus fostering competition.
    - To assess whether the multiple deployment options are of interest to the buyers, we asked the group: "deployment options: are they important?". They all found that they are very important as the deployment in each supply chain is different and tailored to the actors of the chain. One of the main business lines of Entersoft S.A. is software customisation company providing services to big supply chain actors. So, having the option to deploy on premise or on hybrid approach the platform and decide the split of components offers huge and valuable flexibility.

Other comments we received include the following: "At the beginning, it was not easy for us to understand how the platform is connected to the IT platform of the supply chain. The user manual helped but needs to be accompanied by a video". And it is "not easy to understand the flexibility of the platform. Somebody needs to delve into the details to find out".

4.7. FISHY Scalability and Potential Enhancements

The FISHY platform has been shown to efficiently detect a set of attacks. Additionally, it has been proven (based on the MITRE ATT&CK navigation tool) that it can potentially expand to detect other attacks. This would require the implementation of security probes on the side of the supply chain platform and on the configuration of appropriate rules in the FISHY platform. Furthermore, the architecture of the FISHY platform can flexibly integrate additional (open source or not) tools which can use the information captured by FISHY platform, they can also use the central repository and finally exploit the user-friendly FISHY user interface. With respect to the number of IT platforms that FISHY can protect, there is no limitation on this as it has been designed with scalability in mind. To sum up, the FISHY platform is both scalable and expandable with respect to the number of attack it is capable of detecting, with respect to the IT platform it can protect and with respect to the threat detection tools it can integrate. Its designers have pointed out that potential enhancement would follow two directions: the design of a very easy-to-use front end (so that it can be used not only by security officers) and the integration of tools that may be optimized for other IoT threats.

5. Conclusions

To sum up, we have shown that it is possible to have a platform that can detect and recommend the mitigation of multiple attack of different types (from network configuration to blockchain specific threats) and, at the same time, be expandable to be able to detect attacks that may be defined in the future. The FISHY platform efficiently protects the

considered supply chain IT systems against multiple type of attacks, while with almost straightforward configurations, it can protect against a really large set (almost 85%) of the supply chain attacks reported in the MITRE ATT@CK framework. Apart from configuration of the components, in certain cases, some development of the appropriate mechanism to provide FISHY with the required supply chain platform details and data may be needed, but this is considered minor once the components and their user interface to the administrators are ready. Additionally, the flexible deployment of the FISHY platform is well appreciated from external end users. The authors anticipate that security platforms like FISHY have a strong potential not only in the supply chain but also in interconnected IT systems as, for example, the connected health care systems and applications [17], which are of very high importance to the quality and reliability of the health services provided.

Author Contributions: Conceptualization and methodology, H.C.L.; software, A.L. and P.A.K.; MITRE ATT&CK analysis, H.M.D.S. and H.C.L.; resources, E.M.T. and A.A.R.; writing—original draft preparation, P.A.K.; writing—review and editing, A.A.R. and J.P.C.; supervision, E.M.T.; project administration, A.A.R. and E.M.T. All authors have read and agreed to the published version of the manuscript.

Funding: This article has partially been supported by the EU funded H2020 FISHY Project (Grant agreement ID: 952644).

Data Availability Statement: Data are available upon request.

Acknowledgments: The authors would like to acknowledge all FISHY project partners for their technical contributions to the definition and development of the FISHY platform. And would like to acknowledge Ayaz Hussain for his contribution in improving the quality of the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Karamitsios, K.; Orphanoudakis, T. Efficient IoT data aggregation for connected health applications. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 1182–1185. [CrossRef]
2. European Commission. TERAFLOW [Online]. 2023. Available online: https://www.teraflow-h2020.eu/ (accessed on 7 November 2023).
3. European Commission. ENSURESEC [Online]. 2023. Available online: https://www.ensuresec.eu/ (accessed on 7 November 2023).
4. Yin, H.-L.; Fu, Y.; Li, C.-L.; Weng, C.-X.; Li, B.-H.; Gu, J.; Lu, Y.-S.; Huang, S.; Chen, Z.-B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [CrossRef] [PubMed]
5. Zhou, L.; Lin, J.; Xie, Y.-M.; Lu, Y.-S.; Jing, Y.; Yin, H.-L.; Yuan, Z. Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking. *Phys. Rev. Lett.* **2023**, *130*, 250801. [CrossRef] [PubMed]
6. Bulla, L.; Pivoluska, M.; Hjorth, K.; Kohout, O.; Lang, J.; Ecker, S.; Neumann, S.P.; Bittermann, J.; Kindler, R.; Huber, M. Nonlocal Temporal Interferometry for Highly Resilient Free-Space Quantum Communication. *Phys. Rev. X* **2023**, *13*, 021001. [CrossRef]
7. Lella, I.; Theocharidou, M.; Tsekmezoglou, E.; Malatras, A.; Garcia, S.; Valeros, V. *Enisa Threat Landscape for Supply Chain Attacks*; ENISA: Athens, Greece, 2021; ISBN 978-92-9204-509-8. [CrossRef]
8. Trakadas, P.; Karkazis, P.; Leligou, H.C.; Gonos, A.; Zahariadis, T. Farm to fork: Securing a supply chain with direct impact on food security. In Proceedings of the IEEE International Conference on High Performance Switching and Routing, Paris, France, 7–10 June 2021. [CrossRef]
9. Available online: https://attack.mitre.org/ (accessed on 3 October 2023).
10. Jukan, A.; Dizdarević, J.; Carpio, F. D2.4 Final Architectural Design and Technology Radar. Available online: https://fishy-project.eu/sites/fishy/files/public/content-files/deliverables/D2.4%20Final%20Architectural%20design%20and%20technology%20radar_v1.0.pdf (accessed on 10 September 2023).
11. Bensalem, M.; Dizdarević, J.; Carpio, F.; Jukan, A. The role of intent-based networking in ict supply chains. In Proceedings of the 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR), Paris, France, 7–10 June 2021; pp. 1–6.
12. Santos, H.; Oliveira, A.; Soares, L.; Satis, A.; Santos, A. Information Security Assessment and Certification within Supply Chains. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–6.
13. Bensalem, M.; Dizdarević, J.; Jukan, A. Benchmarking various ML solutions in complex intent-based network management systems. In Proceedings of the 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 23–27 May 2022.

14. Settanni, F.; Regano, L.; Basile, C.; Lioy, A. A Model for Automated Cybersecurity Threat Remediation and Sharing. In Proceedings of the 2023 IEEE 9th International Conference on Network Softwarization (NetSoft), Madrid, Spain, 19–23 June 2023; pp. 492–497.
15. Gonzalez, L.F.; Vidal, I.; Valera, F.; Lopez, D.R. Link Layer Connectivity as a Service for Ad-Hoc Microservice Platforms. *IEEE Netw.* **2022**, *36*, 10–17. [CrossRef]
16. Available online: https://www.sofie-iot.eu/ (accessed on 3 October 2023).
17. Hussain, A.; Aguiló-Ghost, F.; Simó-Mezquita, E.; Marín-Tordera, E.; Masip-Bruin, X. An NIDS for Known and Zero-Day Anomalies. In Proceedings of the 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltru, Spain, 17–20 April 2023. [CrossRef]