Continuous Security Assurance of Modern Supply-Chain Ecosystems with Application in Autonomous Driving

The FISHY approach for the secure autonomous driving domain

George Hatzivasilis, Sotiris Ioannidis
Department of Electric and Computer Engineering
Technical University of Crete
Chania, Crete, Greece
{hatzivas, sotiris}@tuc.gr

Grigoris Kalogiannis, Manolis Chatzimpyrros, George Spanoudakis
Innovation Department
Sphynx Technology Solutions AG
Zug, Switzerland
{g.kalogiannis, m.chatzimpyrros, spanoudakis}@sphynx.ch

Guillermo Jiménez Prieto, Araceli Rojas Morgan, Miguel Juaniz Lopez
Capgemini SE
Genoble, France
{guillermo.jimenezprieto, araceli.rojasmorgan, miguel.juaniz-lopez}@capgemini.com

Cataldo Basile
Control and Computer Engineering Department
Politechnico di Torino
Torino, Italy
cataldo.basile@polito.it

Jose Francisco Ruiz
Innovation Department
ATOS Spain SA
Madrid, Spain
josefrancisco.ruiz@atos.net

Abstract— **Cyber security always forms a significant aspect of ICT infrastructure, with threats on supply-chain networks gaining greater attention nowadays. The secure autonomous driving domain presents a unique set of challenges for supply-chain security. Autonomous vehicles rely on a complex ecosystem of hardware and software components, many of which are sourced from third-party suppliers. Ensuring the security and reliability of this supply-chain is essential to maintain the safety and viability of autonomous driving as a technology. To address these challenges, a continuous security assurance approach is necessary. This involves ongoing monitoring, assessment, and improvement of security measures to detect and mitigate potential vulnerabilities in the supply chain. Key measures may include regular vulnerability assessments, penetration testing, and security awareness training for employees and contractors, as well as the implementation of security controls such as secure communication protocols, access controls, and intrusion detection systems. By adopting a continuous security assurance approach for supply chain security in the secure autonomous driving domain, organizations can safeguard their operations and ensure the safety of passengers and other road users. This paper presents a security assurance and certification solution for supply-chain services. Security elements are continuously assessed based on AI operations. The proposal is implemented under the EU funded project FISHY and applied in the supply-chain of secure autonomous driving (SADE) pilot with REMOTIS smart vehicles. Nevertheless, it is a generic solution that can be applied in any domain.**

Keywords—security assurance, artificial intelligence, supply-chain, autonomous driving, REMOTIS, smart vehicle.

I. INTRODUCTION

Modern supply chain services have evolved to leverage cutting-edge technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT) to improve efficiency and transparency [1]-[2]. These services help organizations to optimize their supply chain operations by providing real-time visibility into the movement of goods, reducing costs through automation and predictive analytics, and improving compliance with regulations and industry standards.

Supply chain services are increasingly reliant on digital technologies, which makes them vulnerable to a range of cyber threats [3]-[4]. Such cyber threats can lead to the compromise of sensitive data, disruption of business operations, and financial losses. To address these threats, organizations need to implement robust cybersecurity measures. Additionally, organizations should implement contingency plans to respond to cyber incidents affecting their supply chain to minimize the impact of any security breach. By taking proactive steps to address cyber threats, organizations can safeguard their own operation, as well as the supply chain functions, and maintain the trust of their customers and stakeholders.

Continuous security assurance refers to the practice of continuously monitoring and assessing an organization's security posture to ensure that security controls and processes are working effectively [5]-[6]. Assurance incorporates a range of measures, including regular vulnerability assessments, penetration testing, and security awareness training for employees and contractors. By implementing such strategies, organizations can reduce their risk of a security breach and improve their overall security posture. It also helps organizations meet regulatory compliance requirements and maintain customer trust.

Under the EU funded project FISHY, a continuous security assurance platform for supply-chain ecosystems has been implemented. As an indicative application scenario, this proposal has been deployed and tested in an autonomous driving [7] setting. As autonomous driving technology becomes increasingly advanced, it is essential to address potential cyber risks such as cyber attacks, data breaches, and system failures. These risks can pose a significant threat to the safety of passengers and other road users, as well as to the viability of autonomous driving as a technology. By ensuring the security and reliability, the secure autonomous driving domain is helping to realize the potential benefits of this technology while minimizing the risks.

The rest of the paper is organized as: Sector 2 reviews the threat landscape for supply-chain services and the related cyber security management solutions. Section 3 presents the proposed solution for security assurance and certification management of the EU funded project FISHY. Section 4 details the application of FISHY in a piloting environment for secure autonomous driving. Finally, Section 5 concludes this work and provides directions for future works.

II. Background & Related Works

A. Supply-Chain Services and Market

Supply-chain services are services provided by third-party vendors or suppliers to help manage and optimize a company's supply chain operations [1]. These services may include: i) logistics and transportation services, ii) warehousing and inventory management services, iii) procurement and sourcing services, iv) supply-chain planning and optimization services, v) risk management and compliance services, and vi) sustainability and social responsibility services.

Overall, supply-chain services can help organizations to optimize their supply chain operations, reduce costs, and improve efficiency [2]. By outsourcing these services to third-party vendors or suppliers, organizations can focus on their core business operations while leveraging the expertise and resources of specialized service providers.

The supply chain services market is expected to see significant growth in the coming years, driven by the increasing demand for efficient and cost-effective supply chain operations [8]. The COVID-19 pandemic has also highlighted the importance of resilient supply chains, which is expected to further drive the growth of the market in the coming years [8].

B. Threat Landscape for Supply-Chain Services

Cyber threats to the supply chain have become a major concern in recent years, as more organizations rely on third-party vendors and suppliers to deliver goods and services [3]-[11]. Here are some common types of cyber threats that can impact the supply chain: i) malware and ransomware, ii) phishing attacks, iii) third-party vulnerabilities, iv) insider threats, v) disruption of collaborative services and communication points, and vi) Advanced Persistent Threats.

There have been several high-profile cyber attacks on modern supply chain services in recent years [9]. One example is the SolarWinds hack [10], in which hackers compromised SolarWinds, a software provider used by numerous government agencies and private organizations, to access their customers' networks. The attack exposed sensitive data and potentially compromised the integrity of government and business operations. Another example is the Colonial Pipeline ransomware attack [11], which caused significant disruption to fuel supplies in the eastern United States. The attackers targeted a third-party supplier to gain access to the Colonial Pipeline network and demanded a ransom to restore access to critical systems. These attacks highlight the growing threat posed by cyber attacks on modern supply chain services and underscore the need for robust cybersecurity measures to protect against such threats [9].

To mitigate these cyber threats on their supply chains, organizations can implement a range of security measures, such as implementing multi-factor authentication, performing regular vulnerability assessments and penetration testing, monitoring third-party vendors and suppliers, and implementing security awareness training for employees and contractors (e.g., [7]-[11]). Also, it is important for organizations to have contingency plans in place to respond cyber incidents affecting their supply chain.

C. Continuous Security Assurance

The continuous security assurance market includes a range of solutions such as vulnerability scanners, security information and event management (SIEM) tools, intrusion detection and prevention systems, threat intelligence platforms, and security orchestration, automation, and response (SOAR) solutions [5]. The market is driven by the growing need for organizations to improve their security posture in the face of an increasingly complex and evolving threat landscape (e.g., [5]). As more organizations adopt cloud computing, DevOps, and digital transformation initiatives, they must address the raising security implications.

According to market research reports (e.g., [12]), this global market is expected to grow significantly in the coming years. This is due to the increasing adoption of cloud-based security solutions, the rise in cyber threats/attacks, and the need for regulatory compliance. The market is also being driven by the emergence of new technologies, like artificial intelligence and machine learning, which are being used to enhance security monitoring and threat detection capabilities.

D. FISHY Security and Certification Manager

The FISHY platform aims at automating several security-related operations of each entity in the supply chain. Thereupon, this work presents the developed Security and Certification Management (SACM) component, which offers:

1. Hybrid security assessments that combine threat and vulnerability analysis, static analysis, penetration testing and runtime monitoring to provide a comprehensive analysis of the security posture of an enterprise and its systems.

2. Automated threat and vulnerability analysis.

3. Interoperability with various system platforms and programmatic connectivity to different systems via appropriate probes (e.g., event captors, test tools) that enable the gathering of monitoring and test evidence needed for assurance and certification assessments.

4. Sophisticated event processing capabilities that can realize complex signature or anomaly-based assessments.

5. Model-driven customizations to enable realization of various security standards and risk management requirements.

6. Advanced and customizable reporting for audit purposes.

The platform can be used through onsite installations or as-a-service. Under FISHY, the proposed solution has been applied in several piloting systems, including autonomous driving, farm-to-fork settings, and supply networks for wood-based panels. Nevertheless, it is generic enough and can be deployed in several other supply-chain ecosystems as well.

III. SECURITY ASSURANCE AND CERTIFICATION

The Security Assurance and Certification Management (SACM) component is responsible for monitoring, testing, and assessing complex Information and communications technology (ICT) systems under the scope of the FISHY project. Through an Evidence Collection Engine developed for the purpose, this component audits critical components

and processes of the ICT infrastructure while leveraging monitoring mechanisms developed in the context of the project. Based on that input, the component provides an evidence-based, (self-) certifiable view of the security posture of the ICT system. It also provides accountability provisions for changes that occur in said posture and the analysis of their cascading effects, supporting the runtime checking based on sets of associated claims and metrics.

The mechanisms developed for this component are also enabling and providing the design of audit procedures in ICT systems by considering all ICT components within the supply chain. Finally, the methodology and procedures for the automation of security (self-) certification are also part of this component, providing different certification models tailored to, e.g., specific security standards, service level agreements or legal and regulatory obligations (e.g., GDPR).

The real-time, continuous assessment of the security posture of the complex ICT systems is enabled by a purpose-built Evidence Collection Engine using Elasticsearch (ELK stack). This component is responsible for aggregating the required evidence from multiple sources related to the operation of individual components and the overarching processes where these components are involved. This functional group of modules also includes Audit and Certification functions, leveraging the evidence-based approach of the Assurance solution integrated into the platform. Several built-in Security Metrics addressing the Confidentiality, Integrity, Availability (CIA) principles among custom metrics tailored to the use cases of the FISHY pilot's needs are evaluated by the auditing component.

The SACM is composed of four independent modules (see Fig. 1), which are detailed in the next paragraphs: i) Security Metrics, ii) Audit, iii) Certification, and iv) Evidence Collection Engine. To provide security assurance and a certifiable view of each security assessment, the Security Assurance Platform (SAP) aggregates the assessment results by executing an automated workflow. The data model of the Evidence Collection Engine is based on the Elastic Common Schema (ECS) [13] and the data model for the auditing component is based on the security and privacy patterns described with Event Calculus (EC) [14].

A. *Security Metrics*

The Security Metrics component is a submodule that communicates with a respective database that contains the description of several prebuilt metrics in XML format. Triggered by the administrator from the Intent-based Resilience Orchestrator (IRO), the component pushes the selected latter metrics towards the audit-monitor component. These metrics are currently focusing on the CIA principles. For instance, at runtime: i) check that large amounts of confidential data are not retrieved from a monitored system of the supply network due to a data breach/leak operation, ii) examine that volumes of stored data within a supply chain node are not getting encrypted due to a ransomware attack, and iii) measure the availability of a (web) service and verify that it complies the thresholds of a Service Level Agreement (SLA), signed between the supply chain entities. Nevertheless, other type of metrics can be tailored as well, e.g., for privacy or performance. The XML files of the security metrics contain information regarding the type of the metric, the period of the evaluation, the type of the asset that the security metric is referred to among other internal information necessary that the audit component needs to operate properly.

Fig. 1 SACM: high-level view of the components

B. *Audit*

The Audit component is a monitor module that will be responsible for initiating, coordinating, and reporting the monitoring process results. Audit is a runtime monitoring engine built in JAVA that offers an API for establishing monitoring rules to be checked. The module is made of two basic submodules: i) the *main auditor*, and ii) an *audit manager*.

The main auditor is responsible for initiating, coordinating, and reporting the monitoring process results, and it is based on a monitoring framework, called EVEnt REaSoning Toolkit (EVEREST) [15]. When a security or privacy pattern is activated, it undertakes responsibility for checking conditions regarding the runtime operation of the components that implement the pattern. These conditions are specified within Patterns by monitoring rules expressed in EC-Assertion. EVEREST detects violations of monitoring rules against streams of runtime events, which are sent to it by different and distributed event sources, through the Event Evidence Engine. It also has the capability to: i) deduce information about the state of the system being monitored by using assumptions about the behavior of a system and how runtime events may affect its state, ii) detect potential violations of monitoring rules, and iii) perform diagnostic analysis to identify whether the events causing a violation are genuine or the result of a system fault or an attack. Fig. 2 depicts SACM's graphical interface for two collected events, where one satisfied and the other violated the confidentiality property of a security pattern.

The audit manager submodule interacts with the REST controller component that initiates and provides monitoring assessments. It is implemented in the Docker environment, which offers flexibility, portability, and parallel execution capabilities.

Furthermore, the Audit component includes an Audit database in its internal architecture (MongoDB), which holds all the important attributes to conclude the auditing assessment capability. Also, Audit includes a message broker (RabbitMQ), which interacts with the Evidence Collection Engine through an Event Channel and handles the events received from the Audit Manager component. Finally, the Audit component may communicate with an external database that holds the security assurance model and its components.

C. *Certification*

The purpose of the Certification component is to provide an evidence-based security reporting and certification to the needs of different stakeholders ranging from senior

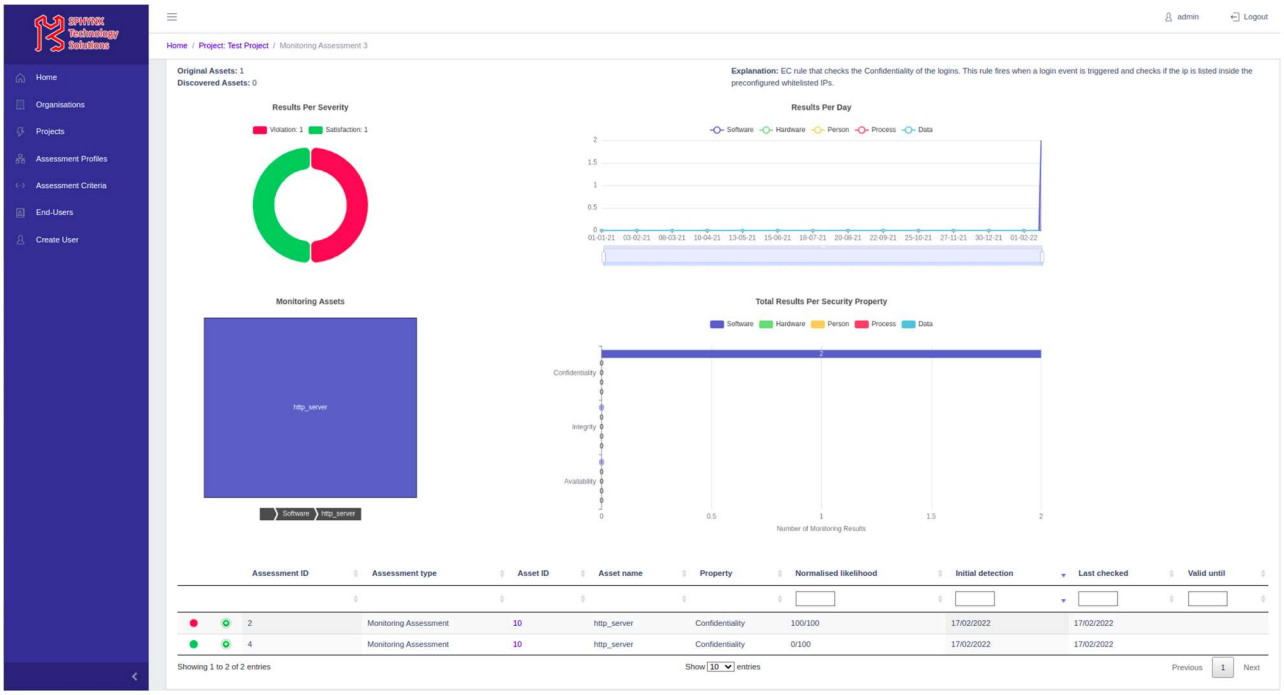

Fig. 2 SACM graphical interface – Illustrates the overall audit details for two collected events, one satisfied and the other violated the confidentiality property of a security pattern.

management to external auditors and regulators, incorporating different access level to the respectively users. The latter component supports the creation of specialized reports based on the findings of the Audit component while it may inform the IRO component for the former results.

Certification process checks for compliance of technical and organizational requirements of the auditee (organization trying to achieve compliance to some standard). FISHY does not focus on a specific standard but rather tries to build a continuous process of compliance checks of technical requirements (and even these specific ones) of a generic security standard similar to EUCS [16]. The results can help with the decisions with respect to additional controls being applied to the target infrastructure (e.g., in the IRO of FISHY). In this process, each Audit Metric Instance is equipped with an additional information (attributes and values) whether the measurement passes or fails expected value of the metric. These values are provided by the configuration process (through set of rules) of the certification component (its API). Evaluation of certification compliance means evaluation of the rules (organized as a tree) of values of the audited metrics.

D. Evidence Collection Engine

The Evidence Collection Engine component is used for real-time, continuous assessment of the security posture of the complex ICT systems as it aggregates in real-time, cross-layer evidence pertinent to the security posture of the ICT infrastructure. This module uses incoming data from Event Captors, a software module that, based on collected data and triggering events, may filter this information to disclose only events that are relevant for the deployed rule sets, and pushes the latter towards the audit component for evaluation.

The Evidence Collection Engine is also developed around Elasticsearch. Data and events are collected through several lightweight shippers, named Beats (e.g., Filebeat, MetricBeat, PacketBeat) that centralize log data and forward them to Elasticsearch. Event Captors are activated when the appropriate event happens. They query Elasticsearch, evaluate the results, and push back the relevant information to the Audit component for further evaluation. Also, Logstash is added in the chain between Beats and Elasticsearch. Logstash is an open server-side data processing pipeline that ingests and process data from a multitude of sources. Here, it has the role of an aggregator/augmenter of data before these are sent to Elasticsearch. Currently, Event Captors are aligned to facilitate the security metrics provided by the respective component of SACM and with respect to the CIA venerable model. However, these captors can be augmented with several others in order to provide a more user case- or pilot-oriented approach. Event Captor's tool is initiated through respectively REST calls from the Audit module, while it communicates with the Elasticsearch via the respective API.

Examples for CIA principles may include captors that: i) collect information from database logs where a rule set checks that an abnormal burst of reads is not getting performed due to a data breach, ii) gather information concerning the running processes of a system where a rule set examines that large portions of files are not getting read and deleted with encrypted copies being produced, and iii) check wherever a service is up and running (e.g., by periodically performing an HTTP request to a web service and recording the HTTP response code) with a rule set measuring the uptime or the mean time to response to service unavailability incidents and compare these values to agreed thresholds on SLAs.

IV. Demonstration in SADE

This Section presents the validation of the SADE use case. This use case focuses on certifying software versions that are safe according to the manufacturer of the IoT device managed by the FISHY platform. There was also an effort on deploying the necessary services for this validation in the 5Tonic environment, the 5G laboratory in Leganes/Spain [19].

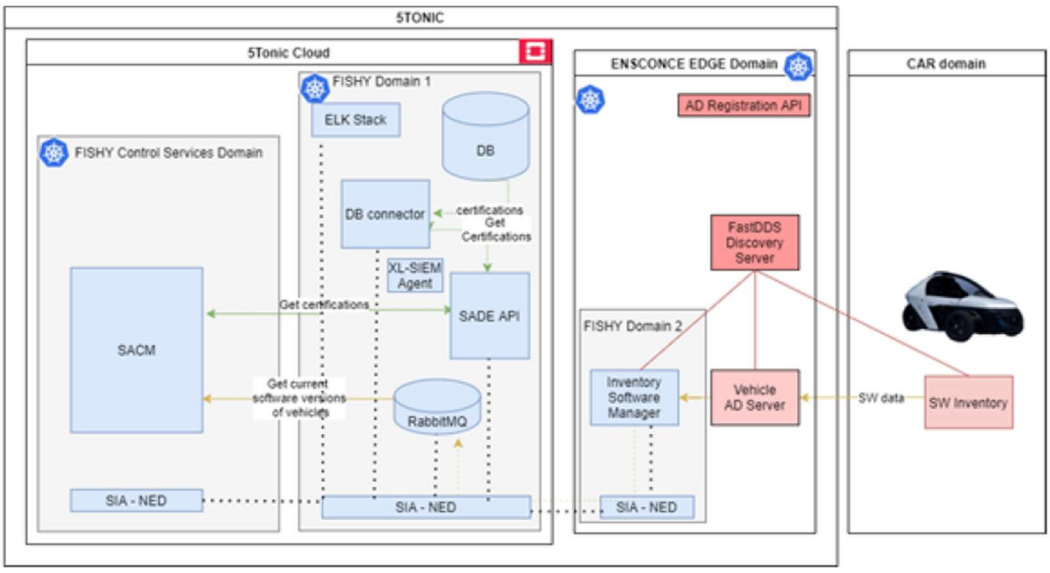

Fig. 3 Communication diagram of the SADE use case

A. Motivating Scenario

Given REMOTIS [18], an autonomous vehicle, the aim of this FISHY use case is to secure all sensor (LIDAR, video cameras, driving parameters, etc.), actuators (brakes, acceleration, steering), and the car itself using FISHY technologies and communication protocols.

From a network perspective, the aim is to develop a highly robust and secure telecom interface between the vehicle and the server (Cloud / Edge Computing), that must be able to provide real-time data transfer and the management of all the actors. For that, the FISHY Secure Infrastructure Abstraction (SIA) functional block provides the means to define an Abstraction of Network Edge Device of the REMOTIS car. Implementation allows to Offload the Security Applications into the EDGE Network.

For that purpose and as representative of the current trends in Automotive Industry, REMOTIS concept car can be expanded with the following services:

- **Biometric Facial Key:** The car is activated with the face of the car user, being able to track and record when each user was driving it as well as information about his/her driving style.

- **Sensors Secure Environment:** Currently, REMOTIS relies on many of the sensor's own security policies to control crypto resources such as passwords, certificates, capabilities (codecs), etc. A single entity can be created to manage those sensors capabilities in a unified manner.

B. SADE Vertical Application

For the validation of the use case, there is an ecosystem of services. These services are deployed at different segments of the infrastructure, depending on the need and the nature of the services. There are several different points for this validation [19]: Cloud (5Tonic), 5G EDGE (ENSCONCE), and the outside world. Several services are in the cloud, while others are in the EDGE where the vehicles are connected. Finally, the vehicle is connected in the outside world via 5G.

Each service has a fixed IP address. Communication between the services uses this address, that belongs to a specific subnetwork, and it is managed by the Network Edge Device (NED) of the Secure Infrastructure Abstraction (SIA) domain. Cloud deployments are done as virtual machines using OpenStack by default. The most complicated integration concerns the integration inside the EDGE as part of the ENSCONCE platform (a Kubernetes-based Edge Compute Platform) [19]. In the current integration, the NED has been separated from the sandbox, deploying the component as a standalone application using the ENSCONCE web portal.

After the provisioning, point-to-point connections have been created between the other FISHY domains. The deployments of the NED and the Software Inventory service have been manually edited to associate some interfaces, allowing the communication through those interfaces with the services located in the three domains.

The second component that is integrated is the SACM. SACM collects information about the software versions of the IoT devices in the vehicle. This information is stored in the RabbitMQ deployed in FISHY domain-1. SACM gets the list of versions of each component by making a request to the SADE REST API. Once all the data is obtained, it checks if everything is correct or if there is a problem with non-certified versions. Fig. 3 illustrates the communications diagram, where the dotted lines are communications through the SIA/NED.

C. Security Enhancements in SADE Pilot

Table I shows an example of information that Original Equipment Manufacturers (OEMs) add, using the FISHY dashboard to certify their software versions. This information is stored in the database.

TABLE I. EXAMPLE OF INFORMATION OEMS

Model	TempMeterXXX
SW Version	1.1235
Safe Update Link (optional)	https://company.com/updates/TempMeterXXX/1.1235/firmware.bin
Update Checksum (optional)	5a000ca5302b19ae8c7a66149f3e1e98

Data from vehicles are sent to FISHY in the form of a JSON object (see Fig. 4), which includes: a Unique Universal ID (UUID), the Timestamp, and related Metadata.

SADE sends this information to a RabbitMQ exchange, deployed in the Sandbox of the FISHY domain-1 as a k8s

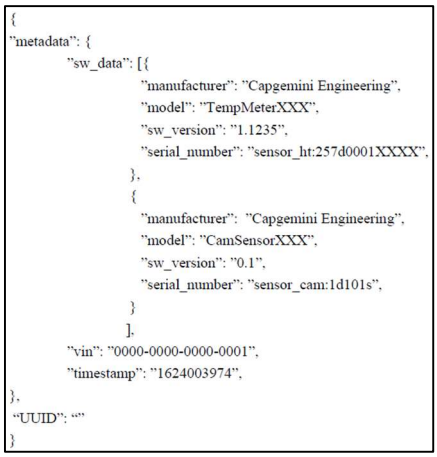

Fig. 4 JSON sample for exchanged messages

POD: i) SACM get JSON messages and parses the received information, and ii) SACM compares with SW certification versions provided by OEMs that can be recovered from the SADE API using REST. Then, there is one *rule set* that checks if one version received is not certified: i) FISHY notifies/alerts users related to the compromised vehicle, ii) FISHY enforces *Update** policy against SADE Service (REST API module).

If an updated version model is certified and contains a safe link for an update, that link must be provided; if not, the service will start a recall notification. FISHY just does not send any link in the POST request.

On the other hand, data collectors send logs to the Cross-Layer Security Information and Event Management (XL-SIEM) of FISHY. XL-SIEM in turn sends elaborated events and alarms to the Risk Assessment Engine (RAE) that can calculate in real-time the cyber risk exposure. An agent of the XL-SIEM is deployed as part of the FISHY appliance and sends logs for the XL-SIEM to detect those attacks. This agent is in charge of obtaining the log files from a number of services related to SADE use case and makes them available to the RAE. The agent is deployed in the same CLOUD infrastructure (same domain) as the other services of the use case, allowing access to the logs by mapping volumes to a common directory, which is accessible by the agent.

Actions like software update or send notifications to car's owner may also be implemented in future iterations.

V. Conclusions & Future Work

Cyber-security is one of the hot research topics at the time. Continuous attacks on global supply-chains are making their protection essential. This paper presents a continuous security assurance and certification solution for supply-chains. This proposal is implemented under the EU funded project FISHY, and its successful deployment and demonstration on the secure autonomous driving pilot is presented in this work.

Nevertheless, the solution is general and can be applied in other sectors as well. This will be the main focus of future deployments. Also, there will be further research on the automated alerting of the user or even the automated administration of the system based on AI procedures.

Acknowledgment

This work has received funding from the European Union's Horizon 2020 research and innovation programmes under grant agreements No. 952644 (FISHY), No. 101021659 (SENTINEL), No. 883540 (PUZZLE), No. 957337 (MARVEL), and No. 101070599 (SecOPERA).

References

[1] Mohamed, B-D, Elkafi, H., Zied, B. (2019), Internet of things and supply chain management: a literature review, International Journal of Production Research, 57: 15-16, 4719-4742.

[2] Manavalan, E., Jayakrishna, K. (2019), A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements, Computers & Industrial Engineerging, Elsevier, 127: 2019, 925-953.

[3] Hassija, V., et al. (2021), A survey on supply chain security: application areas, security threats, and solution architectures, IEEE Internet of Things Journal, IEEE, 8:8, 6222-6246.

[4] Tukamuhabwa, B., Stevenson, M., Busby, J. (2017), Supply chain resilience in a developing country context: a case study on the interconnectedness of threast, strategies and outcomes, Supply Chain Management: An International Journal, Emerald, 22:6, 486-505.

[5] Skula, A., et al. (2022), System security assurance: a systematic literature review, Computer Science Review, Elsevier, 45, 1-29.

[6] Lakka, E., et al. (2022), Incident handling for heathcare organizations and supply-chains, IEEE Conference on ICT Solutions for e-health (ICTS4eHealth), IEEE, Rhodes Island, Greece, 1-7

[7] Bechtsis, D., et al. (2017), Sustainable supply chain management in the digitalisation era: the impact of automated guided vehicles, Journal of Cleaner Production, Elsevier, 142:4, 3970-3984.

[8] Markets and Markets (2022), Supply chain management (SCM) market by component, deployment mode, organization size, vertical and region – Global Forecast to 2027, Available on-line at: https://www.marketsandmarkets.com/Market-Reports/supply-chain-management-market-190997554.html (Accessed 21/03/2023).

[9] Cheung, K.-F., Bell, M. G. H., Bhattacharjya, J. (2021), Cybersecurity in logistics and supply chain management: an overview and future research directions, Transportation Research Part E: Logistics and Transportation Review, Elsevier, 146:1, 102217.

[10] Alkhadra, R., et al. (2021), Solar Winds hack: in-depth analysis and countermeasures, IEEE International Conference on Computing Communication and Networking Technologies, Kharagpur, India, 1-7.

[11] Kilovary, I. (2023), Cybersecuring the Pipeline, Forthcoming, Houston Law Review, 60:1, 1-45.

[12] Apoorv, Md. K., Vineet, K. (2022), Security Assurance Market Research, 2031, Allied Market Research Available on-line at: https://www.alliedmarketresearch.com/security-assurance-market-A31446 (Accessed 21/03/2023).

[13] Elastic Common Schema (ECS) Reference, Elastic, Available on-line at: https://www.elastic.co/guide/en/ecs/current/index.html (Accessed 21/03/2023).

[14] Hatzivasilis, G. (2020), AI-driven composition and security validation of an IoT ecosystem. MDPI Applied Sciences, 10:14, 4862, 1-31.

[15] Spanoudakis, G., Kloukinas, C., Mahbub, K. (2009), The SERENITY Runtime Monitoring Framework, Security and Dependability for Ambient Intelligence, Springer, ADIS 45, 213-237.

[16] EUCS – Cloud Services Scheme, ENISA, Available on-line at: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme (Accessed 21/03/2023).

[17] 5TONIC Laboratory, Available on-line at: https://www.5tonic.org/about-us/ (Accessed 21/03/2023)

[18] Capgemini Engineering, REMOTIS: remote intelligence system for automobiles, Availabla on-line at: https://capgemini-engineering.com/es/en/insight/remotis-remote-intelligence-system-for-automobiles/ (Accessed 21/03/2023).

[19] Sabella, D., et al. (2021), Global MEC supporting automotive services: from multi -operator live trials to standardization, IEEE Conference on Standards for Communications and Networking (CSCN), Thessaloniki, Greece, 7-13.