Improving Detection Capabilities in OT Environments Through Multisource Data Sensors

Jussi Simola, Arttu Takala, Riku Lehkonen, Tapio Frantti and Reijo Savola
University of Jyväskylä, Finland

Jussi.hm.simola@jyu.fi
arttu.h.takala@jyu.fi
riku.p.lehkonen@jyu.fi
tapio.k.frantti@jyu.fi
reijo.m.savola@jyu.fi

Abstract: This research focuses on implementing cyber threat detection in OT environments by combining data from IT and OT sensors and logs to enhance SOC's situational awareness. OT environment is challenging to monitor and includes various sensors. We deal with the key concepts and differences of the industrial operating environment, which create challenges compared to the traditional IT environment. This is important because the policies defined at the European level for the NIS2 regulation will affect all member countries. Hostile actors cause security challenges highlighting the importance of critical infrastructure protection. Cyber security solutions have often solely focused on IT threats, but similar investments have yet to be made in response to the challenges of the OT environment. The security solutions of OT operators rely heavily on solutions from the IT side. Here, we delve into whether it is possible to find threats in the IT/OT ecosystem by combining data from the IT and OT sides. All threats are not found by monitoring data separately from IT or OT sources but we identified hidden threats by monitoring and comparing IT and OT data. This paper shows the importance of detecting OT threats. The study proposes how the detection of cyber threat capabilities should be developed.

Keywords: Operational technology, Testbed, Security operations center, Threat detection, Situational awareness

1. Introduction

NIS2 will create new requirements for companies and their services and digitalized products. Targeting all medium- and large-sized companies is vital to the continuity of the economy. Small vital companies have also followed the main rules and guidelines European Commission (2022). Authorities and authorized actors (for example, service providers of security operation centers) are in a new situation with legal measures set in regulation, which will affect the services they produce. The directive gives the mandate to act so that regulation can be fulfilled. In relation to the NIS2, the European Union-level agency (ENISA), supports cybersecurity policy and aims to enhance and develop services, ICT products, and processes in the European Union (ENISA, 2023). The NIS2 directive will enhance the resilience of network and information systems. There will be two categories for the enterprises' essential and important industries. EU member countries must adopt a national cybersecurity strategy. There were differences between essential providers and digitalized services in the first version of the NIS. This gap is now removed. NIS2 classifies organizations based on their essentiality into two categories: essential and important (European Commission, 2022). However, it has been seen that the European Union will follow the U.S.'s cybersecurity regulations guidelines. Protecting the energy sector and supplying distributed energy resources is one of the main objectives of the new cyber security regulations. This paper concentrates on detection capabilities in OT environments through multisource data sensors at the operational level. It answers the questions “how to enhance OT-SOC-related cyber security capabilities” and “how to develop a governance model”. The paper uses the demonstration and testing platform to develop the governance model. The project’s main goal Is to develop a governance and reference model for the industry stakeholders.

2. Elements of the Research

The CSG (CyberSecurity Governance of operational technology in sector-connected smart energy networks) project will develop a leading-edge cybersecurity sector integration governance model to cover cybersecurity solutions, processes, and methods for operational technology environments. The project aims at considerable cost savings and scalability. The European Union's common aim in the OT/ICS environment is enhancing cyber situational awareness.

Standardization, protocols, or guidelines are not only requirements that are good to follow. Cybersecurity governance is a part of the overall corporate governance management system. It is also a part of company strategy, working culture, and daily routines. Employees are an essential part of cyberphysical ecosystems.

Governance requires cohesion between the crucial elements of the cyber-ecosystem. The importance of the well-organized governance model is emphasized according to the company's size.

It is crucial to connect corporate governance to the cybersecurity governance framework. Essential is how the board of directors and decision-makers approach their strategic goals; as mentioned in previous research (Simola & et.al. 2023), there are four main levels of governance: political, strategic, operational, and technical/tactical. Figure 1 illustrates how cyber-attacks can be seen in an operational technology environment and industrial systems (GAO, 2021).

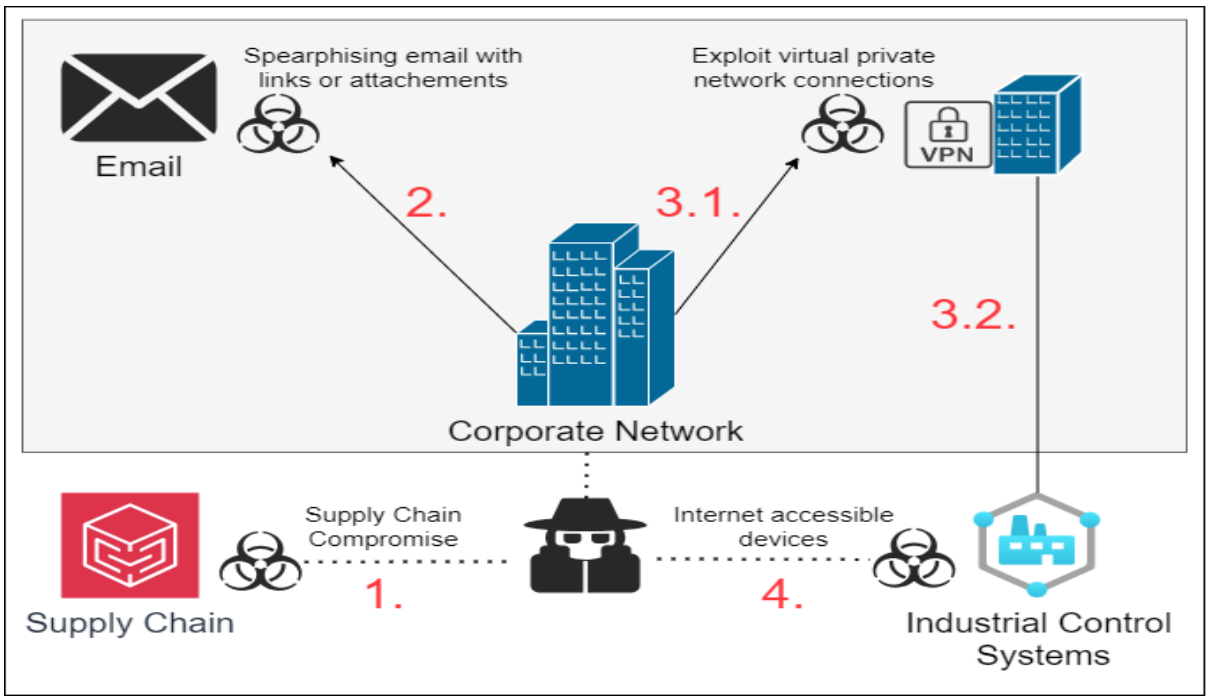

Figure 1: Example of the cyber-attacks against Industrial Control Systems modified from (GAO, 2021)

Attackers compromise the supply chain of industrial control systems by manipulating products, such as hardware or software, before receipt by the end consumer. Another way is to send a "spearphishing" email with links or attachments that include malicious code to a specific individual, company, or industry to gain access to a corporate network. Then, attackers exploit services that allow corporate users to connect to network resources from a remote location, *e.g.*, virtual private network, and the attackers use these services to gain access to and attack industrial control systems. Lastly, attackers can access industrial control systems in cases where systems have direct connections to the internet (GAO, 2022).

2.1 Situational Awareness

Humans are often the weakest link in the operational technology environment. Common situational information is crucial when the aim is to enhance the exchange of information between humans and devices. The formation of the mental model is essential within the team and between the team members to reduce overlapping work (Endsley, 1995). According to Endsley (1995,1988), Situation awareness is the perception of the elements in the environments within the volume of time and space, the comprehension of their meaning, and the projection of their status shortly. Perception is an essential ability in the industrial environment. The formation of situational awareness requires several elements that are connected to each other. Humans cannot process large volumes of data, quickly and consistently. Flexible autonomy should provide a smooth, simple, seamless transition of functions between humans and the system. Regulations of the European Union set new requirements for the formation of cyber situational awareness. Human or automated systems are essential factors that enhance communication methods, procedures, information gathering, and sharing. Mechanisms for that are under development.

2.2 Command and Control and Security Operation Centers

Command and Control Center refers to operative control processes and procedures of military actions. Functionalities and work tasks changed to the Computer Emergency Response Center, which later changed to the Security Operations Center, consisting of different functionalities and actions that control, monitor, and supervise customers' networks (Vielberth et. al. 2020).

2.3 Industrial Control Systems

Industrial control system (ICS) means several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective, such as manufacturing, and transportation of matter or energy (NIST 2022).

2.4 Mitre Att&ck

MITRE ATT&CK framework serves as a universally available repository of adversarial strategies and methods, derived from actual observations. It operates as an intermediary level adversary model, bridging the gap between fundamental elements like exploits and vulnerability databases, and higher-level models such as Cyber Kill Chain (CKC) (Strom et al., 2018). However, MITRE ATT&CK does not operate as a linear sequence chain. It requires analysts to construct the Tactics, Techniques and Procedures (TTP) chain manually by choosing the tactics and techniques that have occurred from within the framework of the MITRE ATT&CK model in the order of occurrence. According to Pols (2017), a technique is not solely associated with a specific tactic as several tactics across various stages of an attack chain frequently utilize it. This increases the complexity of developing TTP chains.

3. Requirements of the OT Environment

3.1 Technical Cybersecurity Requirements

Standards may leave room for interpretation, leading to lower maturity than intended, *e.g.*, configuration change may be logged, but not in-depth, which would be beneficial for incidence forensics, such as what was changed, what was its value changed to. The following standards are crucial in the operational technology environment. The ISA/IEC 62443 series of standards includes control systems used in manufacturing and processing plants and facilities, as well as geographically situated distribution operations and facilities. It is also used in automated and remotely controlled and monitored assets (ISA, 2021). As Table 1 illustrates, the connection between security programs and cybersecurity governance is essential.

Table 1: Relevant Operational Technology-related Standards

Standards and guidelines	Details
IEC 62443, (ISA, 2021)	Security Standards for Industrial Automation and Control Systems
Management of Information security ISO/IEC 27001 ISO/IEC (2022)	Standard for Information Security.
RMF for Information Systems and Organizations NIST 800-37 r2- (NIST, 2018)	Risk management Framework
Guide to Operational Technology (OT) Security SP 800-82r3 (NIST, 2023)	The publication consists of guidance on how to secure operational technology (OT)
Security and Privacy Controls for Information Systems and Organizations NIST 800-53 r5. (NIST, 2020)	Catalog of security and privacy controls
Guide to Cyber Threat Information Sharing NIST SP 800-150 (NIST; 2016)	The publication consists of guidelines for establishing and participating in cyber-threat information-sharing relationships
Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations NIST SP 800-161r1 (NIST, 2022)	The publication consists of identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations

Figure 2 illustrates the importance of the connection between cybersecurity governance, and supply chain management. Still, more than following the separate standard, ISA/IEC 62443 is needed to enhance the overall cybersecurity ecosystem in the operational technology environment.

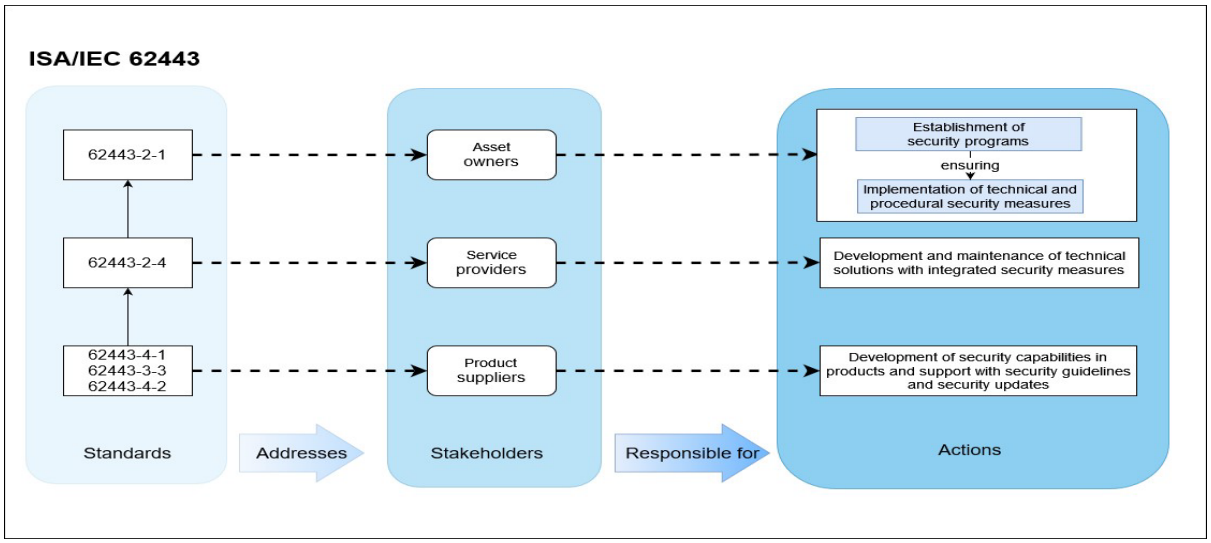

Figure 2: Formation of IEC 63224 Standard, modified from (ISA, 2021)

3.2 Information Exchange Between the Decision-makers

Organizations' decision-makers must have reliable information about the events, risks, and vulnerabilities. The information needed for operational-level management steers the practical processes of information sharing and exchange. The information must be in a form that is understood in the same way, and it cannot change when it changes from one format to another.

3.3 Contents of the Data Exchange

A couple of factors must be taken into account: a) relevant information for stakeholders. Stakeholders must be able to gather and share relevant information with the appropriate stakeholders. b) Company secrets. Companies have their own secret information that they cannot share. This kind of information is classified and belongs under business secrets. Despite that EU, EU-level regulations such as the NIS2 requirements prevent the holding of information about events that may be essential for protecting critical infrastructure. c) Anonymization (difficult to reach the required level without losing information). When information is shared between the SOCs or industries, it is crucial that sensitive information is shared in a way that sensitive information does not prevent compliance with privacy policy. The problem is that sensitive data is relatively easy to find, for example, by combining pieces of data. d) Trusted partners. Very often, that refers to the 3rd party stakeholders, for example, service providers. Every trusted partner must follow the same principles about managing cybersecurity-related issues. e) Legislative requirements. Legislation forms the basis for the standardization. Information sharing and exchange mechanisms should be based on the same standardized levels that regulation requires.

3.4 Requirements of the Information Exchange at the Interface

Efficient information and data sharing require different capabilities in all organization stages. As previous research Simola & et. al., (2023) has indicated, information and data must be changed from the technical environment to the management level. Operational actions require both because sharing information without data is impossible. At the management level, one needs to maintain situational awareness, which requires a combination of information. If the information is achievable and reliable, decision-makers may supervise the operational actions and, the situation of the business and how the strategic goals have been achieved. Cyber situational awareness is one part of overall situational awareness. That means the information must flow between the decision-makers and be unchanging between the units. If the content changes, the situational picture between the units “blurs”.

3.5 Defensive / Mitigations Suggestions

MITRE ATT&CK suggests certain defensive mitigations against techniques and sub-techniques for ICS, enterprise, and mobile environments. These mitigations, however, lack context of the attack's TTP chain and require expert knowledge to know which mitigation is applicable and beneficial to prevent further attacks or how these mitigations are meant to be integrated. For example, network sniffing is provided with mitigation strategy of multi-factor authentication (MFA), but it offers no guidelines on integration or reasoning why it mitigates network sniffing. Additionally, network sniffing may occur both in ICS and enterprise environments, but MFA has different limitations for implementation and functionality depending on the environment it is used in.

The Common Vulnerability Scoring System (CVSS) is an open-access industry benchmark for gauging the gravity of security vulnerabilities in computer systems. It aims to allocate severity scores to such vulnerabilities, enabling those responding to prioritize their actions and resources based on the level of threat. CVSS is used to indicate the severity of a vulnerability in information security and is a fundamental component of many vulnerability scanning tools. Conversely, the Common Vulnerabilities and Exposures (CVE) is a glossary of all publicly disclosed vulnerabilities that includes the CVE ID, a description, dates, and comments (Risto, 2018).

The National Vulnerability Database (NVD) plays a crucial role in enhancing the CVE List, which is overseen by the MITRE Corporation and supported by the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). The NVD enriches this list of publicly known cybersecurity vulnerabilities and exposures by providing additional analysis, CVSS scores, transforming data points into SCAP (Security Content Automation Protocol) datatypes, and offering a comprehensive search engine and specific APIs (Application Programming Interfaces). Security teams can leverage NVD's data feeds to integrate vulnerability intelligence into existing workflows and tools. The NVD supports these feeds by maintaining synchronization with the CVE to ensure that any updates to the CVE List are immediately reflected in the NVD (NIST, 2024).

3.6 Current Situation in the Operational Technology Environment

IT environments are commonly capable of centralized logging and implement it in systems where logs require audit. However, due to the large amount of collected and transferred data, some systems cannot implement centralized logging. To combat this, these IT environments are working towards implementing distributed and decentralized log systems, such as blockchain log systems, to reduce and equalize network overheads and latency occurring within the system. Conversely, OT environments still use local log storage on IED's, such as control relays, and have only recently introduced capabilities on new IED's towards centralized logging. Centralized logging in OT environments is limited due to the hardware and software constraints of older equipment. This limitation hinders the introduction and integration of IT cybersecurity solutions and practices, which are designed with centralized logging and easy access to logs and data in mind.

4. Research Approach

4.1 Test Environment

The connection between the test environment and the designing cyber security governance model is the main aim of the project. Testbed developed for these use cases implements high-end OT hardware and software solutions commonly used in critical infrastructure. They are capable of network connection, which enables environments to be operated, maintained, and surveyed remotely. This enables cybersecurity-related use cases that target the system holistically, as well as each component, their connecting interfaces, and specifically the addition of IT solutions in OT environments. At present, there aren't any widely recognized comprehensive SOC standards or sector-specific guidelines. Most of the existing SOC guidelines are authored by security vendors. The existing guidelines from MITRE SOC suggest the deployment of IT cybersecurity sensors on host machines and network environment. These sensors and their data are essential for making knowledgeable decisions (Knerler, Parker, Zimmerman, 2022). To illustrate the necessity for more comprehensive sensor integration in OT environments, a SOC will be put into place to enhance detection capabilities using a variety of sensor data sources. This implementation will underscore the advantages provided by these comprehensive sensors when the system faces attacks of varying techniques, tactics, vectors, and targets. For example, sensors at different layers might inform SOC of their layer's status and state, but only following one layer will leave other sections vulnerable to attacks. In addition to this, the combination of data sensors may provide additional value towards workflow and process validation, especially when machine learning solutions are used to analyze the combined data flow. The developed system will, in this way, aid in developing a governance model for critical infrastructure

by providing data. Additionally, it enables the development of maturity levels and highlights the possible risks of different maturity IT implementations in OT environments. The test environment is described in Figure 3.

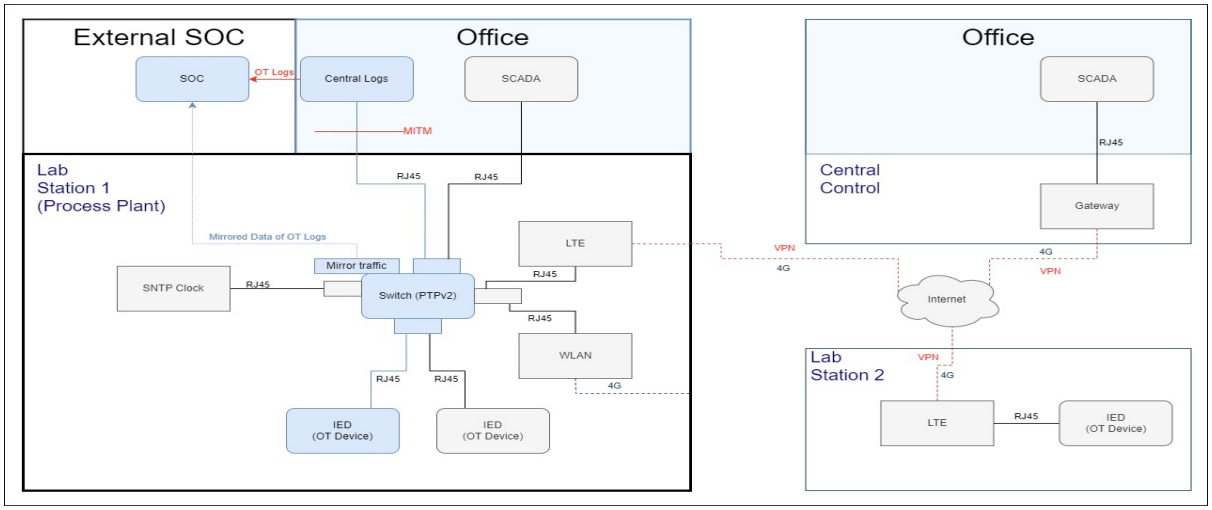

Figure 3: Test environment

The laboratory environment consists of a production facility, an office, and an external SOC (Security Operations Center) solution. The production facility can also be accessed remotely via the internet. Excluding remote connections, the connections are unencrypted. A switch, which serves as the interface between the office and the production facility, mirrors traffic to the SOC via a separate connection. OT Device logs are sent from Central Logs via a separate connection to the SOC. The Man-In-The-Middle (MITM, man = person, device) scenario, which is the focus of this paper, is indicated in red. PITM data compromise is carried out with an additional device which is added to the connection between the process plant and the office. Compromised OT logs are also highlighted in red. The devices utilized in the scenario are highlighted in blue.

4.2 Background of the Use Cases

The use cases simulate the real Operational technology environment, and we must test several threat combinations to see how attacks can be executed and how they affect the devices. By comparing different kinds of logs and other information, it is possible to gather important information about how to affect the operational and technical levels. Testing is important because of the multiplicity of disadvantages. If false information transfers from the lower to the upper level, situational awareness is preserved, and it is impossible to achieve and transfer the right information from the different levels. False information causes supply chain problems and leads to multiple disadvantages, such as rising costs, production interruption, and reputation damage.

The connection between the test-bed results supports governance model development and creates a new platform for industrial operators. Cybersecurity-related supply chain problems at the technical level affect the operational and strategic levels. Workable industrial environments such as energy power supply require that electricity components are reliable, and information flows securely in the network. The link between simultaneous tests and real-world is essential in our studies. Vulnerabilities must be found, and obstacles affecting the continuity management and supply chain management must be identified. This research concentrates on the formation of logs and information needed to maintain situational awareness at all stages of the business environment. The same kind of electricity components are used in different industry sectors. If there are the same IT/OT-related problems, European Union-level cybersecurity requirements still need to be fulfilled (European Commission, 2021). That indicates that the detected vulnerabilities must be shared within the industry-based sectors, between the sectors, and with the authorities. SOCs are crucial to information sharing, and the technical capabilities are directly connected to the SOC maturity in detection processes. Information and data exchange between the SCADA and SOC is crucial, but it is only relevant if the operational environment has combined cyberphysical sensors. Gathering information from equipment by forming logs becomes challenging if there is no capability to gather information.

4.2.1 Determining the Use Cases

The main target is the integrity of the data, not the process that the data is gathered from. The data transfer process is monitored so that the data values remain constant. it is not monitored whether someone has initiated the process. Cybersecurity attacks may occur at different sections of the environment with different footprints.

We compare the two points to each other and their space in Table 2. Cause and effect are not considered.

Table 2: Comparing two points and their space

Test 1 and 2	Possibilities
Two sources in the test	The attack may occur only in one section, where one source registers it.
Two sources in the test	Possible to validate process or source integrity when used in unison

As Figure 4 illustrates, the real-world counterpart to the use case is depicted. The production plant's control system is located in a separate office space. The data transfer between the production plant and the office space is monitored remotely in a separate SOC. In the use case, the attacker has access to the physically less protected office space. The attacker modifies the data transferred between the OT device and the central log. By modifying data delivered to the central control, the attacker can hinder the situational awareness of the control system, evade installed defense mechanisms, and disguise footprints left in the system. MITRE ATT&CK considers the following attack as a Person-In-The-Middle technique and a defense evasion tactic.

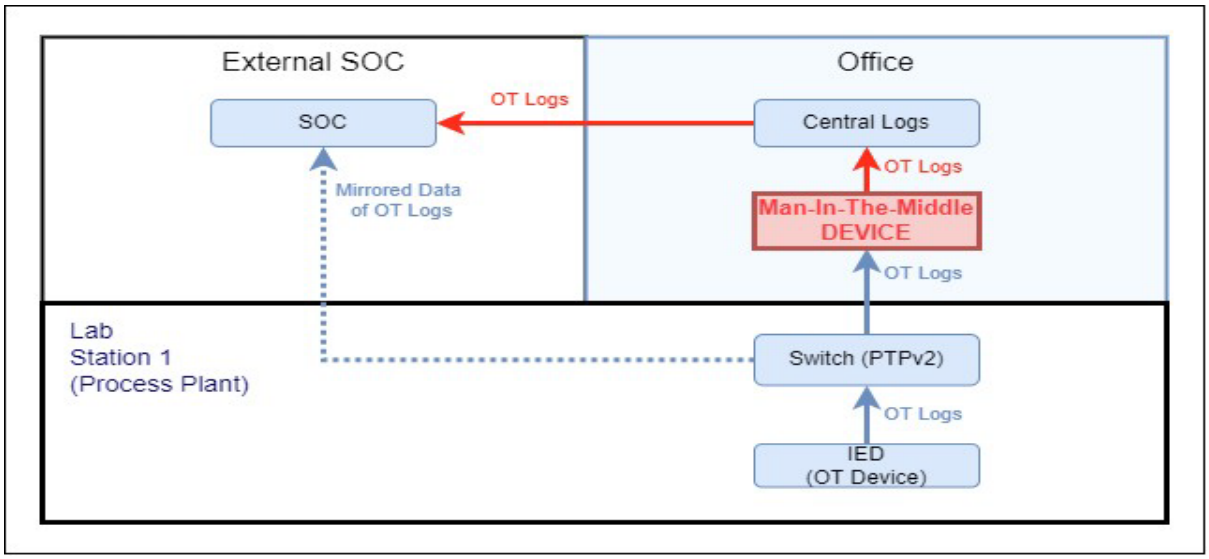

Figure 4: Research lap setup versus real-world

A countermeasure against PITM attacks has been developed, which involves the inclusion of additional sensors at various points within the network. These sensors are isolated from the main network infrastructure to minimize interference with regular data transfers. This applies to data originating from both Operational Technology (OT) and Information Technology (IT) devices, as well as from network-attached sensors, such as data diodes or Near-End Crosstalk analyzers. The data collected by these sensors is transmitted to the SOC at two distinct points: midway at the switch and at the endpoint of the central logs. By comparing the data logs from these different points, an inspection of the device or log status from various locations within the network can be conducted. This approach allows for a more comprehensive situational awareness of the system status.

However, the introduction of additional sensors and data collection points inevitably leads to an increase in network data load and device data processing. To mitigate this, the additional points should be isolated from the normal network environment, thereby enhancing network security without significantly impacting its performance. Another limitation that may occur in OT environments is hardware limitations, such as OT devices lacking capabilities of isolated reporting.

4.3 Research Methodology

The research methodology used is based on the view of design science research (Hevner, 2007; Hevner, A. & Chatterjee, 2010). We have the suitable equipment, software, electricity, and network solutions for the tests. By utilizing the products, it allows us to test different kinds of scenarios and cyber-attacks. The research compares the scenarios-based use cases and the tests we have done are connected to the comparing log information.

Tasks of use cases will produce new data for the governance model and help to develop features and functionalities of the security operations center. It will bring added value to the IT-SOC features because there are missing signal-processing elements that enhance the formation of situational awareness. Gathering data, such as weak signals from the industrial environment where the old-fashioned machines are crucial. Identifying the emergency point, where SOC and detection features must react is critical. In Industrial Control Systems such as SCADA, intrusion prevention or detection tools are relevant machines that we must have under the secured control of operations. We will apply a widely used design science research methodology used traditionally in software and system development.

The laboratory environment at the University of Jyväskylä generates new information about cybersecurity-related technical issues. Components, devices, and software from stakeholders form a new base of knowledge for the governance model development work. The developed and tested use cases highlight crucial technical challenges that generate added value for the operators of the ICS environment. Combining information from sector-based enterprises, analysis of external requirements, and results from the testbed generate a suitable solution for the actors of the critical infrastructure. Results from the testbed produce a new knowledge base into divided classes that are possible to connect to the different kinds of external and internal requirements that have been considered in the analysis of the ICS-related environment. We have used the Delphi method (Worrell J., Di Gangi P., Bush A. 2012). Professional team members also have skills and experience in analyzing the research data.

Regarding (Nunamaker et al., 1991), the multi-methodical approach consists of four case study research strategies: theory building, experimentation, observation, and systems development research based on a systematic analysis of gathered data. We have used Yin´s case study research strategy (Yin,2017), which concentrates on targeted research problems and questions. Yin (2017) identifies five components of research design for case studies: the questions of the study; its propositions if any; its unit(s) of analysis; the logic linking the data to the propositions; and the criteria for interpreting the findings. In this research, our focus is on the question: What are crucial factors and elements that may set obstacles for enhanced continuity management and supply chain management as a part of cyber situational awareness in the OT/ICS environment? We have used official literature sources such as official publications and academic publications in this work. In this research, we concentrate on external industry-specific supply chain-related cybersecurity requirements.

5. Findings

Devices should have the capability to monitor their operations and create their own log entries. These logs are crucial for maintaining a secure and efficient network. However, in OT environments, there are hardware limitations in the automatic mechanism for sending these logs to a centralized location.

To address this with current hardware, a separate network is needed to ask the devices (referred to as relays) about their status and collect this information centrally. This centralized collection is essential for computing needs. However, a challenge arises concerning where this log information should be stored.

If a device retains its log data indefinitely, it opens up the possibility for artificial intelligence solutions to request necessary data from the relay. But, if an unauthorized entity gains access, the reliability of this data is compromised. Therefore, the relay should actively send some information to a specific point to ensure data integrity.

The log data must be stored in a manner that allows for auditing. This requirement presents two separate network problems and a centralized solution problem due to capacity limitations.

The data transfer within the control network is monitored at various points to ensure the correctness of control data and safety-related data. Cybersecurity measures may necessitate a monitoring network where production control and logging are observed. This includes monitoring network traffic and device information.

We have utilized configuration and communication engineering tools for online monitoring and querying. The results are observable on the network and its associated device. Understanding how to break down information into smaller, manageable segments is vital. Furthermore, the use of a device to supervise the activities of the network is equally important.

We advocate the use of decentralized log data storage, which allows for log data distribution. Decentralization is tied to the need for a distinct cybersecurity control. In particular, if an unauthorized entity gains access to the centralized system, it could potentially interfere with the communication between the control and supervisor elements. However, decentralized should be supplemented with a centralized logging system for long-term data analysis. This system should be linked to the main system via a separate network, which helps in mitigating performance overheads. Regarding Ruef (2021), the very commonly used base of MITRE ATT&CK is not the main solution for every cybersecurity-related penetration test because hierarchical structures are not coherent. There are overlapping terms and hierarchy levels of the attack types, for example, but they are good to use as a supporting tool.

6. Conclusions

Improving detection capabilities is critical to the formation of situational awareness. The tested use cases prove that detection capabilities must also consist of multiple sensors from multiple sources. Detection and network data-gathering capabilities are crucial factors affecting the technical maturity level. SCADA and SOC systems combine cyperphysical systems, but it is important to note the point at which events are perceived. If there are two systems that perceive anomalies and log information differences, the difference must be determined and analyzed, as well as how vulnerable it may be.

The use cases that we have done demonstrate that workable supply chain management is not only the secured flow of information. Our network tests simulate the real world when a person in the middle causes problems monitoring the logs; thus, situational awareness cannot maintain any more control of supply chain management interrupts. The workable operational environment requires effective supply chain management. The workable supply chain management is related to the equipment, such as devices and software, and the information-sharing mechanism.

Information technology networks make it possible to enhance monitoring of the operational technology environment but also provide possibilities for adversaries to use networks as a tool to cause interruptions at the technology level. Suppliers may use different kinds of wireless remote controls to manage industrial equipment. Digitalization may cause challenges to whole industrial ecosystems. The research indicates that gathering relevant information from the sensors is essential. Combining different data from different sources makes getting added value for the detection capabilities possible. We have researched different monitoring points and how those differ from each other. The formation of common situational awareness requires common processes and common methods to monitor data.

Acknowledgments

The research was supported by Business Finland (grant number 10/31/2022) and the University of Jyväskylä.

References

Bakis, B., Wang E., (2017). Building a National Cyber Information-Sharing Ecosystem. Mitre Corporation

Endsley, M. R. (1995). Toward a theory of situation awareness. Human Factors. (37), 32-64.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors Society 32nd Annual Meeting. Monica. CA: Human Factors Society, 97-101.

ENISA (2023) Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies. DOI: 10.2824/850466

European Commission (2022). NIS2 Directive (EU) 2022/2555.

GAO (2021) Electricity Grid Cybersecurity. DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems

Hevner, A. (2007) A three-cycle view of design science research, Scandinavian Journal of

Information Systems 19 (2), pp. 87–92

Hevner, A. & Chatterjee, S. (2010) Design research in information systems theory and practice. New York: Springer.

ISA (2021) Applying ISO/IEC 27001/2 and the ISA 62443 Series for Operational Technology Environments

ISO/IEC (2022) Information security, cybersecurity and privacy protection

Knerler, K.,Parker, I.,Zimmerman C. (2022) 11 Strategies of a World-Class Cybersecurity Operations Cente. The Mitre Corporation

NIST (2016) SP 800-150 Guide to Cyber Threat Information Sharing
NIST (2018) Risk management framework for Information Systems and Organizations NIST 800-37 r2- (NIST, 2018)
NIST (2020) Security and Privacy Controls for Information Systems and Organizations NIST 800-53 r5.
NIST (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations NIST SP 800-161r1
NIST (2023) NIST Special Publication. Guide to Operational Technology (OT) Security NIST SP 800-82r3
NIST (2024) General FAQ´s U.S Department of Commerce
Nunamaker Jay F., Minder Chen Jr. & Purdin Titus D.M. (1990) Systems Development in Information Systems Research, Journal of Management Information Systems, 7:3, 89-106, DOI: 10.1080/07421222.1990.11517898
Pols (2017) Designing a Unified Kill Chain for analyzing, comparing and defending against cyber-attacks.
Risto J., (2017) SANS What is Common Vulnerably Scoring System? Retrieved: 1.3.2024. Available: https://www.sans.org/blog/what-is-cvss/
Ruef M., Schneider M. (2021) Mitre Att&ck, flaws of standardization. Available: https://www.scip.ch/en/?labs.20210204
Simola J., Takala A., Lehkonen R., Frantti T., Savola R. (2023) Developing Cybersecurity in an Industrial Environment by Using a Testbed Environment. 22th European Conference on Cyber Warfare and Security ECCWS-2023. The Hellenic Air Force Academy. Athens, Greece
Strom B., Applebaum A., Miller D., Nickels K., Pennington A., Thomas C. (2020) MITRE ATT&CK®: Design and Philosophy
Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. IEEE Access, 8, 227756–227779.
Worrell J. L., Di Gangi P. M., Bush A. A. (2012) Exploring the use of the Delphi method in accounting information systems research, International Journal of Accounting Information Systems, Volume 14, Issue 3,2013, Pages 193-208, ISSN 1467-0895, https://doi.org/10.1016/j.accinf.2012.03.003.
Yin, R. K. (2017). Case study research and applications: Design and methods. (Sixth edition edition) Los Angeles: SAGE Publications, Inc.