Lauri Havi

Security operations centers in information technology and operational technology environments

A literature review of requirements, differences, issues, and improvements of IT and OT SOC environments

School of Technology and Innovations
Master's thesis in Economics and Business Administration
Information Systems

Vaasa 2025

UNIVERSITY OF VAASA
School of Technology and Innovations
Author: Lauri Havi
Title of the Thesis: Security operations centers in information technology and operational technology environments : A literature review of requirements, differences, issues, and improvements of IT and OT SOC environments
Degree: Master's Degree in Economics and Business Administration
Programme: Master's Programme in Information Systems
Supervisor: Tero Vartiainen
Year: 2025 **Pages:** 64

ABSTRACT:
A growing trend that is increasingly spreading in industries that rely on both information technology and operational technology systems to drive digital transformation is the convergence of both domains. The convergence of information technology and operational technology presents both opportunities and challenges for organizations. While this convergence enables automation, data analytics, and improved efficiency, it also creates a complex security landscape where traditional information technology security measures are often inadequate. This research focuses on the information technology and operational technology security operations centers by first comparing them as separate entities, and finally studying the emerging concept of converged security operations centers, where one security operations center maintains security operations for both information technology and operational technology environments.

This study aims to understand the common requirements, differences, issues, and improvements of security operations centers in both information technology and operational technology environments. The research conducts a comprehensive literature review of existing research and industry reports to analyze the requirements and differences between information technology and operational technology security operations centers, identify key issues, and explore improvements for implementing effective information technology and operational technology security operations centers. This analysis aims to create a holistic view of the current landscape of the state of the security operations centers in both environments. After that, based on the results, the concept of converged security operations centers is studied to determine whether this model is possible and what potential benefits or drawbacks it brings to the organizations using this model.

The research reveals that the unique characteristics of information technology and operational technology environments necessitate distinct approaches to security monitoring, incident response, threat intelligence gathering, regulatory compliance, and personnel training. The review identifies key requirements for successful both information technology and operational technology security operations centers, highlighting the importance of specialized expertise, communication & collaboration with external teams & specialists, robust security tools, integrated security processes, and strong governance frameworks. The findings emphasize the need for a comprehensive approach to managing information technology and operational technology security, recognizing the interconnected nature of these environments and the potential for attacks to spread between them. The research concludes with recommendations for organizations seeking to establish or enhance their converged security operations center capabilities, stressing the importance of collaboration, ongoing training, and the continuous adaptation of security strategies to address evolving threats.

KEYWORDS: Security Operations Center, Operational Technology, Information Technology, Cyber Security, Information Security

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen akateeminen yksikkö
Tekijä: Lauri Havi
Tutkielman nimi: Security operations centers in information technology and operational technology environments : A literature review of requirements, differences, issues, and improvements of IT and OT SOC environments
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tietojärjestelmätiede
Työn ohjaaja: Tero Vartiainen
Vuosi: 2025 **Sivumäärä:** 64

TIIVISTELMÄ:
Kasvava trendi, joka leviää yhä enemmän eri toimialoilla, jotka tukeutuvat sekä tietotekniikkaan, että operatiivisen teknologian järjestelmiin digitaalisen muutoksen edistämiseksi, on molempien ympäristöjen läheneminen. Tietotekniikan ja operatiivisen teknologian läheneminen tarjoaa organisaatioille sekä mahdollisuuksia että haasteita. Vaikka tämä läheneminen mahdollistaa automaation, data-analytiikan ja tehokkuuden parantamisen, se luo myös monimutkaisen turvallisuusympäristön, jossa perinteiset tietoturvan toimenpiteet ovat usein riittämättömiä. Tämä tutkimus keskittyy tietotekniikan ja operatiivisen teknologian tietoturvakeskuksiin vertaamalla niitä ensin erillisinä yksiköinä ja lopuksi tutkimalla kasvavaa yhdistettyjen tietoturvakeskusten käsitettä, jossa yksi tietoturvakeskus ylläpitää tietoturvaa sekä tietotekniikan että operatiivisen teknologian ympäristöissä.

Tämän tutkimuksen tavoitteena on ymmärtää tietoturvakeskusten yhteisiä vaatimuksia, eroja, ongelmia ja parannuksia sekä tietotekniikan että operatiivisen teknologian ympäristöissä. Tutkimuksessa tehdään kattava kirjallisuuskatsaus olemassa oleviin tutkimuksiin ja alan raportteihin analysoidakseen tietotekniikan ja operatiivisen teknologian tietoturvakeskusten vaatimuksia ja eroja, tunnistaakseen keskeiset haasteet ja tutkiakseen parannuksia tehokkaiden tietotekniikan ja operatiivisen teknologian tietoturvakeskusten toteuttamiseksi. Tämän analyysin tavoitteena on luoda kokonaisvaltainen kuva molempien ympäristöjen turvallisuusoperaatiokeskusten nykytilasta. Tämän jälkeen tulosten perusteella tutkitaan yhdistettyjen tietoturvakeskusten käsitettä sen määrittämiseksi, onko tämä malli mahdollinen ja mitä mahdollisia hyötyjä tai haittoja se tuo mallia käyttäville organisaatioille.

Tutkimus paljastaa, että tietotekniikan ja operatiivisten teknologian ympäristöjen ainutlaatuiset ominaisuudet edellyttävät erilaisia lähestymistapoja tietoturvan seurantaan, tapahtumiin reagointiin, uhkien tiedonkeruuseen, sääntelyiden noudattamiseen ja henkilöstön koulutukseen. Katsauksessa tunnistetaan sekä tietotekniikan että operatiivisten teknologian tietoturvakeskusten menestyksekkään toiminnan keskeiset vaatimukset korostaen erikoisosaamisen, ulkoisten tiimien ja asiantuntijoiden kanssa tapahtuvan viestinnän ja yhteistyön, vankkojen tietoturvatyökalujen, integroitujen tietoturvaprosessien ja vahvojen hallintokehysten merkitystä. Tulokset korostavat kokonaisvaltaisen lähestymistavan tarvetta tietotekniikan ja operatiivisen teknologian turvallisuuden hallintaan, tunnustaen näiden ympäristöjen toisiinsa kytkeytyneen luonteen ja hyökkäysten leviämismahdollisuuden niiden välillä. Tutkimus päättyy suosituksiin organisaatioille, jotka pyrkivät luomaan tai parantamaan yhdistetyn tietoturvakeskusten valmiuksiaan, korostaen yhteistyön, jatkuvan koulutuksen ja tietoturvastrategioiden jatkuvan mukauttamisen merkitystä kehittyvien uhkien torjumiseksi.

AVAINSANAT: Tietoturvakeskus, Operatiivinen teknologia, Tietotekniikka, Kyberturva, Tietoturva

Contents

1 Introduction 9
1.1 Research Problem 10
1.2 Research Objectives 10
1.3 Scope and Limitations 11
2 Information Technology and Operational Technology convergence 12
2.1 Information Technology 12
2.2 Operational Technology 17
2.3 Integration of IT and OT 20
3 Security Operations Center 23
3.1 Introduction to SOCs 23
3.2 IT SOC 25
3.3 OT SOC 27
4 Methods 29
4.1 Literature Search and Selection 29
4.2 Data Analysis 31
5 Results 33
5.1 Common requirements for IT and OT SOCs 33
5.1.1 People 34
5.1.2 Processes 36
5.1.3 Technology 37
5.1.4 GRC 38
5.2 Differences in IT and OT SOCs 42
5.2.1 People 43
5.2.2 Processes 43
5.2.3 Technology 44
5.2.4 GRC 45
5.3 Issues and improvements in IT and OT SOCs 46

5.3.1 People 46
5.3.2 Processes 47
5.3.3 Technology 48
5.3.4 GRC 50
5.4 Converged SOCs 51
6 Discussion 54
6.1 Summary of Findings 54
6.2 Implications for Practice 55
6.3 Future Research 56
References 58

Figures

Figure 1. Open Systems Interconnection model 14

Figure 2. TCP/IP Model 15

Figure 4. Simple SCADA system architecture 19

Figure 5. Purdue Enterprise Reference Architecture 21

Figure 6. SOC tier model & external teams 25

Tables

Table 1. The structure of the thesis 10

Table 2. Common threats in IT systems 16

Table 3. Common OT system assets 17

Table 4. CIA triad attacks and IT SOC responses 26

Table 5. Literature search parameters 29

Table 6. Selected papers 29

Table 7. Chosen articles' SOC type classification 31

Table 8. Recognized regulations, standards, frameworks, and best practices 39

Abbreviations

AI	Artificial Intelligence
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AV	Antivirus
C2	Command and Control
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CNN	Convolutional Neural Network
COBIT	Control Objectives for Information and Related Technologies
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
DCID	Director of Central Intelligence Directive

DCS	Distributed Control System
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial-of-Service
DPO	Data Protection Officer
ERP	Enterprise Resource Planning
FDA	Food and Drug Administration
FDIS	Final Draft International Standard
FERC	Federal Energy Regulatory Commission
FFIEC	Federal Financial Institutions Examination Council
FTP	File Transfer Protocol
FW	Firewall
GDPR	General Data Protection Regulation
GNN	Graph Neural Network
GRC	Governance, Risk, and Compliance
GxP	Good 'x' Practices
HIDS	Host-based Intrusion Detection System
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IMRaD	Introduction, Methods, Results, and Discussion
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Incident Response
IS	Information System
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standards
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library

LAN	Local Area Network
LLM	Large Language Model
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
MISP	Malware Information Sharing Platform
ML	Machine Learning
MQTT	Message Queue Telemetry Transport
NERC	North American Electric Reliability Corporation
NIDS	Network Intrusion Detection System
NIS 2	Network and Information Security 2
NIST	National Institute of Standards and Technology
OPC UA	Open Platform Communications Unified Architecture
OS	Operating System
OSI	Open Systems Interconnection
OT	Operational Technology
PCI DSS	Payment Card Industry Data Security Standard
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controller
POP3	Post Office Protocol version 3
PPP	Point-to-Point Protocol
RMF	Risk Management Framework
RTU	Remote Terminal Unit
SANS	SysAdmin, Audit, Network, and Security
SCADA	Supervisory Control and Data Acquisition
SI	Security Intelligence
SIEM	Security Information and Event Management
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SOX	Sarbanes-Oxley Act
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TI	Threat Intelligence
TLS	Transport Layer Security
UBA	User Behavior Analytics
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
WAN	Wide Area Network
XDR	Extended Detection and Response
XGBoost	eXtreme Gradient Boosting

1 Introduction

A growing trend that is increasingly spreading in industries that rely on both information technology (IT) and operational technology (OT) systems to drive digital transformation is the convergence of both domains. Traditionally, OT systems have handled industrial operations, machinery, and physical processes, whereas IT systems have focused on data processing, management, and communication (Murray et al., 2017, p. 149). According to Murray et al., the boundaries between IT and OT are blurring as organizations look to increase productivity, enhance operational effectiveness, and make better decisions. Modern industrial control systems (ICS), critical infrastructure, and smart manufacturing settings require this integration, often known as IT/OT convergence (Murray et al., 2017, p. 149). The convergence of these two domains has also been driven by the emergence of the IIoT, cloud computing, and the growing need for data-driven decision-making. Although its advantages, this development has introduced new complexities and security considerations that call for an examination of standard cybersecurity approaches.

Security Operations Centers (SOCs), which often are the first line of defense in IT environments against cyberattacks, are now required to adjust to the specific and complicated requirements of OT systems (Kaliyaperumal, 2021, p. 1). OT systems require continuous accessibility and operational safety to successfully carry out their operational tasks, in contrast to IT environments, which place a higher emphasis on data integrity and confidentiality. Additionally, as OT settings have specific demands, including strict uptime requirements and real-time processing, typical IT security techniques are unable to handle these OT risks. Furthermore, the importance of OT systems, which are frequently connected to vital services like transportation, water supply, and power grids, raises the stakes for cyber incidents. Consequently, one of the most important elements of modern cybersecurity strategy is the emergence of the combined IT/OT SOC, which can efficiently monitor and safeguard both IT and OT environments (Kaliyaperumal, 2021, p. 8).

1.1 Research Problem

There is an absence of academic research that explicitly looks at the distinctions and requirements of IT and OT SOC environments, despite the increasing significance of IT/OT convergence. The majority of the existing literature tends to focus on the broader challenges of IT/OT integration and/or cybersecurity or the general principles of SOC operations, without delving into the nuances and unique characteristics of IT and OT SOCs.

1.2 Research Objectives

This paper aims to examine the common requirements, differences, issues, and improvements associated with the SOCs in IT and OT environments. Furthermore, this paper aims to research whether the emerging concept of the IT/OT SOC model is possible and what benefits it brings for the organizations.

This thesis is structured according to the IMRaD format, providing a comprehensive review of the existing literature on IT and OT environments and SOCs. The remaining chapters are described in Table 1:

Table 1. The structure of the thesis

Chapter	Chapter description
2	Provides a foundational understanding of both IT and OT environments, highlighting their unique characteristics and the implications of their convergence for security.
3	Explores the concept of SOCs and analyzes the distinct requirements for both IT and OT SOCs.
4	Details the methodology used for conducting the literature review, including the search terms, databases, and selection criteria employed.

5	Presents the findings of the literature review, identifying key requirements, issues, improvements, and differences for IT and OT SOCs, and finally discussing the emerging IT/OT SOC model.
6	Discusses the implications of the findings for organizations seeking to establish effective IT and OT SOCs and identifies promising areas for future research in this rapidly evolving field.

The following subchapter will address the scope and limitations of this study.

1.3 Scope and Limitations

The security requirements and challenges faced by IT and OT SOCs throughout an array of industrial sectors, such as manufacturing, energy, transportation, and healthcare, are the primary focus area of this literature review. To ensure that the most recent advancements and insights are included, the review will mainly concentrate on academic research and industry reports that have been published in the last ten years.

It is essential to recognize that any static review has inherent limits due to the quick development of IT and OT technologies and environments. As new technologies and risks constantly affect the IT/OT security landscape, future research is required to stay up to date. This literature review will add to the increasing body of knowledge regarding the integration of cybersecurity practices across multiple technical ecosystems by examining the distinctive features of IT and OT environments and the implications for SOCs.

2 Information Technology and Operational Technology convergence

The convergence of IT and OT environments is a rapidly evolving phenomenon, driven by factors such as automation, data analytics, and IoT. This convergence presents both opportunities and challenges, requiring a comprehensive understanding of both IT and OT systems and their unique security needs. As organizations strive to leverage the benefits of digital transformation, the integration of IT and OT environments has become increasingly prevalent. To better understand this convergence, it is essential to first examine the distinct characteristics and security requirements of both IT systems and OT systems, which form the crucial components of the overall landscape. The following sections will delve into the specific aspects of IT and OT environments, including their hardware and software components, network architecture, and common security concerns.

2.1 Information Technology

Information Technology can be broadly defined as the use of computer systems to access information, to communicate, and to manage and process data (CompTIA, 2023; Berardi et al., 2023, p. 2). According to Berardi et al. (2023, p. 3), IT systems were designed to connect applications and share data, resulting in IT systems tending to be open and standards-based. The information technology infrastructure in an organization is composed of different major components such as hardware, software, networking, data management, and storage (Laudon et al., 2022, p.209).

Modern IT environments rely on a wide range of hardware components, including servers, physical storage devices, networking equipment, and workstations. These components are interconnected and work together to support various applications and services.

Computer programs that control the operation of computer hardware are referred to as software (Stair & Reynolds, 2018, p. 138; Laudon et al., 2022, p. 210). According to Stair & Reynolds (2018, p.138) and Laudon et al. (2022, p.210), systems software and application software are the two categories of software. According to them, operating systems, utilities, and middleware are examples of system software that manage the operations and functions of other applications and hardware across the computer system. Furthermore, they continue that programs known as application software assist users in resolving specific computer issues. For example, a spreadsheet application or a program that records and displays data to allow for manufacturing process monitoring are two examples of this type of software (Stair & Reynolds, 2018, p. 138).

A computer network is a group of connected computers or systems and equipment that enables electronic communication (Stair & Reynolds, 2018, p. 15). An organization's computer network's fundamental components are the hardware, software, and protocols (IBM, n.d.; Davies, 2019, p. 9; Stair & Reynolds, 2018, p. 241). According to IBM (n.d.), the network's infrastructure is made up of how these fundamental components interact with one another, and the topology in which a LAN or WAN's nodes are connected to one another is known as the network infrastructure, where these connections use cables or wireless technologies to connect devices like hubs, switches, routers, and bridges.

To enable vendor-neutral communication between devices, standardized models are needed to have a common framework of network communication. The two most common reference models to represent networking are the OSI model created by the ISO and the TCP/IP model (Davies, 2019, p. 251). OSI Model in Figure 1:

OSI Model

Layer No.	Layer Name	Commonly used protocols
7	Application Layer	HTTP, HTTPS, FTP, SMTP
6	Presentation Layer	MIME, SSL/TLS
5	Session Layer	Sockets (session establishment)
4	Transportation Layer	TCP, UDP
3	Network Layer	IP, IPsec, ICMP
2	Data Link Layer	PPP, SLIP
1	Physical Layer	

Figure 1. Open Systems Interconnection model

The OSI model is a network model comprising seven individual layers, as shown in Figure 1 above. Each of the layers communicates to the layers adjacent to it and its equivalent layer on the receiving device (Davies, 2019, p.252). According to Davies (2019, p.253), the data undergoes a process known as encapsulation as it passes through the OSI model on the sending device, where the layers add a header (and occasionally a trailer) to the data from the previous layer and send it on to the subsequent layer, where the procedure is repeated.

Nowadays, however, the more modern TCP/IP model is being used by pretty much all networking devices (Davies, 2019, p. 268). TCP/IP model in Figure 2:

TCP/IP Model

OSI Model Layer No.	Layer Name	Commonly used protocols
5-7	Application Layer	HTTP, HTTPS, FTP, SMTP, DHCP, DNS
4	Transport Layer	TCP, UDP
3	Internet Layer	IP, IPsec
2	Link Layer	MAC

Figure 2. TCP/IP Model

Like in the OSI model, the TCP/IP model uses encapsulation and de-encapsulation, and headers and trailers are added and removed from the data as it progresses up and down the model. (Davies, 2019, p. 270). When compared to the OSI model, the Layers 5 to 7 are represented as a one application Layer in the TCP/IP model.

In the OSI model layers 5-7 and the TCP/IP model application layer act as an interface between the applications themselves and the network stack (Davies, 2019, p. 271). For example, FTP works in this layer to transfer files. The transport layer has the same role in both models, where it controls communication between 2 hosts (Davies, 2019, p. 278). Most common protocols in this layer are connection-oriented TCP and connectionless UDP (Davies, 2019, p. 279). The Internet layer in the TCP/IP model or the network layer in the OSI model provides logical addressing using IPv4 and IPv6 addresses. (Davies, 2019, p. 279). Finally, the link layer in the TCP/IP model and data link & physical layers in the OSI model are responsible for communications mainly outside the host's network and for routing this data, and managing MAC addresses (Davies, 2019, p. 280).

Some of the other commonly used protocols for networking are for example DNS which is responsible for translating and mapping IP addresses to domain names and vice versa, DHCP which dynamically assigns IP addresses to devices in a network, ICMP that is used for sending error messages and operational information, SMTP & POP3 which are used for email services, and ARP that is used for mapping MAC addresses to IP addresses in a network (ManageEngine, 2023).

High levels of complexity, including networked systems, software programs, and data repositories, define IT environments and make them susceptible to a variety of cyber-threats because of their complexity (Vielberth et al., 2020, p. 227773). Some of the most common information security threats are listed in Table 2:

Table 2. Common threats in IT systems **(**Osazuwa & Mitchell, 2023, p. 1949; Akhtar, 2021, pp. 1-3**)**

Threat	**Definition**
Phishing	Phishing is a form of social engineering attack where perpetrators often employ deceptive emails or text messages that mimic the appearance of authentic communications originating from reputable entities. Phishing often aims to steal a victim's personal or financial information or login credentials.
Malware	Malware is a type of software specifically engineered with the intention of causing damage, stealing information, or causing disruption to a computer system. Some of the most common types of malware are ransomware, which encrypts a computer system's files and demands payment in exchange for decrypting the files. Another common malware is a virus that is capable of replicating itself. Trojan horses are viruses that disguise themselves as standard software. In addition, some other common types of malware are adware, keyloggers, droppers, worms, and rootkits.
Data Breaches	Data breaches happen when private information is illegally taken from a network or computer system. Hacking, insider threats,

	and physical theft are some of the ways that data breaches can appear.
Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS)	DoS attacks are malicious actions that overload a computer system or network with traffic, making it unavailable to legitimate users. A distributed denial-of-service attack is an instance of a DoS attack in which multiple sources are used simultaneously to carry out the attack.

In addition to these common threat types, there are numerous other types of information security threats to organizations. New threats and vulnerabilities are found every day, meaning that the IT security professionals need to actively reduce the attack surface of their IT systems.

2.2 Operational Technology

Operational technology can be defined as hardware or software that causes or detects changes by either monitoring or controlling physical devices, processes, and events in an organization (Moura & Ceotto, 2024, p. 12; Stouffer et al., 2023, p. 8). According to Moura & Ceotto (2024, p. 12), ICSs are a part of OT systems that are responsible for the control and automation of industrial plants. Some of the most common components in OT environments are SCADAs, PLCs, DCSs, RTUs, IEDs, HMIs, control servers, engineering workstations, data historians, sensors, and actuators (Moura & Ceotto, 2024, p. 12; Stouffer et al., 2023, pp. 8-13). Common OT environment assets are defined in Table 3:

Table 3. Common OT system assets

Asset	**Definition**
PLC	An industrial computer control system that controls actuators and/or monitors sensors (Stouffer et al., 2023, p. 12; Advanced Micro Controls, 2017).
DCS	DCSs are used to control production systems within the same geographic location. These systems are usually process control or discrete part control systems. (Stouffer et al., 2023, p. 19).

RTU	Microprocessor-based electronic device that controls actuators and/or monitors sensors (Stouffer et al., 2023, p. 12; Awati, 2024).
IED	IEDs control actuators and/or monitors sensors (Stouffer et al., 2023, p. 12). According to Stouffer et al. IEDs also provide a direct interface for operating and maintaining sensors and equipment. Furthermore, IEDs typically include local programming that enables them to act without direct commands from the control center, and they can be directly polled and controlled by the control server.
HMI	HMIs are used by operators to monitor and configure the set points, control algorithms, and adjust and establish parameters in the controller, and it also displays process status information and historical information (Stouffer et al., 2023, p. 10).
Control server	Stores and processes the information from RTU or PLC inputs and outputs and controls their function (Stouffer et al., 2023, p. 12).
Engineering workstation	The engineering workstation is used to access the programming interface of PLC/RTU (Stouffer et al., 2023, p. 21).
Data historian	A data historian is a centralized database that stores the data from the processes (Stouffer et al., 2023, p. 21).
Sensor & Actuator	A sensor is a device that measures a physical attribute and transmits this data to the controller as controlled variables (Stouffer et al., 2023, p. 10). Actuators, which include motors, switches, breakers, and control valves, are used to modify the controlled process in accordance with controller commands (Stouffer et al., 2023, p. 10).

SCADA systems are used to control dispersed assets for which centralized data acquisition is as important as control (Stouffer et al., 2023, p. 12). According to Stouffer et al. (2023, p. 12), SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a control center, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real-time (Stouffer et al., 2023, p. 12). A simple SCADA system architecture is displayed in Figure 4:

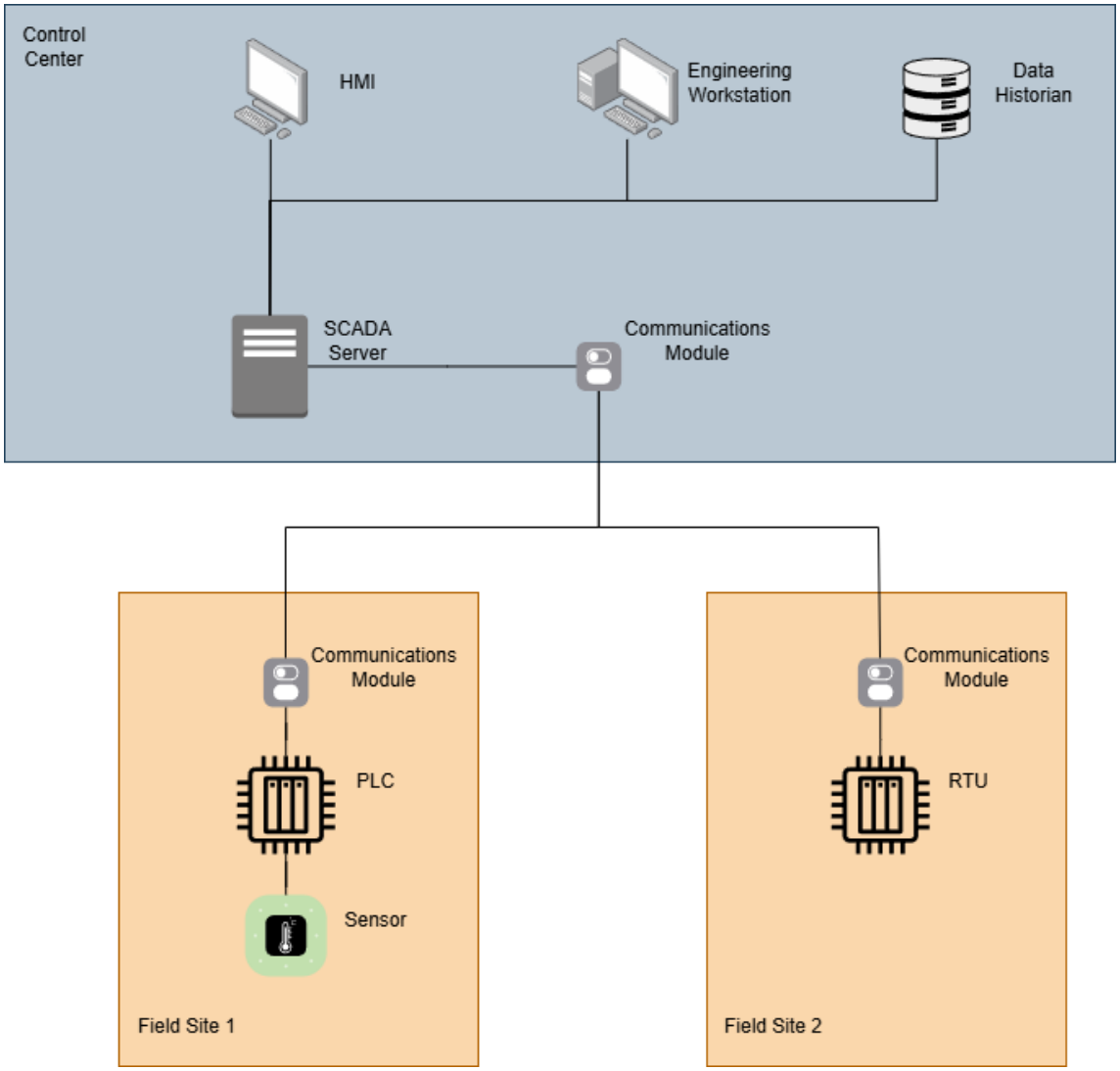

Figure 3. Simple SCADA system architecture

One of the most important aspects that differentiates OT systems from IT systems is that some of the OT systems include a significant risk to the health and safety of human lives, serious damage to the environment and property (Stouffer et al., 2023, p. 25). OT systems generally have different priorities regarding security compared to IT systems, like for example prioritizing system safety above all other aspects (Stouffer et al., 2023, p. 28). One other key difference between IT and OT systems is that OT systems have much stricter uptime requirements, and the operations are often required to perform in real-time (Moura & Ceotto, 2024, p. 14; Stouffer et al., 2023, pp. 30-31). Furthermore, the average lifespan of OT systems' components is from 10 to 15 years compared to IT

systems average ranging typically range from 3 to 5 years (Stouffer et al., 2023, p. 31; Murray et al., 2017, p. 149). This long lifecycle of components, combined with the strict uptime requirements mentioned before, makes patch management challenging compared to IT environments since systems cannot necessarily be stopped for patching as easily (Stouffer et al., 2023, p. 31; Kanamaru, 2020, p. 41; Murray et al., 2017, p. 149). According to Stouffer et al. (2023, p. 31), the long lifecycle of the components might also lead to a lack of vendor support regarding security patches. One unique method to reduce the attack surface of an OT system is “air-gapping”. This is achieved by isolating ICSs from the internet either physically or logically (Na & Sundharakumar, 2024, p. 2).

2.3 Integration of IT and OT

The convergence of IT and OT systems is being driven by the need for quantitative management reporting, assisted by ‘big data’ and sensor technology, artificial intelligence, physical automation, remote operations, cloud computing, and analytics (Murray et al., 2017, p. 152). According to Murray et al. (2017, p.152), all of which have the potential to enhance productivity; however, to facilitate all of this requires organizations to increase network connectivity and access to both IT and OT systems using, for example, Ethernet, WI-FI, and/or TCP/IP standards. This rate of informatization in companies has steadily increased with these advancements in technology, and there is an increasing number of ICS that are connected to the Internet either directly or indirectly each year (Tao et al., 2019, p. 1; Stouffer et al., 2023, p. 26). This pattern causes, however, the ICS attack vector to grow, which results in significant security issues and attacks like Stuxnet, Black Energy, WannaCry, and others, that have drawn attention to the security of OT systems (Tao et al., 2019, p. 1). The growing exposure of ICS to IT networks, combined with OT specific cybersecurity weaknesses, can make these systems relatively easy targets to exploit (Murray et al., 2017, p. 149).

IT and OT are closely connected environments in modern organizations, making it sometimes difficult to determine whether a particular asset falls under the scope of the OT or IT environment. Sometimes the difference between OT and IT is defined in the Purdue model, also known as PERA, where levels 0 to 3 are under OT security and levels 4 to 5 are under IT security, having level 3.5 or DMZ in the middle (Tao et al., 2019, pp. 1-2; Williams, 1993, p. 559). Purdue Model in Figure 5:

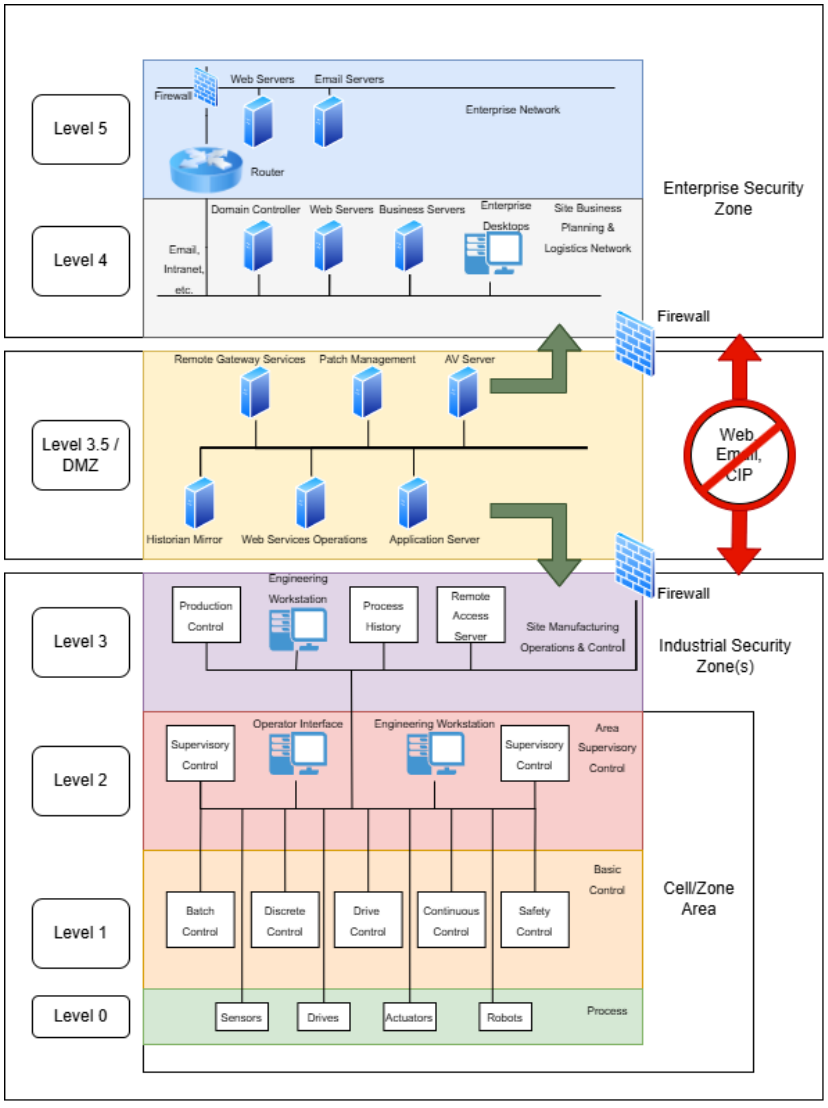

Figure 4. Purdue Enterprise Reference Architecture

A set of information systems under the control of a single authority and security policy that are connected by one or more internal networks is known as a security zone (Mahan

et al., 2011, p. 4). In the Purdue Model, levels 4 and 5 are under the enterprise security zone, levels 0 to 3 are under the Industrial security zones, and levels 0 to 2 are under the cell area security zone (Tao et al., 2019, p. 2; Tripwire, 2019). The enterprise zone contains traditional IT systems typically used in corporate systems, such as ERP systems, enterprise IT servers, and enterprise office networks (Tao et al., 2019, p.3; Mahan et al., 2011, p. 5). The DMZ is a layer between the enterprise security zone and industrial security zone that is used for providing a secure exchange of IT information without directly exposing critical infrastructure in the layers 0 to 3 to the Internet (Tao et al., 2019, p.3; Stouffer et al., 2023, p. 4). Commonly present in the DMZ are data historians, patch management servers, security servers, backup servers, and remote gateway services (Tao et al., 2019, p.3). In the industrial control zone, the PERA's level 3 includes systems and devices used for the monitoring, control, and automation of site processes (Tao et al., 2019, p.2; Stouffer et al., 2023, p. 86). In addition to this Industrial Security zone consists of cell area security zone(s), which host field level devices and local control systems that range from PERA's levels 0 to 2 (Tao et al., 2019, p.2; Stouffer et al., 2023, p. 86).

3 Security Operations Center

Security Operations Centers (SOCs) represent the cornerstone of modern cybersecurity defense strategies, serving as centralized units that continuously monitor, detect, analyze, and respond to security threats across organizational infrastructure. While the fundamental mission of threat detection and incident response remains consistent, the implementation and operational focus of SOCs can vary significantly depending on the technological environment they protect. This chapter provides an examination of SOC environments, beginning with an introduction to their core principles and functions, followed by a detailed analysis of IT-focused SOCs that protect traditional information technology assets, and concluding with an exploration of OT SOCs specifically designed to safeguard operational technology and industrial control systems. Understanding these distinctions is crucial for organizations seeking to implement appropriate security monitoring capabilities that align with their specific technological landscape and operational requirements.

3.1 Introduction to SOCs

SOC is a centralized unit that consists of three basic components that are people, who are also known as analysts, processes, and technology, to protect an organization from cyber threats (Vielberth et al., 2020, p. 227758; Alharbi, 2020, p. 3973). According to Vielberth et al. (2020, p. 227758), SOCs' function is to detect, analyze, and respond to cybersecurity threats and incidents employing previously mentioned people, processes, and technology that are defined by the governance and compliance aspect, since it offers the framework in which people operate and according to which the processes and technologies are built.

Organizations can use two models of SOC, which are internal SOC, where the SOC is managed and operated internally, in which it is part of the organization, or they can outsource SOC, where the organization pays for SOC services to an independent party that manages and operates the SOC (Alharbi, 2020, pp. 3973-3974). These SOCs use systems like SIEM to collect security-relevant data in a centralized manner and provide security analytics capabilities by correlating log events (Vielberth et al., 2020, p. 227759). Another commonly used tool in SOC environments is SOAR, which is used to automate many of the common manual tasks to improve both efficiency and consistency in SOC operations (Bridges et al., 2023, p. 2). Another newly emerging tool used by SOCs is XDR, which is a solution that automatically collects and correlates data from multiple security products to improve threat detection and provide an incident response capability (Gartner, 2021). Gartner (2021) provides an example where an attack that caused alerts on email, endpoint, and network can be combined into a single incident by using XDR.

These systems collect data from various data sources, which is then normalized to a unified format (Vielberth et al., 2020, p. 227765). This data is then filtered for data elements that are likely to contain important information from a security perspective, and after that, reduction is done where unimportant data fields are sorted out (Vielberth et al., 2020, p. 227765). Finally, similar log events are aggregated into a single data element and prioritized according to importance to facilitate further processing (Vielberth et al., 2020, p. 227765). These logs can then be further analyzed by automated data analysis and detection rules to create alerts that can be triaged, analyzed, and prioritized by SOC analysts (Vielberth et al., 2020, pp. 227765-227766; Cox, 2024).

The people component in SOC is typically divided into positions by tier model, where analysts range from tier 1 to tier 3, who work in collaboration with other teams and specialists, such as the vulnerability assessment team (Vielberth et al., 2020, pp. 227762-227763). A “tierless” model also exists, where analysts are not divided into different tiers, but the three-tiered model is more common. An example of three-tier SOC roles and external teams is shown in Figure 6:

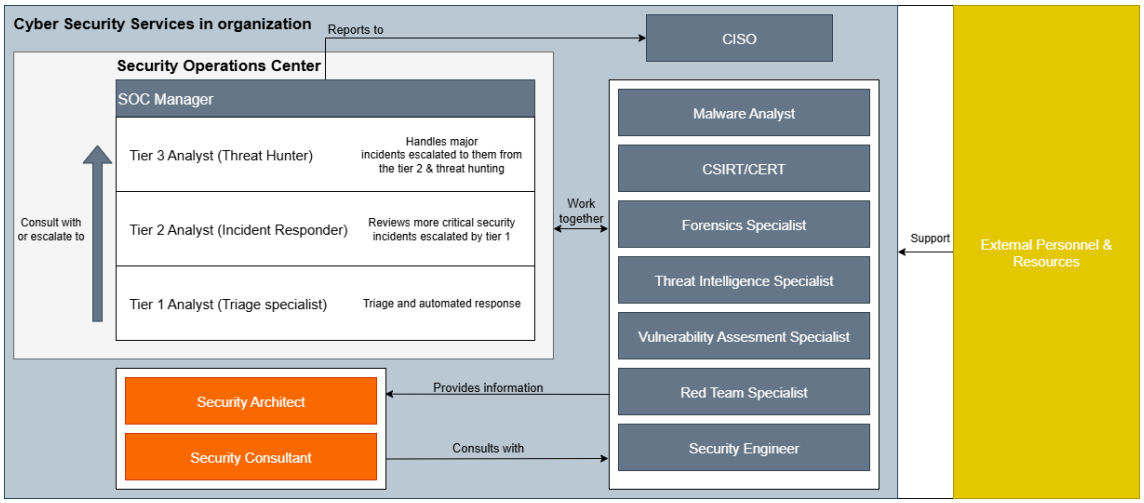

Figure 5. SOC tier model & external teams (Vielberth et al., 2020, p. 227763; Simos et al., 2019)

To operate SOC properly, an organization requires skilled professionals who utilize the processes and the technology available to analyze and mitigate cyber threats and incidents.

3.2 IT SOC

IT SOC detects, analyzes, and responds to cybersecurity threats and incidents occurring in the organization's IT systems. IT SOCs are responsible for monitoring layers five, four, and some parts of 3.5 in the Purdue model discussed in the previous chapter. This includes, for example, monitoring of domain controllers, email servers, application servers, endpoints, networking devices, mobile devices, identities, and accounts managed by an organization.

One of the most common measurements for information security has been the CIA triad (Conklin, 2016, pp. 2642-2643). According to Conklin (2016, p. 2643) this is achieved by "Preserving authorized restrictions on information access and disclosure, including

means for protecting personal privacy and proprietary information" to maintain confidentiality, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity" to maintain integrity, and "Ensuring timely and reliable access to and use of information" to ensure availability. IT SOC aims to ensure that the CIA triad is maintained in the organization's IT systems, with the main focus on confidentiality (Koizumi & Shiozaki, n.d., p. 31). Examples of attacks affecting the CIA triad and example IT SOC responses to these attacks are in Table 4:

Table 4. CIA triad attacks and IT SOC responses (Martin, 2025; SOCFortress, 2022; Traficom, 2022)

CIA triad element affected	Attack method	Example IT SOC response
Confidentiality	Successful phishing attack resulting in loss of credentials and unauthorized access	Disabling the user's account. Blocking potential C2 or other channels to the attacker. Resetting the user's sessions and password. Containing the user's endpoint. Deletion phishing message. AV scanning device(s).
Integrity	Ransomware attack on the user's endpoint.	Isolating device. Stopping backups. Powering down non-encrypted systems & disconnecting share drives. AV scanning device. Resetting user sessions and passwords.
Availability	Network layer protocol denial-of-service attack on the web server	Restricting the traffic based on identifiers, e.g., user agent or country. Potentially contact the ISP to help by employing a packet washer.

As discussed before, SOC works closely with other teams within the realms of cybersecurity, IT, etc. For example, when IT SOC has restricted a ransomware on one endpoint from spreading to the organization's network, it might have to notify IT support so that the end user receives a new endpoint to work on. In addition to this, other parties in the organization, such as DPO, CISO, forensics team, network team, etc., might have to be

notified about the incident, so that mandatory privacy notices and other actions can be performed.

3.3 OT SOC

OT SOC detects, analyzes, and responds to cybersecurity threats and incidents occurring in the organization's OT and ICS infrastructure. OT SOCs are responsible for monitoring layers from zero to three, and some parts of 3.5 in the Purdue model discussed in the previous chapter. When IT systems had the priority in the confidentiality aspect of the CIA triad, the highest priority in the OT domain is availability, and monitoring focuses on safety, reliability, and productivity (Koizumi & Shiozaki, n.d., p. 31). This makes the OT SOCs' top priority to keep the systems safely and reliably running rather than shutting systems down or isolating them to maintain confidentiality. This means that the traditional IT SOC approaches cannot necessarily be applied to the OT SOC operations.

One unique challenge OT SOC has compared to the IT SOC is the log format, since the communication protocols differ compared to traditional IT systems (Koizumi & Shiozaki, n.d., p. 31). According to Koizumi & Shiozaki (n.d., p. 31), OT systems use various protocols, such as Modbus, MQTT, OPC UA, and industrial Ethernet (PROFINET Ethernet/IP), depending on the type of equipment, and some log formats used in OT systems are not disclosed. Therefore, the OT SOC has to come up with different mechanisms for monitoring logs, events, networks, and event sequences to collect, analyze, and visualize various data sets (Koizumi & Shiozaki, n.d., p. 31).

In IT SOC, the analysts can often do triaging and mitigation of incidents by themselves, as discussed before, but in the OT SOC, this is often not possible. According to Joffel (2022, pp. 24-25), in many cases analyst has to first confirm whether the asset should be in the OT network by searching it from CMDB or consulting a site engineer. If the incident

is deemed as a true positive, the analysts escalate the incident to the IR manager rather than mitigating the threat by themselves (Joffel, 2022, pp. 24-25).

4 Methods

This chapter outlines the systematic methodological approach employed to investigate and analyze the research objectives of this study. The research process begins with a systematic approach to identifying, gathering, and evaluating relevant academic and industry literature to establish a solid foundation of existing knowledge and current practices. Following the collection phase, a structured analytical framework is applied to extract meaningful insights and patterns from the gathered data.

4.1 Literature Search and Selection

To obtain suitable academic papers for the research appropriate database and suitable parameters were chosen. Literature search parameters displayed in Table 5:

Table 5. Literature search parameters

Database	IEEE Xplore
Search query	("OT" OR "operational technology" OR "IT" OR "information technology") AND ("SOC" OR "security operations center")
Years	2015 – 2026
Publication topics	Security Operation Centers
Publication type	Conferences & Journals

Searching the IEEE Xplore database with these parameters resulted in 34 papers. Out of the 34 papers, 21 were initially chosen based on the relevance of the paper's title and abstract. These papers are listed and given an ID in Table 6:

Table 6. Selected papers

ID	Title	Author(s)

1	Analysis of the Functionalities of a Shared ICS Security Operations Center	Dimitrov & Syarova
2	Security Operations Center: A Systematic Study and Open Challenges	Vielberth et al.
3	Towards the Design of Grid Cyber-Physical Integrated Security Operations Center Visualizations	Reyna et al.
4	Threat Hunting as a Cyber Security Baseline in the Next-Generation Security Operations Center	Bikov et al.
5	SOC and Academia – Building Resilient Systems	Zimmerman & Bhargav-Spantzel
6	A user-centric machine learning framework for cyber security operations center	Feng et al.
7	"SOCaaS-IoT" A Security Operations Center as a Service Approach for IoT Applications Using Open-Source SIEM	Arfaoui et al.
8	Taxonomy for Unsecure Big Data Processing in Security Operations Centers	Miloslavskaya et al.
9	Towards a Responsive Security Operations Center for UAVs	Tlili et al.
10	Supporting NIS 2 Directive with SOC	Pikó et al.
11	Toward a Security Operation Center for Operational Technology in Industrial Networks	Gaggero et al.
12	Review of Detection and Prevention Techniques for Cyberattacks in SOCs: State of the Art and Future Challenges	Lotfi & Mandar
13	Designing a Framework of an Integrated Network and Security Operation Center: A Convergence Approach	Shahjee & Ware
14	The Next Gen Security Operation Center	Perera et al.
15	Security Operations Centers for Information Security Incident Management	Miloslavskaya
16	Enhancing intelligence SOC with big data tools	Andrade & Torres
17	Empowering Security Operation Center with Artificial Intelligence and Machine Learning—A Systematic Literature Review	Khayat et al.
18	Network IDS Alert Classification Using Hybrid Transfer-Active Learning: Reducing Analyst Burden in SOC Environments	Hasan et al.
19	Integrating IoT Monitoring for Security Operation Center	Weissman & Jayasumana
20	Novel Method of Improving Cybersecurity Posture with Real-Time Analytics in Security Operations Centers	Boljam et al.
21	Implementation of a Security Operation Center - An Essential Cybersecurity Solution for Organizations	Mocanu & Scripcariu

The following subchapter outlines the data analysis methods used to extract meaningful data from the chosen articles.

4.2 Data Analysis

The data analysis phase represents a critical component of this research methodology, where the information gathered through the literature search is systematically examined to extract meaningful insights and identify patterns relevant to the research objectives. This analytical process employs both qualitative and quantitative approaches to ensure a comprehensive evaluation of the collected materials, allowing for a nuanced understanding of the current state of knowledge in the field.

The analytical framework begins with the categorization of the selected literature based on predefined themes and emerging patterns identified during the initial review process. Each source is systematically evaluated for its contribution to key research areas, methodological rigor, and relevance to the research questions. This structured approach enables the identification of consensus areas, knowledge gaps, and conflicting perspectives within the existing body of literature.

The chosen articles can be categorized by the type of SOC they discuss, which is displayed in Table 7:

Table 7. Chosen articles' SOC type classification

SOC type	Papers
IT	2, 4-6, 8, 10, 12-18, 20, 21
OT	1, 2, 7, 9, 11, 17
IT/OT	3, 19

It can be seen that IT SOC-related articles have a big majority, with about 67% of all of the research papers being IT SOC-related, while OT SOC-related articles make up about 29% of the research papers, and IT/OT SOC-related articles about 10% of the research papers. A couple of research papers included both IT and OT SOCs in their research, but kept both as their own entities. These were articles 2 and 17. This distribution can be

expected, since IT SOCs have been around for a much longer time than OT SOCs or IT/OT SOCs, as discussed in the earlier chapters.

To identify what types of requirements, differences, issues, and improvements exist in IT and OT SOCs, the papers are systematically reviewed. Different components of SOC, which were previously discussed, people, processes, technology, and GRC, are recognized in the papers. Using these components, each one's requirements, issues, improvements, and differences between OT and IT SOCs are reviewed in the next chapter. Finally, based on these results, the concept of integrated IT/OT SOC is also discussed.

5 Results

This chapter presents the comprehensive findings derived from the systematic literature analysis and data evaluation conducted in accordance with the methodology outlined in Chapter 4. The results are organized to provide a clear and logical progression of discoveries, highlighting key themes, patterns, and insights that emerged from the examination of the selected literature. These findings directly address the research questions posed at the outset of this study and provide the empirical foundation for subsequent discussion and recommendations.

The analysis of the collected data revealed several significant trends and patterns within the current body of knowledge, offering valuable insights into both established practices and emerging developments in the field. The results demonstrate a complex landscape of findings that span multiple dimensions of the research topic, with certain areas showing strong consensus among sources while others reveal notable gaps or conflicting perspectives that warrant further investigation.

The presentation of results follows a structured approach, beginning with overarching themes that emerged across the literature, followed by more specific findings related to individual research components. Each finding is supported by evidence from the analyzed sources, with particular attention paid to the frequency of occurrence and relevance to practical applications. This systematic presentation ensures that readers can readily understand both the breadth and depth of the discoveries while maintaining clear traceability back to the source materials.

5.1 Common requirements for IT and OT SOCs

The analysis of the literature reveals that despite the distinct operational environments and specialized requirements of IT and OT SOCs, both share a foundational set of core requirements that are essential for effective security operations. These common requirements form the backbone of any successful SOC implementation, regardless of whether the focus is on traditional IT infrastructure or OT systems. The identified shared requirements can be categorized into four fundamental components that consistently emerge across the literature as critical success factors for SOC effectiveness. Understanding these commonalities provides valuable insight for organizations seeking to establish or optimize their security operations capabilities, as these elements represent the universal building blocks upon which specialized SOC functions are constructed. The following subsections examine each of these core requirement areas in detail, highlighting how they apply across both IT and OT environments while laying the groundwork for understanding the specialized adaptations required for each domain.

5.1.1 People

One of the most common requirements for SOC operations is skilled staff. In total, 13 out of the 21 papers examined mentioned having a skilled staff as a core aspect of the SOC operations. For example, article 1 mentions that the SOC team is made up of security professionals who are dedicated to protecting businesses and that the staffing requirements are extremely high. Furthermore, articles 5, 7, and 9 also characterize SOC as a dedicated unit or team with an appropriate level of expertise. According to 5 of the examined articles, the teams handling SOCs are large, but no exact numbers are being discussed. The skills found in the articles that the SOC staff needs to possess are domain knowledge and technical skills, like knowledge of security tools (such as SIEMs, SOARs, AVs, and FWs), OSes, log analysis skills, and networking skills. In addition to these skills, SOC staff also require a set of soft skills, like communication skills, continuous learning abilities, analytical mindset, performing under stress, commitment, teamwork, curiosity, and practical organizational skills.

Three articles mentioned the previously discussed three-tiered model as the way personnel in SOC operate. These were articles 2, 10, and 14. According to article 14, a level 1 analyst's job is to make a case through alarms, and then the level 2 analyst has a responsibility to investigate and mitigate such attacks. Article 10 discussed that three levels are usually distinguished, between which the responsibilities and the required level of knowledge gradually increase. Article 2 discusses similar tiers with tasking the tier 1 analysts with collecting raw data as well as reviewing alarms and alerts. Then at tier 2, analysts review the more critical security incidents escalated by triage specialists and do a more in-depth assessment using threat intelligence, and finally at tier 3, the analysts are the most experienced workforce in a SOC, who handle major incidents escalated to them from the incident responders. Tier 3 analysts may also perform or at least supervise vulnerability assessments and penetration tests to identify possible attack vectors. In addition to these 3 tiers of analysts, article 2 also discusses the SOC manager, who supervises the security operations team. They can also provide technical guidance if needed. In addition to the analysts and manager, articles 4, 10, and 15 discuss that SOC requires security engineers and/or data analysts. According to article 4, data analysts could help make the ML more usable in SOCs. Furthermore, article 15 discusses that any SOC should have a few operators entering data and analysts on staff who focus solely on analytics. Article 10 mentions that security engineers are responsible for updating and maintaining the security tools and systems used in SOC, whereas the analysts are tasked with identifying and mitigating threats.

Collaboration with other teams and specialists in-house and externally was also discussed. For example, article 2 mentions that "especially in high-pressure environments like a SOC, collaboration amongst the various team members is essential". Article 5 discusses that security operations are a collaborative effort that requires coordination and communication among different roles and teams. Article 13 has similar thoughts on this subject and argues that teams should share and coordinate seamlessly and utilize each other's knowledge and backgrounds to recognize, address, and fix incidents efficiently

and effectively. Furthermore, according to article 15, SOCs should work together with the local incident response team, which in turn collaborates with the national CERT.

5.1.2 Processes

One of the first things when designing a SOC is identifying its necessary functions it needs to perform. According to article 1, this can be performed by architects who need to align their solutions with regulations and custom requirements. Article 4 argues that the SOC team should collect the business requirements, build sustainable architecture, and develop use cases to analyze the data and trigger meaningful alarms. Articles 1, 5, 8, 10, and 11 mention that the SOC's processes should be aligned with laws and regulations that are relevant to its industry or region.

Nearly every article agreed that some of the key processes associated with SOCs are data collection or logging, monitoring, alert & incident categorization and prioritization, and incident response. For example, according to article 3, this requires real-time data collection and detection analysis, aggregation and prioritization of alerts, and visualization of data streams and alerts. Article 2 discusses a similar process comprised of detection, analysis, alert prioritization, and triage. Article 15 highlights that monitoring is understood as a continuous elicitation of events, as well as the collection, analysis, and generalization of the monitoring results. Articles 10 and 13 also highlight the continuous nature of the SOC processes. Article 17 argues that the triage process is an integral part of incident management, which involves reviewing and prioritizing security alerts in a structured manner to ensure that the most meaningful threats are resolved first. Furthermore, articles 1, 2, and 5 all emphasize that the incident response lifecycle should be used by SOCs to ensure efficient management of incidents. Article 6, on the other hand, states that incidents should be forwarded to a dedicated incident response team for further investigation and remediation. Articles 1, 4, 5, 8, 9, 10, 15, and 16 mention the post-

incident response review and/or lessons learned as a crucial component of SOC's processes.

Out of the 21 articles, 8 mentioned that SOC processes should include proactive functions. This includes activities such as regression testing before implementing updates to critical assets, according to article 1. Another proactive approach proposed in article 4 was threat hunting in addition to rule-based alerts. Articles 5, 8, 9, and 15 argue that vulnerability scanning and threat analysis are important proactive SOC functions. In addition to these processes, forensics was also mentioned in articles 8 and 9. Article 10 highlights that proper documentation can speed up SOC processes. Finally, articles 1 and 10 mention that SOCs should also have a framework to reduce 3rd party or supply chain risk.

5.1.3 Technology

Technology is a key aspect of SOC operations, and this is seen mainly as different tools and platforms utilized by SOC analysts. 18 out of the 21 articles mentioned SIEM as a requirement for SOC operations. For example, article 2 states that SIEM is an integral part of many SOCs to cover a large part of the technological requirements. Article 6 claims that the SIEM system is in place to normalize security events from different preventive technologies and flag alerts. Another commonly discussed system in the articles was IDS. This was mentioned by 16 articles. Some articles specified NIDS or HIDS, while others discussed IDSs in general. IPSs were also mentioned by 8 of the articles. For example, article 18 states that "Network Intrusion Detection Systems (NIDS) represent a cornerstone of modern cybersecurity infrastructure", and "a typical Suricata NIDS deployment in a production environment can generate approximately 200,000 alerts daily". Article 7 mentions that IDS and IPS have been considered as effective protection solutions. Articles 5 and 10 state that SOCs also use XDR systems to integrate data from multiple security domains, like endpoint, network, cloud, and email. SOAR systems were

mentioned in articles 5, 10, and 16. Article 5 characterizes SOARs as systems that automate and streamline the incident response process. In addition to these detection and response systems articles, 9 articles mentioned AV, EDR, and/or FW solutions, which all can act as a log source and can also be used for incident prevention and/or remediation. Articles 5, 7, 10, and 13 mention vulnerability scanners. Article 5 states that SOCs use vulnerability assessment tools to detect and evaluate vulnerabilities and their severity. Article 10 also mentions the use of honeypots.

Several intelligence platforms and other databases were also recognized from the articles. Article 1 mentions that SOC should have an asset inventory with "comprehensive details for each asset and a logical map of devices and connections, including a view of communication flows and variable access done by each asset". According to articles 7 and 17, SOCs should also have a MISP. Article 17 states that MISP enables real-time sharing of threat intelligence and incident response capabilities for SOC operations. Article 17 also states that TI platforms should be integrated with alerts to streamline workflows. Article 20 adds that TI feeds can potentially be used to predict possible attacks.

5.1.4 GRC

Different regulations and frameworks are a crucial part of SOC operations. Article 5 even states that a SOC itself is essential for any organization that wants to maintain a high level of cybersecurity and comply with various regulations and standards. Article 2 continues this by stating that a SOC can help to ensure that certain compliance regulations are met and mentions that many of the standards focus on one domain or task within SOCs. A collection of different regulations, standards, frameworks, and best practices was recognized from the reviewed articles. In total, there were 41 of these. They are listed in Table 8:

Table 8. Recognized regulations, standards, frameworks, and best practices

Name	Location	IT	OT	Industry	Type	Domain
ANSI/ISA-99	Worldwide	x	x	Industrial/Manufacturing	Standard	Industrial Control Systems Security
BSI-Standard 100-4	Germany/Worldwide	x	x	Multiple Industries	Standard	Business Continuity
COBIT	Worldwide	x		Multiple Industries	Framework	IT Governance
DCID	USA	x		Defense/Intelligence	Directive	Information Systems Security
DISA	USA	x		Defense/Government	Standard	Defense Information Systems
FDA GXP	USA/Worldwide	x		Pharmaceutical	Regulation	Good Practice Guidelines
FERC/NERC CIP	USA	x	x	Electric Utilities	Regulation	Critical Infrastructure Security
FFIEC	USA	x		Financial Services	Guidance	Financial IT Security
GDPR	EU/Worldwide	x		Multiple Industries	Regulation	Data Protection and Privacy
IEC 62443	Worldwide	x	x	Industrial/Manufacturing	Standard	Industrial Control Systems Security
ISACA Vulnerability Management	Worldwide	x	x	Multiple Industries	Best Practice	Vulnerability Management
ISO 17799	Worldwide	x		Multiple Industries	Standard	Information Security (Legacy)
ISO 22301:2012	Worldwide	x	x	Multiple Industries	Standard	Business Continuity
ISO 22313:2012	Worldwide	x	x	Multiple Industries	Standard	Business Continuity Guidance
ISO/FDIS 22313	Worldwide	x	x	Multiple Industries	Standard	Business Continuity Guidance
ISO/IEC 27001 & 27002	Worldwide	x	x	Multiple Industries	Standard	Information Security Management

ISO/IEC 27005	Worldwide	x	x	Multiple Industries	Standard	Information Security Risk Management
ISO/IEC 27035:2016	Worldwide	x	x	Multiple Industries	Standard	Incident Management
ISO/IEC 27037:2012	Worldwide	x		Multiple Industries	Standard	Digital Evidence Collection
ISO/IEC 27041:2015	Worldwide	x		Multiple Industries	Standard	Digital Forensics Investigation
ISO/IEC 27042:2015	Worldwide	x		Multiple Industries	Standard	Digital Evidence Analysis
ISO/IEC 30141:2018	Worldwide	x	x	IoT/Multiple Industries	Standard	IoT Security
ITIL	Worldwide	x		Multiple Industries	Framework	IT Service Management
MITRE ATT&CK	Worldwide	x	x	Multiple Industries	Framework	Threat Intelligence
NIS / NIS 2	EU	x	x	Critical Infrastructure	Directive	Network and Information Security
NIST 800-12	USA/Worldwide	x		Multiple Industries	Guidance	Computer Security
NIST 800-14	USA/Worldwide	x		Multiple Industries	Guidance	IT Security Principles
NIST 800-26	USA/Worldwide	x		Multiple Industries	Guidance	Security Self-Assessment
NIST 800-40	USA/Worldwide	x		Multiple Industries	Guidance	Patch Management
NIST 800-53	USA/Worldwide	x	x	Multiple Industries	Standard	Security Controls
NIST 800-61	USA/Worldwide	x	x	Multiple Industries	Guidance	Incident Handling
NIST 800-82	USA/Worldwide	x	x	Industrial/Manufacturing	Guidance	Industrial Control Systems Security
NIST 800-83	USA/Worldwide	x		Multiple Industries	Guidance	Malware Prevention
NIST 800-86	USA/Worldwide	x		Multiple Industries	Guidance	Digital Forensics
NIST 800-92	USA/Worldwide	x	x	Multiple Industries	Guidance	Log Management
NIST CSF	USA/Worldwide	x	x	Multiple Industries	Framework	General Cybersecurity
NIST RMF	USA/Worldwide	x	x	Multiple Industries	Framework	Risk Management

PCI DSS	Worldwide	x		Payment Card Industry	Standard	Payment Security
SANS Implementing a Vulnerability Management Process	Worldwide	x	x	Multiple Industries	Best Practice	Vulnerability Management
SANS Incident Handler's Handbook	Worldwide	x	x	Multiple Industries	Best Practice	Incident Response
SOX	USA/Worldwide	x		Public Companies	Act	Financial Reporting Controls

It can be seen that several different regulations, standards, frameworks, etc., impact SOCs. It can also be seen that some items in Table 8 affect only IT or OT SOCs, and some apply to both of these environments. However, it must also be noted that not every item in Table 8 affects every SOC. It depends on a case-by-case basis from aspects such as the organization's region, industry, size, and many other elements. Article 1 also notes that some of the regulatory measures oblige organizations to maintain communications with multiple external organizations across different stages of the cyber protection life cycle, such as the national CERT mentioned by article 15 before.

Nine out of the 21 articles stated that compliance is a key requirement for SOC operations. Article 1 highlights that the management of security policies involves compliance with regulatory requirements, business policy, and organizational goals, and compliance with the requirements of security standards. According to article 15, compliance with SOC binds events to existing laws, IS policies, and standards. One way to measure compliance and SOC efficiency is through metrics. In total, 4 articles mentioned the use of metrics to measure efficiency and/or compliance. Article 2 mentions that metrics are quantifiable measures used to track and assess the status of a process or system. Article 10 adds that SOCs can use GRC tools to track and report metrics.

Additionally, SOCs should have risk management policies and plans. Article 10 states that "organizations should create governance frameworks, organizational structures, policies, and procedures to analyze the cybersecurity risks they are facing". Article 10 adds that the development of risk management policy is the first step in managing risk. According

to article 15, organizations should conduct risk management and risk ranking based on business impact analysis, including passive and active risk assessment & treatment, monitoring, and communication.

It can be noticed that SOCs have a large number of common requirements. Article 13 summarizes this by stating that “all organizations should specify and provide essential resources, including a budget allocation, cybersecurity policies, processes, procedures, and internal standards, cybersecurity metrics, services, personnel, and their proficiency, awareness, and inter-communication”. In the next subchapter, the key differences between IT and OT SOCs will be discussed.

5.2 Differences in IT and OT SOCs

While the previous section established the fundamental commonalities that correspond to both IT and OT SOCs, the literature analysis reveals significant distinctions that differentiate these two SOC types in their operational approach, technical implementation, and organizational structure. These differences stem from the unique characteristics of the environments they protect, with IT SOCs focusing on data confidentiality and information system availability, while OT SOCs prioritize operational safety, system reliability, and physical process continuity. The identified differences across the four core pillars of People, Processes, Technology, and GRC demonstrate how the shared foundational requirements must be adapted and specialized to address the distinct challenges, risk profiles, and operational priorities inherent in each domain. The following subsections examine how each of the four fundamental pillars manifests differently in IT versus OT SOC implementations, providing insight into the specialized approaches required for effective security operations in each environment.

5.2.1 People

For the People aspect of the SOC operations, there weren't a huge number of differences between IT and OT SOCs mentioned in the reviewed papers. Article 2 mentions that it is inevitable to include domain knowledge of security experts and even non-security experts in both settings, meaning that the knowledge of the dedicated environment differs between IT and OT systems. Article 19 also highlights the understanding of your own domain's technology and communication. Article 1 adds that the ICS personnel do not necessarily understand the extent of facilities' vulnerability to cybersecurity threats and do not realize that facilities may have internet connectivity, since OT systems were not often designed to operate in networked environments. This means that analysts working in OT SOCs have to consider this aspect when collaborating with ICS personnel.

5.2.2 Processes

The processes in the SOC operations differ in the IT SOCs compared to the OT SOCs. Even though these SOCs shared many common aspects in their processes, they also have some differing approaches. 5 out of the 21 articles mentioned the different requirements in the OT and IT systems that affect the processes conducted by SOCs. Article 1 mentions that organizations need to take into account a lot of differences between security requirements and needs for traditional ICT systems and ICS systems. Article 11 states that traditional IT cybersecurity countermeasures are generally not suitable for OT environments due to fundamental differences and operational environments & requirements. Article 7 adds that some OT networks are having trouble using typical IDS techniques because of things like limited resources, particular protocols, energy consumption, and other unique elements of OT systems. Article 7 adds that SIEM systems also face these issues due to the same unique aspects of OT systems. According to article 1, the identification of the data sources on SCADA systems is difficult.

These differences in IT and OT system requirements and operational environments create an array of challenges in the world of digital forensics, monitoring, and incident response in OT SOCs. According to Article 11, traditional IT security processes, such as frequent patching, antivirus scans, and software updates, can introduce latency and require system reboots, which are unacceptable in OT contexts, making the processes OT and IT processes inherently different. Article 3 highlights the physical aspect of OT systems, which may require physical incident response processes that are not commonly found in IT SOC processes. Furthermore, article 3 highlights that OT systems handle physical operations, such as power flow between substations. This makes physical safety a unique and critical aspect for OT SOCs to consider in their processes, which is not commonly present in IT SOC processes.

5.2.3 Technology

In the Technology aspect, some key differences between IT and OT SOCs were observed in the reviewed papers. Articles 1, 2, 3, 7, 11, and 19 discussed the technical limitations in OT devices. Article 1 states that embedded OT devices have low memory and processing power. Furthermore, article 1 mentions that many OT systems were not intended for this connected world, and therefore, security testing was formerly neglected. Article 1 also mentions that these technical limitations in OT systems limit the data retention of these systems and make forensics difficult. Article 11 also states that ICS devices often run on legacy hardware and software, which may not be compatible with modern IT security solutions. Article 7 adds that IoT networks are having trouble using typical IDS techniques because of similar limitations, like limited resources, particular protocols, and energy consumption. Article 19 also states that many IoT devices are limited in bandwidth, power, and overall process functionality, and proprietary IoT designs add challenges to security controls.

These technical limitations affect the tooling used in OT SOCs. According to article 3, software used for modeling IT and communications network security is not adapted for modeling OT systems. According to article 3, there is also a lack of network tools specific to OT field devices. In addition to this, SIEMs have been historically deployed in IT environments, but the complexity and criticality of OT systems, along with network access, segmentation, and the architecture of OT network infrastructure, make it difficult to adapt them to OT SOCs. Article 2 also states that SOC tools typically only cover the standard IT technologies and have no visibility into OT systems. Article 7 continues with tooling incompatibility between IT and OT SOCs. According to article 7, signature-based detection methods, which are typically used in IT SOCs, are not suitable for OT systems due to the previously mentioned technical limitations.

5.2.4 GRC

Differences in the GRC landscape of IT and OT SOCs mainly differed in the different legal regulations and frameworks unique to both environments, according to the reviewed papers. Primarily, this was seen by OT SOC-related articles 1, 9, 11, and 17, mentioning that OT SOCs are required to follow regulations, such as FERC/NERC CIP, ANSI/ISA-99, IEC 62443, NIST 800-82, and NIST 800-53, which are specific to OT SOCs. On the other hand, Articles 2 and 17 mention IT SOC-related regulations, such as DCID, FFIEC, NIST 800-14, SOX, and PCI DSS.

Subchapter 5.2 presented a set of key differences existing in the IT and OT SOCs. In some of the four aspects, the differences were minimal, whereas in some, there were significant differences between the two SOC environments. The following subchapter will outline some issues and improvements in IT and OT SOCs that were presented in the chosen papers.

5.3 Issues and improvements in IT and OT SOCs

Building upon the understanding of both the shared foundations and distinctive characteristics of IT and OT SOCs established in the previous sections, the literature analysis reveals a comprehensive landscape of challenges, limitations, and opportunities for enhancement across both SOC types. While sections 5.1 and 5.2 outlined what constitutes effective SOC operations and how these manifest differently across IT and OT environments, the current findings highlight persistent gaps, emerging threats, and evolving requirements that demand continuous improvement and adaptation. The identified issues span from fundamental resource constraints and skill shortages to sophisticated technical challenges and evolving regulatory demands that affect both IT and OT SOC operations. Simultaneously, the literature presents improvement strategies, emerging best practices, and innovative approaches that can be implemented to address these challenges and enhance their security operations capabilities. The following subsections examine these issues and corresponding improvement opportunities across the four core SOC pillars, providing a balanced perspective on both the obstacles facing modern SOC operations and the practical solutions being developed to overcome them.

5.3.1 People

Several key issues and improvements were found in the reviewed papers. According to article 8, there is a lack of budget and organizational agility in SOCs. Article 8 also adds that another issue is the lack of skill and knowledge among personnel. Articles 1, 2, 10, 13, and 15 also highlighted the lack of personnel skill. Furthermore, articles 1, 10, and 13 emphasize that there is a lack of personnel in the SOC field altogether. These issues seemed to exist regardless of the environment of the SOC. Some improvements were presented to lack of personnel and skill among personnel. Article 1 proposed a shared SOC, where one OT SOC operates in multiple environments. According to article 1, this

could help to mitigate the lack of skilled personnel. Furthermore, articles 1, 2, 10, 13, 15, 17, 19, and 21 highlighted the importance of employee training and awareness. This was the most commonly emerging approach to combat the lack of skilled staff. Article 8 noted that personnel should also learn from the incidents and vulnerabilities that occurred in their environments.

According to articles 2 and 5, there is limited access to the data that staff need to perform their duties. This issue also seems to exist in both IT and OT environments. Both of the articles proposed the use of workflow automation, data integration, and improved communication & knowledge sharing to improve this issue. Finally, one of the most commonly existing issues in both environments was alert fatigue and mundane tasks experienced by the SOC personnel. This issue was brought up by articles 2, 4, 5, 6, 12, 17, 18, and 20. For mundane tasks, article 2 proposed a gamification approach to SOC operations to retain SOC operators' motivation. Alert fatigue was commonly mitigated by adding automation, ML & AI tooling, and fine-tuning to create more meaningful alerts to SOCs.

5.3.2 Processes

Issues in the Processes aspect were mainly focused on different issues regarding the alarms SOCs receive. In OT SOCs, according to articles 1 and 19, identification of data sources on OT systems was specifically an issue that didn't seem to exist in IT SOCs. According to article 1, this lack of source identification made forensic processes not possible or very limited for OT systems. Furthermore, article 4 discusses issues existing in IT SOCs regarding logging and alarms. According to article 4, some of the key issues are manual log review, which is nearly impossible to use to find suspicious activities due to the continuous manner of logging, prioritization, and implementation issues, which are caused by organizations trying to implement much of services as possible without having a clear strategy. Finally, articles 4, 5, 12, 14, 19, 20, and 21 mentioned a lack of

meaningful alarms generated as a key issue in SOCs. Article 14 states that tracking alerts is a cumbersome process, which takes many human hours, and if it results in false positives, it is a waste of valuable time. Article 19 also emphasizes the importance of avoiding false negatives.

Examined papers had improvements to these issues regarding alarms and logging processes. In both environments, 10 articles proposed an increase in the use of automation to make SOC processes more effective. Articles 6, 12, 17, 18, and 19 even included the use of ML to enhance SOC processes. Furthermore, articles 7, 10, 14, 17, 18, 19, 20, and 21 suggested that by reducing the false positive rate in SOCs, you could improve the SOCs processes. This could be achieved by a few things, such as having better visibility in environments, as proposed by article 13. Another way, proposed by articles 10, 14, and 17, is to integrate TI platforms and capabilities to enhance SOC processes and reduce the rate of false positives. According to article 5, SOCs should be able to SOCs should be able to transform natural language descriptions of detection concepts, like rules, signatures, or indicators of compromise, into an executable format that can run on their security tools and systems to reduce false positives and improve SOC processes. Articles 4 and 14 propose that SOCs should use hunting rules as analytics rules in security tools. With this approach, the normally manual threat hunting is being converted into an automated process. In addition to these improvements, Article 13 proposes the use of secure development life cycle practices to address the security concerns and to help with vulnerability management.

5.3.3 Technology

For the OT environments, the main issue in the Technology aspect was the lack of suitable tools for OT SOC operations. Articles 1, 2, 3, 7, and 11 all highlight this issue, with article 1 stating that there is a lack of forensic tools for OT environments. According to article 2, the traditional SOC tools used in IT SOCs are not suitable for OT environments

in most cases. Article 3 states that there is a lack of networking tools for OT field devices. Article 11 tries to address this issue by developing its own platform to monitor OT networks.

Alert fatigue and the rate of false positives were issues discussed in previous subchapters. The articles examined provided several technological solutions to these issues. 10 of the 21 reviewed articles proposed the use of ML and AI capabilities integrated into the SOCs in both OT and IT environments. Article 1 states that SOCs could use reinforcement learning for vulnerability discovery. According to Article 7, SOCs could use random forest ML algorithms to learn the baseline from the network traffic. Article 9, on the other hand, suggests that SOCs could utilize AI-powered both static and dynamic code analysis techniques to identify possible injection attacks. Article 10 suggests that SOCs should strive to use technologies, such as ML and AI, to strengthen their cybersecurity capabilities. Article 12 proposes its own model that uses a hybrid approach integrating XGBoost, CNN-Transformer, Autoencoder-GNN, and LLM to improve classification accuracy and reduce false positives, capture complex patterns in logs, and detect anomalous behaviors more accurately. Article 14 states that ML is a valuable component for automation in a SOC, and it mainly helps the threat hunting process by automating various threat hunting processes with the help of process analysis. According to article 17, recent AI and ML advancements have revolutionized the potential of SOCs by offering tools to augment capabilities by automating routine tasks and innovatively analyzing abundant security data. In addition to ML and AI technologies, Article 2 proposes the integration of UBA tooling to SIEM solutions. This solution improves the monitoring of misused credentials in an organization. Furthermore, articles 14, 15, and 17 highlight the use of SI tooling. According to article 15, this integrated architecture offers protection against attacks, provides full visibility and control, and context-driven SI for SOCs. Finally, article 21 brings up the improvement of the cost-efficiency for SOCs by using open-source solutions in SOCs.

5.3.4 GRC

In the GRC aspect of SOCs, the first issue that seemed to be especially OT SOC-specific was outdated regulations and policies. Article 1 states that regulations and policies are unable to keep up to date with the latest security threats as they emerge. According to article 2, comprehensive standards and industry-specific guidelines are lacking compared to other components of SOCs. According to article 3, conflicting and outdated regulatory policies can pose a significant challenge to OT SOCs. Regulatory issues also appeared in IT SOCs. Article 5 states that “Many SOCs have to operate in a legal, regulatory, and compliance 'grey' area-if their security hygiene, privacy, regulators, and lawyers knew every detail of what they did and how they did it, they'd be hobbled or out of business”. Furthermore, article 1 also highlights the lack of reporting as an issue SOCs often face.

A few solutions were recognized to improve SOCs' GRC posture. Articles 9, 13, and 15 stated that SOCs should continuously update their policies. This applied to both IT and OT SOCs. Article 9 suggests that knowledge from SOC operations can be employed to update security policies and make any required modifications to their frameworks. According to article 16, updating and changing policies is a continuous development and integration process. Article 10 addresses the lack of reporting issue brought up by article 1. Article 10 proposes that SOCs can use SIEM systems to generate automated reporting. Additionally, article 10 proposes that SOCs should implement dedicated GRC tools to help with reporting. Article 17 proposes that there should be a pan-European cybersecurity incident information-sharing platform to support cooperative detection and mitigation of cyber threats. According to article 17, this platform would correspond with the recent NIS2 directive objectives and cross-border collaboration. Finally, article 20 aims to improve the cost-efficiency of SOCs by implementing the Gordon-Loeb model in the SOCs. According to article 20, SOCs could use this model to estimate a global optimal resource allocation while achieving a smaller predicted loss than a collection of the best traditional models that dynamically adjust to the threat's changes across time and space.

5.4 Converged SOCs

The preceding analysis has treated IT and OT SOCs as separate entities to systematically identify their common characteristics, differences, issues, and improvements. However, the literature increasingly recognizes a trend driving the need for a more integrated approach, with the convergence of IT and OT networks. As industrial systems become more connected and data-driven, the traditional air gap is dissolving, creating a seamless attack surface that invalidates siloed security monitoring. In response to this reality, the concept of converged or IT/OT SOCs emerges as a strategic model for unifying security operations. Drawing upon the findings from the previous sections, this final results subchapter synthesizes the data from the reviewed articles to explore this advanced paradigm. It will examine the arguments for achieving holistic visibility and a unified response capability, while also considering how the foundational differences and challenges identified in this study must be carefully managed within a single, cohesive operational framework.

The converged SOC model is not impossible to execute, since there already exist solutions with this model. For example, papers 3 and 19 propose this type of solution from the research articles. However, it must be noted that while article 3 proposes a SOC model with IT/OT SOC that includes ICSs, article 19 only focuses on IoT devices, which are a subset of OT systems. There is a collection of similarities, differences, issues, and improvements in both IT and OT systems as discussed before. These need to be considered in how these aspects affect, improve, and/or worsen the implementation of IT/OT SOC.

One of the key requirements for this type of SOC would be the SOC analysts and other supporting staff who are capable of operating in IT/OT SOCs. As discussed before, finding skilled staff for either IT or OT SOCs is difficult, so combining these environments raises

the skill requirements even further and making the finding of suitable staff even more difficult. Article 19 states that the SOC team also needs to acquire a fundamental understanding of the IoT protocols and security weaknesses that are different from other computer platforms. This would also apply in those cases where SOCs are not limited to just IoT but OT as a whole. Article 3 also highlights that another challenge could arise from communication with other teams, since the OT and IT systems are often maintained by separate entities.

In the IT/OT SOC model, the SOCs would have to define their processes to be suitable for both environments. This may be difficult, since OT systems have an architecture and different goals compared to IT systems. For example, article 3 highlights that in incident response processes, different approaches are used for IT and OT environments. This means that organizations should have separate processes depending on whether it concerns IT and/or IT environments. However, the IT/OT SOC provides better visibility for SOC operations as a whole. This is particularly useful if there is a major incident that concerns both IT and OT environments at the same time. In this case, the greater visibility could provide a better understanding of the scale of the incident and help to mitigate it faster.

As discussed before, the OT environment lacks proper tooling for SOCs. The lack of suitable tools would be a greater issue in a converged environment since the IT/OT specific tools are even more scarce. One solution is to use different tooling for different environments, but the downside is the cost and the added complexity of the SOC architecture. Modern SOC tools, such as XDR, TI, and SI solutions, would be greatly beneficial in these types of environments, since XDR collects, correlates, and aggregates data from multiple different platforms and sources, and can also be used to respond to the alarms and incidents. The SI & TI tools could further enhance the converged SOC operations by bringing meaningful threat and security intelligence to aid the SOC's efficiency. Furthermore, the integration of ML and AI solutions would greatly enhance the speed, create meaningful alerts, and reduce alert noise in the converged SOCs.

In a regulatory view, there are conflicting requirements in IT/OT SOCs. According to article 3, conflicting and outdated regulatory policies can pose a significant challenge to the IT/OT data convergence and data management. Furthermore, as discussed before, there are a lot of different regulations, frameworks, best practices, etc. Some of these only applied to IT environments, some to only OT environments, and some to both. Depending on the organization's region, industry, and many other aspects, the number of different regulations the organization needs to be compliant with can be large. This can be expensive, time-consuming, and conflicting for the organization.

It can be seen that there are several key requirements and issues that organizations need to address if they want to implement the IT/OT SOC model. However, if an organization can overcome these requirements, the added visibility and response capabilities benefit the overall security posture of the whole organization.

6 Discussion

The convergence of IT and OT systems has led to a new era of automation, data analytics, and operational efficiency, revolutionizing industries across the globe. However, this convergence also presents significant challenges to cybersecurity, as discussed before. This research, through a comprehensive literature review, has investigated the requirements, differences, issues, and improvements of IT and OT SOCs and the emerging field of IT/OT SOCs.

6.1 Summary of Findings

The review revealed that the unique characteristics of IT and OT environments necessitate distinct approaches to security operations. IT environments are typically characterized by well-defined infrastructure, standardized protocols, and established security practices. However, OT environments often involve legacy systems, proprietary protocols, and real-time operational constraints, posing unique challenges to security management. Moreover, the integration of IT and OT systems introduces new vulnerabilities, as attacks can now potentially propagate from IT networks into critical infrastructure, with potentially devastating consequences.

The research identified key requirements for successful IT & OT SOCs. These include personnel with a deep understanding of both IT and OT security. Furthermore, effective IT & OT SOCs must utilize a range of specialized security tools designed to detect, analyze, and respond to threats in both IT and OT environments. These tools should be capable of monitoring diverse data sources, including industrial control system data, network traffic, and system logs. This requires standardized processes for threat detection, incident response, and communication across different teams and departments. Finally, to ensure effective IT & OT security, organizations must establish robust governance

frameworks that define clear security policies, risk management procedures, and compliance requirements.

6.2 Implications for Practice

The findings underscore the importance of a comprehensive and integrated approach to IT/OT security. Organizations must recognize the interconnected nature of these environments and implement strategies that address the unique challenges of securing both IT and OT systems. This includes:

1. Establishing teams with expertise in both IT and OT security is crucial for effective security operations. These teams should work collaboratively to share threat intelligence, coordinate incident response, and develop integrated security strategies.
2. The rapid evolution of IT/OT technologies and threats requires ongoing training and education for security personnel. This includes training in new technologies, emerging threats, and best practices for managing security in converged IT and OT environments.
3. SOC processes must be continuously adapted to address evolving threats and the introduction of new technologies. Organizations must monitor the security landscape, evaluate emerging vulnerabilities, and adjust their security controls accordingly.

The research concludes with several recommendations for organizations seeking to establish or enhance their IT/OT SOC capabilities:

1. Recruit and retain personnel with expertise in both IT and OT security.
2. Consider investing in training programs to enhance the skills of existing staff.

3. Utilize a suite of security tools designed to monitor, detect, and respond to threats in both IT and OT environments.
4. Establish clear and standardized processes that are documented, tested, and regularly reviewed for threat detection, incident response, and communication across IT and OT teams.
5. Implement a comprehensive, regularly reviewed, and updated security governance framework that includes clear security policies, risk management procedures, and compliance requirements.

By implementing these recommendations, organizations can build robust IT/OT SOCs that effectively mitigate cyber risks, ensure the secure operation of converged IT and OT systems, and protect critical infrastructure from evolving threats.

6.3 Future Research

While this literature review provides insights into the fields of IT, OT, and IT/OT SOCs, the rapid evolution of technologies and the evolving threat landscape necessitate ongoing research and exploration. Several promising areas for future research can build upon the findings of this review:

1. Developing standardized frameworks for converged IT/OT SOCs would significantly enhance the implementation and management of integrated security operations.
2. The rapid adoption of technologies like cloud computing, AI & ML, and IIoT has significant implications for IT/OT security.
3. Future research should explore how human factors, such as training, skill development, team dynamics, and organizational culture, impact the performance and effectiveness of IT/OT SOCs.

4. Future research could focus on specific industries to investigate the unique security challenges and requirements of these sectors. For example, research could explore the security considerations for IT/OT SOCs in the energy sector, manufacturing, healthcare, or transportation.

Further research in these areas will contribute to the development of best practices, standardized frameworks, and robust security strategies for managing IT/OT security in the increasingly interconnected and dynamic environments.

References

Advanced Micro Controls. (2017). What is a PLC? Amci.com. https://www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/

Akhtar, Z. (2021, January). *Malware Detection and Analysis: Challenges and Research Opportunities*. ResearchGate. https://www.researchgate.net/publication/348675495_Malware_Detection_and_Analysis_Challenges_and_Research_Opportunities

Alharbi, S. (2020). A QUALITATIVE STUDY ON SECURITY OPERATIONS CENTERS IN SAUDI ARABIA: CHALLENGES AND RESEARCH DIRECTIONS. *Journal of Theoretical and Applied Information Technology*, *31*, 24. https://www.jatit.org/volumes/Vol98No24/5Vol98No24.pdf

Andrade, R., & Torres, J. (2018). Enhancing intelligence SOC with big data tools. https://doi.org/10.1109/iemcon.2018.8614779

Ansari, S., Castro, F., Weller, D., Babazadeh, D., & Lehnhoff, S. (2019). Towards Virtualization of Operational Technology to Enable Large-Scale System Testing. https://doi.org/10.1109/eurocon.2019.8861980

Arfaoui, B., Mrabet, H., & Jemai, A. (2023). "SOCaaS-IoT" A Security Operations Center as a Service Approach for IoT Applications Using Open-Source SIEM. https://doi.org/10.1109/amcai59331.2023.10431525

Awati, R. (2024, July 16). What is remote terminal unit (RTU)? Techtarget. https://www.techtarget.com/whatis/definition/remote-terminal-unit

Berardi, D., Callegati, F., Giovine, A., Melis, A., Prandini, M., & Rinieri, L. (2023). When Operation Technology Meets Information Technology: Challenges and Opportunities. Future Internet, 15(3), 95. https://doi.org/10.3390/fi15030095

Bikov, T., Radev, D., Iliev, T., & Stankovski, D. (2021). Threat Hunting as Cyber Security Baseline in the Next-Generation Security Operations Center. 2021 29th Telecommunications Forum (TELFOR). https://doi.org/10.1109/telfor52709.2021.9653361

Boljam, A. M., Saini, V., Bojja, S. G. R., Mohammed, H. UL. H., & Alluri, V. R. R. (2025). Novel Method of Improving Cybersecurity Posture with Real-Time Analytics in

Security Operations Centers. 1–8. https://doi.org/10.1109/ic-ctdc64446.2025.11157987

Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S. C., & Erwin, S. (2023). Testing SOAR tools in use. *Testing SOAR Tools in Use*, *129*, 103201–103201. https://doi.org/10.1016/j.cose.2023.103201

CompTIA. (2023). What is information technology. CompTIA. https://www.comptia.org/content/articles/what-is-information-technology

Conklin, A. (2016). IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience. 2016 49th Hawaii International Conference on System Sciences (HICSS). https://doi.org/10.1109/hicss.2016.331

Cox, R. G. (2024, February 13). Detection Engineering the SOC: Writing a Detection Rule. InfoSec Write-Ups; Medium. https://infosecwriteups.com/detection-engineering-the-soc-writing-a-detection-rule-e24f4d7f69e8

Davies, G. (2019). Networking Fundamentals. Packt Publishing. ISBN 978-1-83864-350-8

Dimitrov, W., & Syarova, S. (2019). Analysis of the Functionalities of a Shared ICS Security Operations Center. https://doi.org/10.1109/bdkcse48644.2019.9010607

Feng, C., Wu, S., & Liu, N. (2017). A user-centric machine learning framework for cyber security operations center. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). https://doi.org/10.1109/isi.2017.8004902

Gaggero, G. B., Caviglia, R., Girdinio, P., & Marchese, M. (2024). Toward a Security Operation Center for Operational Technology in Industrial Networks. 160–164. https://doi.org/10.1109/techdefense63521.2024.10863654

Gartner. Top 9 Security and Risk Trends for 2020. (n.d.). https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020

Hahn, A. (2016). Operational Technology and Information Technology in Industrial Control Systems. Advances in Information Security, 51–68. https://doi.org/10.1007/978-3-319-32125-7_4

Hasan, M. M., Rahman, M. M., Rahman, M. M., Farhad, M. K. R., Billah, M. M., & Ullah, N. (2025). Network IDS Alert Classification Using Hybrid Transfer-Active Learning:

Reducing Analyst Burden in SOC Environments. 2025 IEEE 7th Symposium on Computers & Informatics (ISCI), 333–338. https://doi.org/10.1109/isci65687.2025.11167382

Hupp, W., Hasandka, A., Carvalho, R. M., & Saleem, D. (2020). Module-OT: A Hardware Security Module for Operational Technology. 2020 IEEE Texas Power and Energy Conference (TPEC). https://doi.org/10.1109/tpec48276.2020.9042540

Hu, L., Li, H., Wei, Z., Dong, S., & Zhang, Z. (2019, March 1). Summary of Research on IT Network and Industrial Control Network Security Assessment. IEEE Xplore. https://doi.org/10.1109/ITNEC.2019.8729052

IBM. (n.d.). What are the basic elements of a network? Www.ibm.com. https://www.ibm.com/docs/en/zos-basic-skills?topic=networks-what-are-basic-elements-network

Joffel, E. (2022). IT SOC transition combined to IT and OT SOC TJK 17 Kehitysprojektin raportti. https://www.aaltoee.fi/media/aalto-ee-publications/tjk/joffel-esa-it-soc-transition-combined-to-it-and-ot-soc-.pdf

Kaliyaperumal, L. N. (2021). *The Evolution of Security Operations and Strategies for Building an Effective SOC*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

Kanamaru, H. (2020). Requirements for IT/OT Cooperation in Safe and Secure IACS. 39–44. https://doi.org/10.23919/sice48898.2020.9240295

Khayat, M., Barka, E., Serhani, M. A., Farag Sallabi, Shuaib, K., & Khater, H. M. (2025). Empowering Security Operation Center with Artificial Intelligence and Machine Learning – A Systematic Literature Review. IEEE Access, 1–1. https://doi.org/10.1109/access.2025.3532951

Koizumi, S., & Shiozaki, T. (n.d.). IIoT SOC Service. Retrieved October 4, 2025, from https://web-material3.yokogawa.com/1/33381/files/rd-te-r06501-006.pdf

Kok, A., Martinetti, A., & Braaksma, J. (2024). The impact of integrating information technology with operational technology in physical assets: a literature review. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3442443

Laudon, K., & Laudon, J. (2022). *Management Information Systems: Managing the Digital firm, Global edition.* (17th ed.). Pearson Education Limited. ISBN 978-1-292-40328-1

Lotfi, I., & Meriem Mandar. (2025). Review of Detection and Prevention Techniques for Cyberattacks in SOCs: State of the Art and Future Challenges. 1–6. https://doi.org/10.1109/iccsc66714.2025.11135218

Mahan, R., Burnette, J., Fluckiger, J., Goranson, C., Clements, S., Kirkham, H., & Tews, C. (2011). Secure Data Transfer Guidance for Industrial Control and SCADA Systems. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

ManageEngine (2023). Network Monitoring Software by ManageEngine OpManager. ManageEngine OpManager. https://www.manageengine.com/network-monitoring/network-protocols.html

Martin, M. (2025, July 31). CIA Triad in Cybersecurity: Principles & Real-World Examples. Atlassystems.com; Atlas Systems Pvt. Ltd. https://www.atlassystems.com/blog/cia-triad-in-cybersecurity

Miloslavskaya, N. (2016). Security Operations Centers for Information Security Incident Management. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*. https://doi.org/10.1109/ficloud.2016.26

Miloslavskaya, N., Tolstoy, A., & Zapechnikov, S. (2016). Taxonomy for Unsecure Big Data Processing in Security Operations Centers. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). https://doi.org/10.1109/w-ficloud.2016.42

Mocanu, F., & Scripcariu, L. (2023). Implementation of a Security Operation Center - An Essential Cybersecurity Solution for Organizations. https://doi.org/10.1109/icstcc59206.2023.10308432

Moura, R. L., & Ceotto, L. L. (2024). Operational Technology: The New Role of Enterprise Architecture in the Context of IT & OT Convergence. 10–16. https://doi.org/10.1109/aeis65978.2024.00010

Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. *The Proceedings Of 15th Australian Information Security Management Conference (Pp. 149-155)*. https://doi.org/10.4225/75/5a84f7b595b4e

Na, M. R. & Sundharakumar, K. B. (2024). A Study on Air-Gap Networks. https://doi.org/10.1109/icitiit61487.2024.10580382

Nafees, M. N., Saxena, N., Cardenas, A., Grijalva, S., & Burnap, P. (2023). Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review. ACM Computing Surveys, 55(10), 1–36. https://doi.org/10.1145/3565570

Osazuwa, M. C., & Mitchell, O. (2023). Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature. *International Journal of Innovative Science and Research Technology*, *8*(12). https://doi.org/10.5281/zenodo.10464076

Paul, P. K., Aithal, P. S., Saavedra, R., Sinha, R. R., Aremu, B., & Mewada, S. (2021). Information Systems: The Changing Scenario of Concepts, Practice and Importance. Scholedge International Journal of Management & Development ISSN 2394-3378, 7(7), 118. https://doi.org/10.19085/sijmd070701

Perera, A., Rathnayaka, S., Perera, N. D., Madushanka, W. W., & Senarathne, A. N. (2021, April 1). The Next Gen Security Operation Center. IEEE Xplore. https://doi.org/10.1109/I2CT51068.2021.9418136

Pikó, A., Bánáti, A., & Kail, E. (2024). Supporting NIS 2 Directive with SOC. 533–540. https://doi.org/10.1109/sisy62279.2024.10737537

Reyna, A., Collins, T., Shamina Hossain-McKenzie, Blakely, L., Goes, C., Anderson, R., & Hubbell, C. (2024). Towards the Design of Grid Cyber-Physical Integrated Security Operations Center Visualizations. 1–6. https://doi.org/10.1109/kpec61529.2024.10676242

Shahjee, D., & Ware, N. R. (2022). Designing a Framework of an Integrated Network and Security Operation Center: A Convergence Approach. https://doi.org/10.1109/i2ct54291.2022.9825084

Simos, M., Laidler, K., & Dellinger, J. (2019, April 23). CISO Series: Lessons learned from the Microsoft SOC—Part 2a: Organizing people. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2019/04/23/lessons-learned-microsoft-soc-part-2-organizing-people/

SOCFortress. (2022). Playbooks for SOC Analysts. GitHub. https://github.com/socfortress/Playbooks/tree/main

Sonkor, M. S., & García de Soto, B. (2021). Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective. Journal of Construction Engineering and Management, 147(12). https://doi.org/10.1061/(asce)co.1943-7862.0002193

Stair, R., & Reynolds, G. (2016). Principles of information systems. (13th ed.). Cengage Learning. ISBN 978-1-305-97177-6

Stouffer, K., et al. (2023). Guide to Operational Technology (OT) Security. Guide to Operational Technology (OT) Security. https://doi.org/10.6028/nist.sp.800-82r3

Tao, Y., Xu, W., Li, H., & Ji, S. (2019, July 1). Experience and Lessons in Building an ICS Security Testbed. IEEE Xplore. https://doi.org/10.1109/ICIAI.2019.8850804

Theis, T. N., & Wong, H.-S. P. (2017). The End of Moore's Law: A New Beginning for Information Technology. Computing in Science & Engineering, 19(2), 41–50. https://doi.org/10.1109/mcse.2017.29

Tlili, F., Ayed, S., & Fourati, L.C. (2024). Towards a Responsive Security Operations Center for UAVs. 2022 International Wireless Communications and Mobile Computing (IWCMC), 1263–1268. https://doi.org/10.1109/iwcmc61514.2024.10592542

Traficom. (2022). Instructions - Denial-of-service attack. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohyokkays_EN.pdf

Tripwire. Navigating Industrial Cybersecurity: (2019). Tripwire.com. https://www.tripwire.com/resources/guides/navigating-industrial-cybersecurity

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/access.2020.3045514

Weissman, D., & Jayasumana, A. (2020, June 1). Integrating IoT Monitoring for Security Operation Center. IEEE Xplore. https://doi.org/10.1109/GI-OTS49054.2020.9119680

Williams, T. J. (1993). The Purdue Enterprise Reference Architecture. IFAC Proceedings Volumes, 26(2), 559–564. https://doi.org/10.1016/s1474-6670(17)48532-6

Zimmerman, C., & Bhargav-Spantzel, A. (2023). SOC and Academia – Building Resilient Systems. 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 396–399. https://doi.org/10.1109/tps-isa58951.2023.00055