Exploring the Interaction between Security Operations Center and Industrial in-house Response Teams

Vahiny Gnanasekaran
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
vahiny.gnanasekaran@ntnu.no

Poul E. Heegaard
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
poul.heegaard@ntnu.no

ABSTRACT

This study aims to explore the interaction between Security Operations Center (SOC) and industrial companies during critical cyber incidents using a qualitative research approach. Interviews and observational studies will be conducted to identify factors affecting effective communication and collaboration. The findings will contribute to the development of strategies to enhance SOC and industrial client cooperation in safeguarding Operational Technology (OT)assets against cyber threats.

KEYWORDS

Security Operations Center, Industrial Control System, ICS, OT

ACM Reference Format:
Vahiny Gnanasekaran and Poul E. Heegaard. 2023. Exploring the Interaction between Security Operations Center and Industrial in-house Response Teams. In *Proceedings of 10th ACM Celebration of Women in Computing (womENcourage '23).* ACM, New York, NY, USA, 2 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

In recent years, there has been a significant increase in the adoption of Security Operational Centers (SOCs) by companies providing IT services, especially in the context of integrating Operational Technology (OT) systems with IT solutions. Industrial companies are exploring the possibilities of continuously monitoring their OT infrastructure for cyber incidents, breaches, and policy violations by appropriately responding, logging, and investigating the events. The SANS Institute's report on OT/ICS cybersecurity revealed that adopting SOCs to OT environments has increased drastically from 2019 to 2021 [2].

However, there are several considerations to review when transferring IT-supported services to OT environments [4, 7, 8]. For instance, OT systems consist of legacy systems and highly regard upholding process availability, indicating a reluctance for unplanned shutdowns. Distinct communication patterns in the OT domain might differ from a traditional IT perspective, thereby alerting monitoring services even when there are no cyber risks. Additionally, SOCs monitoring OT systems should be aware of the increased risk from maintenance and external personnel bringing infected devices into the digital infrastructure.

To provide sufficient and adequate monitoring, detection, response, and recovery of OT systems, coordination, procedures, and processes between the client's incident response team are paramount to ensure time efficiency during critical cyber incidents. This presents a two-fold communication challenge. On the one hand, the in-house response team carries domain-specific knowledge about the OT installations (e.g., maintenance, response time, detecting fault origins). On the other hand, the SOC is proficient in detecting and handling security incidents. In addition, the response team may not necessarily have sufficient experience in handling cyber incidents, and the SOC might carry experience managing incidents, albeit from pure IT systems. The distinct but complementary knowledge base poses a challenge in possessing the same level of understanding, expectations, and coordination during critical events. However, it provides an opportunity to complement each other's tasks without performing the same work twice.

This paper briefly introduces the related work in the area and presents a research design based on qualitative studies. The study emphasizes three perspectives: (1) the client's incident response team, (2) the SOC, and (3) the interaction and collaboration between them. The insights contribute to answering the following research questions:

(1) What do the SOC and client's incident response team expect from each other in terms of knowledge and experience?
(2) How is the interaction and collaboration between the SOC and the response team during a cyber incident?
(3) How can we ensure that the SOC and the client's response team communicate and cooperate effectively?

2 RELATED WORK

Security Operations Centers (SOCs) are commonly used by companies to safeguard their IT infrastructure. Various approaches exist for operating a SOC, including outsourcing to a Managed Security Service Provider (MSSP), or managing an in-house SOC. A hybrid approach is becoming more popular, where continuous monitoring services are outsourced, but the incident response team is maintained internally [9]. Additionally, SOCs can be categorized as cloud-based or on-premise, with the former being more easily deployable and the latter requiring a more thorough onboarding process.

Onwubiko et al. (2019) [9] highlight the challenges and key factors of inefficient SOCs, primarily from an IT perspective. They stress that clear role specifications, policies, procedures, and tailored processes for each customer are important factors for determining efficiency. Clients should also develop unique competencies and

womENcourage '23, September 22–23, 2023, Trondheim, NO

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

skill sets to accommodate the increasing complexity of multiple digital connections. This is especially relevant in OT domains, which require multidisciplinary knowledge and experience.

A report by Dragos (2017) [4] identifies the main differences between IT and OT SOCs, such as the need for increased collaboration and experience sharing among security personnel and operations teams to eliminate culture clash, and the lack of insights into the threat landscape for Industrial Control Systems. Although the data on ICS cyberattacks is less than that of the IT domain, the increasing integration of OT and IT makes IT vulnerabilities more relevant for the OT domain. The relatively static communication environment between Programmable Logic Controllers (PLCs) in lower layers of the Purdue model provides an advantage for OT SOCs to set whitelisted patterns for ICS.

Dimitrov et al. (2019) [3] propose a shared OT SOC, where multiple ICS environments are connected to duplicate the same services for similar OT systems, enabling security monitoring with lower costs. They argue that aggregating experience into one entity can combat the lack of cybersecurity knowledge, resulting in earlier detection of cyberattacks. However, this approach is challenging due to the need for the SOC to adapt to each installation and the complex OT architecture, which complicates data extraction. Field tools also lack the computational power and memory to adopt forensic tools.

Jacq et al. (2018) [6] report similar challenges in developing a testbed for maritime SOC. Their findings emphasize critical and unique requirements for the naval SOC operation, using the "People, Process, and Technology" perspective. System patching and verifying the patch on a combination of legacy and new systems is time-consuming. Using satellite links poses bandwidth constraints that prioritize the vessel's and crew's safety over transmitting data to the SOC.

Overall, the related work highlights the challenges of the complex infrastructure, clear procedures, and specialized knowledge required to provide adequate monitoring services for SOCs in the OT domain. A qualitative study could further strengthen the literature findings and set the groundwork for possible solutions.

3 METHODOLOGY

This study aims to assess the preparedness of SOCs to detect and respond to operational technology (OT) cyberattacks, both in tabletop and full-scale exercises. The research design involves conducting observational studies of current SOC operations, with a particular focus on examining organizational practices and incident response. To supplement these observations, semi-structured interviews will be conducted with key personnel to investigate the existence of incident response procedures and role definitions, and to what extent these are known by the IT/OT response team. This includes IT/OT security incident response plans and IT/OT control rooms and networks. In addition, participants will have the opportunity to discuss their aims, motivation, and initial expectations prior to the preparedness exercises taking place, in order to fully take advantage of the observational study [1].

The exploratory study adopts an ecological study design to assess how the SOC and in-house incident response teams affect each other during a cyber incident. The study aims to assess the entire

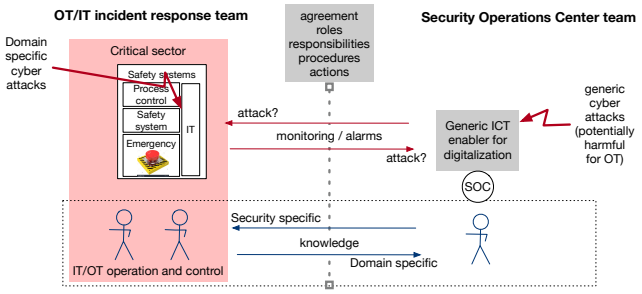

Figure 1: Technical and non-technical interactions between IT/OT and SOC to handle cyberattacks on OT systems.

population (i.e., SOC and client) during a particular time (i.e., OT cyber-incident response) [5]. Fig. 1 illustrates the importance of close collaboration and coordination between the two stakeholders. The study will investigate this further through joint cybersecurity tabletop or full-scale exercises to understand how the teams collaborate and coordinate their tasks with each other.

ACKNOWLEDGMENTS

This research was funded by the Norwegian Research Council through the Cybersecurity Barrier Management project, grant number 326717.

REFERENCES

[1] Maria Bartnes and Nils Brede Moe. 2017. Challenges in IT security preparedness exercises: A case study. *Computers and Security* 67 (2017), 280–290. http://dx.doi.org/10.1016/j.cose.2016.11.017

[2] Mark Bristow. 2021. *A SANS 2021 Survey: OT/ICS Cybersecurity.* Technical Report. SANS Institute. 1–23 pages.

[3] Willian Dimitrov and Svetlana Syarova. 2019. Analysis of the Functionalities of a Shared ICS Security Operations Center. In *Proceedings of the 2019 IEEE Conference on Big Data, Knowledge and Control Systems Engineering (BdKCSE) Analysis.* IEEE, 1–6. https://doi.org/10.1109/BdKCSE48644.2019.9010607

[4] Dragos. 2017. *Insights into Building an Industrial Control System Security Operations Center.* Technical Report. Dragos Inc. 12 pages.

[5] Thomas W. Edgar and David O. Manz. 2017. Exploratory Study. In *Research Methods for Cyber Security.* Elsevier, Chapter 4, 95–130. https://doi.org/10.1016/B978-0-12-805349-2.00003-0

[6] Olivier Jacq, Xavier Boudvin, David Brosset, Yvon Kermarrec, and Jacques Simonin. 2018. Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre. In *2018 2nd Cyber Security in Networking Conference (CSNet).* IEEE, 1–9.

[7] Toshio Miyachi and Tsutomu Yamada. 2014. Current issues and challenges on cyber security for industrial automation and control systems. *Proceedings of the SICE Annual Conference* (2014), 821–826. https://doi.org/10.1109/SICE.2014.6935227

[8] Tor Onshus, Lars Bodsberg, Stein Hauge, Martin Gilje Jaatun, Mary Ann Lundteigen, Thor Myklebust, Maria Vatshaug Ottermo, Stig Petersen, and Egil Wille. 2022. Security and Independence of Process Safety and Control Systems in the Petroleum Industry. *Journal of Cybersecurity and Privacy* 2, 1 (Feb. 2022), 20–41. https://doi.org/10.3390/jcp2010003

[9] Cyril Onwubiko and Karim Ouazzane. 2019. Challenges towards Building an effective Cyber Security Operations Centre. *International Journal on Cyber Situational Awareness* 4, 1 (2019), 11–39. https://doi.org/10.22619/ijcsa.2019.100124