Blue Team Fundamentals: Roles and Tools in a Security Operations Center

Jenny Hofbauer *, Kevin Mayer †
CARISSMA Institute for Electric, Connected, and Secure Mobility
Technical University Ingolstadt
Germany
e-mail: *jeh7703@thi.de, †kevin.mayer@carissma.eu

***Abstract*—The evolution from low-impact malicious code in the mid-70s to current Denial-of-Service (DoS) attacks, widespread malware campaigns, and Advanced Persistent Threats (APTs) shaped the furtherance of Information Technology (IT) security services that Security Operations Centers (SOCs) provide to protect against cyberattacks. Despite the ever-growing importance of SOCs, there is little academic and fundamental research. Terminology and the associated definitions are highly influenced by companies developing proprietary software and training and are mostly not standardized. This paper closes part of the gap and provides a suitable research base regarding people and technologies. For this purpose, literature research was conducted using academic literature and industry data, such as advertising material, company white papers, and employment advertisements. A survey with 24 experts in various areas of IT security was conducted to validate and expand the identified roles and tools, allowing the creation of an overview of roles and tools currently utilized in the industry. These can be seen as building blocks, whereas the company's individual needs determine its presence, capabilities, and association within SOCs. The percentage of participants who classified the defined roles and tools as part of SOCs is detailed. The survey furthermore captured the affiliation of roles between SOCs and Computer Emergency Response Teams (CERT) or Computer Security Incident Response Teams (CSIRT), often seen as specialized sub-capabilities that work on data SOCs provide. The common terminology creates a uniform basis for further research and more efficient communication and defines roles and technologies in SOCs that can be used to identify possible gaps.**

***Keywords*-Security Operations Center; SOC; SOC Roles; SOC Tools; Blue Team.**

I. Introduction

In its annual report *The State of IT Security in Germany* [1], the Federal Office for Information Security describes the current threat situation in Information Technology (IT) security as tense to critical with the highest level of cybercrime ever recorded. Cyberattacks' quantitative and qualitative development has grown in recent years, making cybersecurity increasingly crucial for businesses. Security Operations Centers (SOCs) utilize people, technologies, and processes to protect against cyberattacks [2]. Software tools and knowledge needed to operate efficient SOCs are primarily proprietary. There is little public and objective information, standardization, and fundamental research, not only because most cybersecurity software is not freely accessible but also because of paid training courses. This work closes part of the gap by providing a suitable research base of the industry's current SOC roles and tools. It compiles an overview of standardized terminology for enterprise IT SOC roles and tools and defines their capabilities. First, the definition of SOCs in the context of this paper is established in Section II. Based on this definition, Section III highlights already conducted SOC research and places this paper within the context. Section IV details the research methodology of this paper, which is based on literature research and surveys with experts. The developed SOC roles and tools are listed and provided with context in Sections V and VI. Section VII gives insights and reasoning behind some of the classifications, while the final Section VIII concludes the results of the research.

II. Definition of a Security Operations Center

The systematic study by Vielberth et al. [2] defined SOCs as an IT security service provider that protects against cybersecurity threats and information loss. It identifies, detects, and mitigates cyberthreats through people, processes, and technologies. As highlighted by Hofbauer et al. [3], there is no standardized definition of enterprise IT SOCs. Affiliations and tasks differ between individual companies and sub-organizations. Functions traditionally assigned to Computer Emergency Response Teams (CERT) or Computer Security Incident Response Teams (CSIRT) are also considered in this paper since companies often do not have dedicated resources or responsibilities overlap. All aspects of product security are excluded. This paper lists roles and tools that implement the primary SOC capabilities defined by [3]:

- Change and Asset Management
- Threat Intelligence Management
- Vulnerability Management
- Data Collection and Management
- Security Event Management
- Incident and Crisis Management
- Forensic and Investigation of Security Incidents
- Compliance Management and Reporting
- Recommendations and Advice
- Security Awareness Training

III. Related Work

To the best of our knowledge, no research paper addresses the terminology and definition of roles and tools in SOCs in detail. Olt [4] published a rough overview of SOC roles and their interactions, which has been used as the basis of numerous other papers [2], [5], [6]. These include a paper published in 2020 by Vielbert et al. [2] that uses a holistic approach to define the state of the art of SOCs and open challenges, especially in the collaboration between people and technology. The individual aspects of the paper are examined in greater detail in the

books from Knerler et al. [7] and Nathans [8]. Nathans' work from 2014 includes a detailed list of SOC tools divided into organizational, operational, and support infrastructure, with the umbrella terms still used similarly in current general SOC works [5], [9]–[13]. Many works deal with individual tools or roles in SOCs, but do not provide a general overview. Since a large part of the further development of SOCs is done by companies, product portfolios and information from SOC as a service providers show the current state of SOC roles and tools in the industry. However, such articles are primarily designed to sell software solutions or services and do not correspond to scientific standards.

IV. Research Methodology

The research methodology for establishing roles, responsibilities, and tools in a traditional enterprise IT SOC is divided into two phases. In the first phase, a detailed literature review was carried out. Since the literature is limited, the findings were expanded and validated through a survey in the second phase. People and technologies considered part of the SOC by at least one expert were included. Quick and Hall [14] suggested an appropriate sample size of 4-50 participants in their study about qualitative research, a range we adhered to. The experts were selected based on their involvement in previous SOC-related research projects and peer-reviewed publications or needed to be at least fairly confident in one of the areas of IT security. During the selection, we strived to achieve diversity across industry (Figure 1), age (Figure 2) and experience (Figure 3). The survey was conducted over two months via the survey platform SoSci [15]. Each participant was presented with an overview of roles, tools and their descriptions in SOCs established through the literature research. They were given the option to confirm, deny, or not answer whether every role and tool belonged in SOCs and encouraged to provide additional comments on their choice and suggest any missing assets. This approach ensured transparency and allowed for a comprehensive understanding of the participants' perspectives. Unfinished surveys or ones that did not meet the requirements of an expert were not considered. Twenty-four valid interviews were conducted; the raw data from the interview can be found at [16].

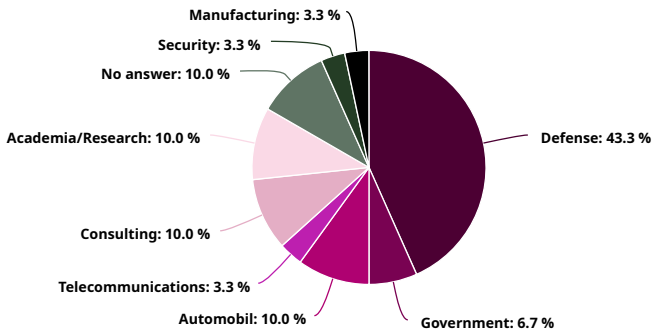

Figure 1. SOC Survey Participant Industry.

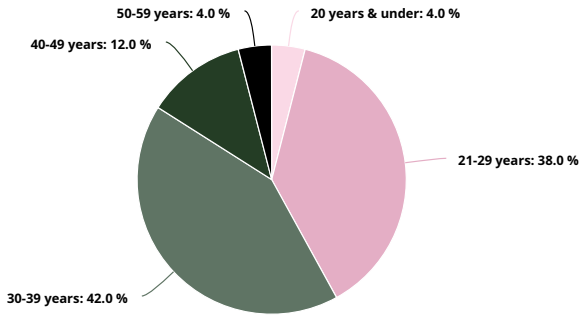

Figure 2. SOC Survey Participant Age.

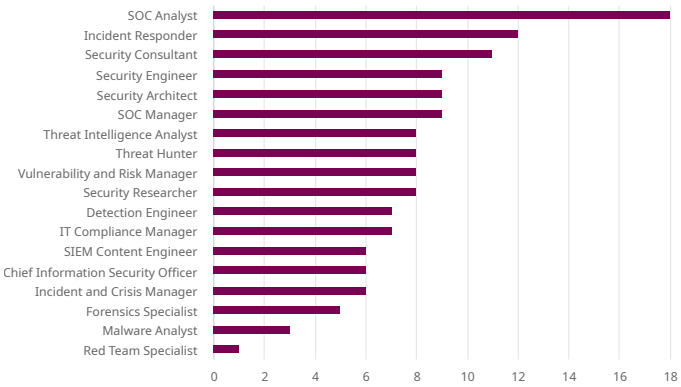

Figure 3. SOC Survey Participant Experience.

V. Roles in an Enterprise SOC

The following roles and descriptions were compiled from academic literature [2], [4], [7], [9], [12], [17]–[21], SOC provider advertising material [22]–[25] and appropriate job listings from employment website marked with the search terms "Security Operations Center", "Computer Emergency Response Team", "Computer Security Incident Response Team", "Blue Team" and excluded any listings related to product security and penetration testing. Due to the limited academic literature and the widespread implementation of SOCs in the industry, advertising material was assessed for reliability and is considered equivalent to reputable sources. Company-specific role titles were not considered. During the literature research and the interviews, other terms for roles with the insert "Chief" were occasionally found; this is primarily used in American companies where the word "Chief" indicates seniority. Roles and their descriptions were grouped into technical (Table I), management (Table II), and consulting (Table III). The literature research was expanded and validated by interviews described in Section IV.

A. Technical SOC Roles

This section examines the technical roles in SOCs. Table I lists the role name and description. Figure 4 shows the percentage of survey participants who consider each role part of the SOC. Various literature works [2], [17], [19], [22] refers

to a tier 1 SOC analyst as a triage or alert specialist, tier 2 as an incident responder, and tier 3 as a threat hunter. The roles established in this paper do not follow those labels. It was noted several times in the interviews that the division of SOC analysts into tiers is only theoretical and not implemented in practice. The forensics analyst was generally attributed to a CERT/CSIRT and an often outsourced role since continuous practice is needed that a single company environment can rarely provide. Through the increase of modern tools like Endpoint Detection and Response (EDR) and the need for fast response, forensic analysts are commonly restricted to disk forensics and finding legal evidence. The Security Information and Event Management (SIEM) content engineer is often not a specifically dedicated role but rather done by the SOC analyst or architect. Since many companies are moving away from the single platform strategy of only using a SIEM, the role will be called security tool content engineer in this paper. The incident responder is also typically attributed to a CERT/CSIRT. The role overlaps with a forensic expert or SOC analyst on a technical basis; they are usually the interface between technical roles and the supporting teams, such as server operations and management. Based on the literature research, the red team specialist was initially categorized as a technical role but was attributed to the consulting roles due to survey comments.

TABLE I. TECHNICAL SOC ROLES

Role	Description
SOC Analyst	Review and triage real-time alarms and alerts and determines if they are a false or true positive. Conduct in-depth analyses of security incidents, contain them, and introduce recovery mechanisms. Perform vulnerability assessments and penetration testing to proactively identify and treat threats and vulnerabilities.
Threat Intelligence Analyst	Collect, analyze, produce, and share cyberthreat intelligence.
Malware Analyst	Analyze malware functionality to collect necessary information for detection and incident response.
Forensics Specialist	Investigate incidents to collect legally sound evidence.
Detection Engineer	Design, test, and maintain threat detection logic.
Security Engineer	Develop, integrate, and maintain tools the Security Operations Center uses.
Security Tool Content Engineer	Manage, parse, correlate, and enrich logs and data for the security tools.
Threat Hunter	Proactively search the network and infrastructure to detect unknown threats.
Incident Responder	Discover intrusion artifacts to mitigate and provide technical support to resolve cyberincidents and act as an interface between involved parties.

B. Management SOC Roles

All established management roles are listed in Table II with the corresponding Figure 5 visualizing the belonging to a SOC. Regarding the management roles, the IT compliance manager can be seen as part of SOCs or the company since aspects such as data protection are relevant outside of IT security. A security incident and crisis manager is usually part of a CERT/CSIRT and has a corresponding non-security, general incident, and crisis manager role in the organization. The vulnerability and risk manager is located in the CERT/CSIRT and can be split into separate cybersecurity-only vulnerability and risk manager roles. The cybersecurity awareness officer was added as a separate role since survey comments stated that it is common practice in larger companies.

TABLE II. MANAGEMENT SOC ROLES

Role	Description
Chief Information Security Officer	Define strategies, policies, and goals for the security operations of the entire company.
SOC Manager	Manage and supervise the Security Operations Center team's daily operations and tactical direction.
IT Compliance Manager	Organize compliance aspects such as data protection and information security.
Security Incident and Crisis Manager	Coordinate all aspects regarding security incident and crisis response.
Vulnerability and Risk Manager	Identify, assess, manage, prioritize, contextualize, and prevent vulnerabilities.
Cybersecurity Awareness Officer	Understand and triage human risks and take measurements to mitigate those behaviors.

C. Consulting SOC Roles

The following roles listed in Table III are often located outside SOCs or entirely outsourced and only provide services for SOCs. Figure 6 shows the percentage of survey participants who consider each role part of the SOC.

TABLE III. CONSULTING ROLES

Role	Description
Security Architect	Research and design a robust security infrastructure.
Red Team Specialist	Attack systems to identify vulnerabilities and possible evasions for cybersecurity defenses.
Security Consultant and External Personnel	Provide independent audits and consulting in specific areas, for instance, cloud or artificial intelligence security consulting or expertise from a security tool manufacturer.

VI. TOOLS IN AN ENTERPRISE SOC

Technologies are the second central pillar, including tools that SOCs do not directly manage but leverage functionalities or data. Few academic publications exist in this area [5], [8]–[13], which is why advertising material from companies [26]–[37] was primarily used. The researched tools were categorized with the help of the infrastructure chapter of Nathans' work [8], the primary SOC capabilities, and the structure of cybersecurity company websites. Table IV and Figure 7 highlight the tools responsible for the collection and management of data. Every tool involved in the organization and analysis of incidents is depicted in Table V and Figure 8. Security solutions that protect the infrastructure are separated into their area of application. This includes the security of the network (Table VI and Figure 9), endpoints (Table VII and Figure 10), and the combination of both labeled infrastructure (Table VIII and Figure 11). Table IX and Figure 12 highlight security applications running on servers and endpoints. Tools used to manage the security of a company are depicted in Table X and Figure 13. Lastly, tools that are not directly managed but influenced or leveraged by SOCs are combined under the categories of identity attestation

(Table XI and Figure 14) and security awareness (Table XII and Figure 15).

TABLE IV. DATA COLLECTION AND MANAGEMENT

Tool	Description
Security Information and Event Management (SIEM)	Aggregates event data from infrastructure and endpoints, correlates events, and compares them to behavior rules to detect potential threats.
Threat Intelligence Platform (TIP)	Platform to collect, aggregate, enrich, and organize threat intelligence.
Vulnerability Scanner, Penetration Testing Tools, and Breach and Attack Simulation (BAS)	Scans infrastructure and endpoints for vulnerabilities and misconfigurations.
Threat Hunting Tools	Enables the proactive search for cyberthreats that have bypassed established security solutions.
Log Collection and Management Tool	Collects and manages log data not limited to security-relevant data.
Honeypot	A system that is purposefully insecure to gather threat intelligence, detect attackers, and deflect from real systems.

TABLE V. INCIDENT ANALYSIS

Tool	Description
Malware Analysis Sandbox / Platform	Dynamic or static analysis and execution of malware in a secure environment.
Digital Forensics and Incident Response Tools (DFIR)	Hardware and software tools for recovering and preserving digital evidence and attacker methodologies to contain, remediate, and testify in case of an incident.
Security Orchestration, Automation and Response (SOAR)	Automates the contextualisation of security-relevant data and processing of security events/incidents.

TABLE VI. NETWORK SECURITY

Tool	Description
Firewall	Blocks traffic to prevent unauthorized access to and from networks. The SOC usually leverages the tool's logs and does not manage/maintain it.
Network Access Control (NAC)	Restricts unauthorized hardware and users from accessing networks. The SOC usually leverages the tool's logs and does not manage/maintain it.
Network-Based Intrusion Detection System (NIDS)	Monitors connections, data traffic, and activity on the network for malicious activity and reports it.

TABLE VII. ENDPOINT SECURITY

Tool	Description
Endpoint Detection and Response (EDR)	Modern term for a Host-Based Intrusion Detection System that records activities and monitors for suspicious behavior on endpoints.
Host-Based Intrusion Detection System (IDS)	Monitors connections, data traffic, and activity on endpoints for suspicious behavior and reports it.
Intrusion Prevention System (IPS)	Uses mitigation measures to contain suspicious behavior detected by an IDS.
User and Entity Behavior Analytics (UEBA)	Uses various data streams, such as logs and packet captures, to identify anomalies in the behavior of users and non-human entities.
Virus Scanner	Automatically detects and quarantines malware. The SOC usually leverages the tool's logs and does not manage/maintain it.

TABLE VIII. INFRASTRUCTURE SECURITY

Tool	Description
Extended Detection and Response (XDR)	Extension of an EDR system that adds vendor-specific capabilities.

TABLE IX. APPLICATION SECURITY

Tool	Description
Email Security and Protection	Protection and control of email accounts as well as incoming and outgoing email communication. The SOC usually leverages the tool's logs and does not manage/maintain it.
Web Application Firewall (WAF)	A firewall specifically designed to filter and monitor web traffic. The SOC usually leverages the tool's logs and does not manage/maintain it.
Runtime Application Self-Protection	Detects and blocks attacks on software in real-time with insight from inside the running software.

TABLE X. MANAGEMENT PLATFORM

Tool	Description
Asset Management and Discovery Platform	Network scanner that detects hardware and software in the network and extracts and stores detailed information about the asset.
Device Configuration, Update, and Patch Management Platform	Platform to organize and perform device configuration, updates, and patches. The SOC usually leverages the tool's logs and does not manage/maintain it.
Ticketing System	Platform to create and manage work tasks between different people and teams.
Change Management Platform	Supports the planning, implementation, authorization, and non-repudiation of security-relevant organizational changes, often integrated with the general IT or business.
Vulnerability Management Platform	Platform to keep track of identified vulnerabilities and corresponding mitigation measures.
Cybersecurity Risk Management Software	Platform to keep track of identified risks and corresponding mitigation measures.
Knowledge Management Platform	Used to document, manage, and share cybersecurity knowledge within the organization.
Case and Incident Management Platform	Platform for organizing and managing security cases, incidents, and associated context information.
Supplier Management Platform	Consolidates supplier data to have a single knowledge point in case of a supplier alarm.
Compliance Scanner	Monitors if system configurations are compliant with security policies.
Information Security Management System (ISMS)	Platform to establish, improve, and monitor policies and procedures to manage information security.

The security awareness and identity attestation tools documented in Table XI and XII are the responsibility of the information security officer. Parts of the execution, use of log data, and administration can fall under the responsibility of SOCs.

TABLE XI. IDENTITY ATTESTATION

Tool	Description
Public Key Infrastructure (PKI)	Creates, revokes, manages, and distributes a digital certificate and corresponds to the owner.
Identity and Access Management System	Administration, maintenance, and authorization management of user accounts and resources in a network.
Password Manager	A program that stores and manages usernames and passwords securely.

TABLE XII. SECURITY AWARENESS

Tool	Description
Bug Bounty Platform	Allows users and external security researchers to report identified vulnerabilities for a reward.
Security Awareness Platform	Platform to enhance cybersecurity user awareness.

VII. HIGHLIGHTS

This section captures highlights, trends, and reasoning behind some classifications based on the survey comments. Survey takers suggested specialized roles like cloud or artificial intelligence security analysts. The paper did not include these since they can be categorized as security architects or consultants. This highlights the importance of specializations, as no definitive distinction between roles often exists in the industry. A shortage of skilled workers forces SOC employees to take on several roles simultaneously, or individual capabilities are not needed or outsourced. Automation is frequently utilized to counteract the shortage of workers and to free up capacity for other activities. Moreover, job titles can differ between countries or even individual industry sectors. Regarding tools, their capabilities depend heavily on the manufacturer partly due to the increase of specialized solutions replacing the previously predominant single-platform SIEM approach.

VIII. CONCLUSION

SOCs are as flexible as the cyberattacks they protect against, adapting to the company's or industry's requirements. The industry mimics this and tries to stand out from the competition through convoluted marketing that promises that their newly coined terminology solves cutting-edge security problems. Fostering a need for standardized terminology and definitions to allow for objective comparison and better communication in security operations. Based on literature and expert interviews, our research defines the roles and tools that can be part of individual SOCs. While our listing is not exhaustive, it provides an overview and standardized vocabulary of the most common roles and tools used in the industry. Even though the SOC field is dominated by the industry, academic research, as a critical and neutral observer, can add significant value. Further research could include the establishment of standardized SOC frameworks for areas like SOC processes.

ACKNOWLEDGEMENTS

We want to extend a special thank you to all survey participants for their input and insights, which made this paper possible. This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement No 101069748.

REFERENCES

[1] Federal Office for Information Security, "The State of IT Security in Germany 2023", 21/11/2023, [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.html?nn=1021082.

[2] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges", *IEEE Access*, vol. 8, pp. 227 756–227 779, 2020. DOI: 10.1109/ACCESS.2020.3045514.

[3] J. Hofbauer, K. Mayer, and H.-J. Hof, "From SOC to VSOC: Transferring Key Requirements for Efficient Vehicle Security Operations", Oct. 2023. DOI: 10.13154/294-10389.

[4] C. Olt, "Establishing Security Operation Centers for Connected Cars", *ATZelectronics worldwide*, vol. 14, no. 5, pp. 40–43, 2019. DOI: 10.1007/s38314-019-0050-4.

[5] A. Reisser, M. Vielberth, S. Fohringer, and G. Pernul, "Security Operations Center Roles and Skills: A Comparison of Theory and Practice", in *Data and Applications Security and Privacy XXXVI: 36th Annual IFIP WG 11.3 Conference, DBSec 2022, Newark, NJ, USA, July 18–20, 2022, Proceedings*, Newark, NJ, USA: Springer-Verlag, 2022, pp. 316–327, ISBN: 978-3-031-10683-5. DOI: 10.1007/978-3-031-10684-2_18.

[6] C. DeCusatis, R. Cannistra, A. Labouseur, and M. Johnson, "Design and Implementation of a Research and Education Cybersecurity Operations Center", in Jun. 2019, pp. 287–310, ISBN: 978-3-030-16836-0. DOI: 10.1007/978-3-030-16837-7_13.

[7] K. Knerler, I. Parker, and C. Zimmerman, *11 Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, 2022, ISBN: 979-8-9856450-4-0.

[8] D. Nathans, *Designing and Building Security Operations Center*. Waltham, MA: Syngress, 2014, ISBN: 9780128010969.

[9] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A Tale of Three Security Operation Centers", in *SIW '14 : proceedings of the 2014 ACM Workshop on Security Information Workers : November 7, 2014, Scottsdale, Arizona, USA*, R. Biddle, Ed., ACM, 2014, pp. 43–50, ISBN: 9781450331524. DOI: 10.1145/2663887.2663904.

[10] P. Jacobs, A. Arnab, and B. Irwin, "Classification of Security Operation Centers", in *2013 Information Security for South Africa*, 2013, pp. 1–7. DOI: 10.1109/ISSA.2013.6641054.

[11] N. Miloslavskaya, "Security Operations Centers for Information Security Incident Management", in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016, pp. 131–136. DOI: 10.1109/FiCloud.2016.26.

[12] S. Schinagl, K. Schoon, and R. Paans, "A Framework for Designing a Security Operations Centre (SOC)", in *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 2253–2262. DOI: 10.1109/HICSS.2015.270.

[13] J. Hajny *et al.*, "Framework, Tools and Good Practices for Cybersecurity Curricula", *IEEE Access*, vol. 9, pp. 94 723–94 747, 2021. DOI: 10.1109/ACCESS.2021.3093952.

[14] J. Quick and S. Hall, "Part two: Qualitative research", *Journal of Perioperative Practice*, vol. 25, no. 7-8, pp. 129–133, 2015, ISSN: 1750-4589. DOI: 10.1177/1750458915025007-803.

[15] SoSci Survey GmbH, "SoSci Survey – the Solution for Professional Online Questionnaires", 27/05/2024, [Online]. Available: https://www.soscisurvey.de/en/index.

[16] GitHub, "Survey-data/blue-team-fundamentals at main · securityinmobility/survey-data", 31/05/2024, [Online]. Available: https://github.com/securityinmobility/survey-data/tree/main/blue-team-fundamentals.

[17] M. Shutock and G. Dietrich, "Security Operations Centers: A Holistic View on Problems and Solutions", in *Proceedings of the 55th Hawaii International Conference on System Sciences*, T. Bui, Ed., ser. Proceedings of the Annual Hawaii International Conference on System Sciences, Hawaii International Conference on System Sciences, 2022, pp. 7555–7564. DOI: 10.24251/HICSS.2022.907.

[18] D. Crémilleux, C. Bidan, F. Majorczyk, and N. Prigent, "Enhancing Collaboration Between Security Analysts in Security Operations Centers", in *Risks and Security of Internet and*

Systems. Springer Berlin Heidelberg, Jan. 2019, pp. 136–142, ISBN: 978-3-030-12142-6. DOI: 10.1007/978-3-030-12143-3_12.

[19] F. Kokulu *et al.*, "Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues", in *CCS'19*, Association for Computing Machinery, Nov. 2019, pp. 1955–1970, ISBN: 978-1-4503-6747-9. DOI: 10.1145/3319535.3354239.

[20] B. Hámornik and C. Krasznay, "A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers", D. Nicholson, Ed., ser. Advances in Intelligent Systems and Computing, vol. 593, Springer, Jul. 2018, pp. 224–236, ISBN: 978-3-319-60584-5. DOI: 10.1007/978-3-319-60585-2_21.

[21] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Towards a Framework for Measuring the Performance of a Security Operations Center Analyst", in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2020, pp. 1–8. DOI: 10.1109/CyberSecurity49315.2020.9138872.

[22] Palo Alto Networks, "Security Operations Center (SOC) Roles and Responsibilities", 13/11/2023, [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities.

[23] Cybersecurity and Infrastructure Security Agency CISA, "Cyber Defense Incident Responder", 13/11/2023, [Online]. Available: https://www.cisa.gov/careers/work-rolescyber-defense-incident-responder.

[24] SANS Institute, "Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey", 13/11/2023, [Online]. Available: https://www.sans.org/white-papers/39060/.

[25] Indeed, "12 Types of Cybersecurity Roles (With Duties and Salaries)", 13/11/2023, [Online]. Available: https://www.indeed.com/career-advice/finding-a-job/types-of-cyber-security-roles.

[26] Splunk, "Splunk Products", 22/05/2024, [Online]. Available: https://www.splunk.com/en_us/products.html.

[27] Mandiant, "Threat Intelligence Solutions | Cyber Security Services & Training", Tue, 09/07/2021, [Online]. Available: https://www.mandiant.com/.

[28] Proofpoint, "2023 Human Factor Report: Analyzing the Cyber Attack Chain", 2023, [Online]. Available: https://www.proofpoint.com/.

[29] Kaspersky, "Kaspersky Security for Business Portfolio", 27/05/2024, [Online]. Available: https://www.kaspersky.com/small-to-medium-business-security/resources/products/kaspersky-security-for-business-portfolio.

[30] Fortinet, "Global Leader of Cybersecurity Solutions and Services", 27/05/2024, [Online]. Available: https://www.fortinet.com/.

[31] Cloudflare, "Cloudflare Product Portfolio", 27/05/2024, [Online]. Available: https://www.cloudflare.com/cloudflare-product-portfolio/.

[32] CrowdStrike, "CrowdStrike: Stop breaches. Drive business", 13/05/2024, [Online]. Available: https://www.crowdstrike.com/en-us/.

[33] Palo Alto Networks, "Products a-z", 22/05/2024, [Online]. Available: https://www.paloaltonetworks.com/products/products-a-z.

[34] Trend Micro, "Products", 27/05/2024, [Online]. Available: https://www.trendmicro.com/en_us/business/products.html.

[35] Darktrace, "AI Cyber Security Solutions", 27/05/2024, [Online]. Available: https://de.darktrace.com/products.

[36] SentinelOne DE, "The Enterprise Security AI Platform | Securing Endpoint, Cloud, Identity, and Data", 7/05/2024, [Online]. Available: https://de.sentinelone.com/.

[37] CyberArk, "Product Datasheets", 27/05/2024, [Online]. Available: https://www.cyberark.com/resources/product-datasheets.

APPENDIX

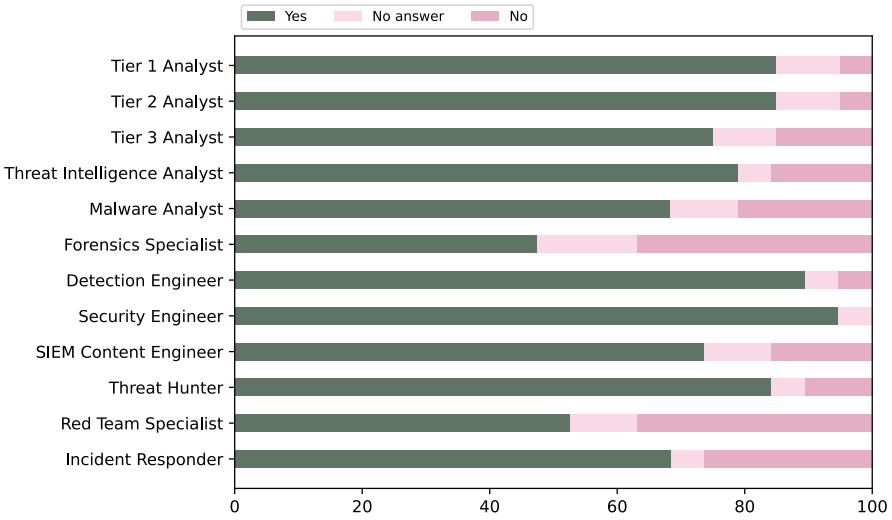

FIGURE 4. CLASSIFICATION OF TECHNICAL SOC ROLES.

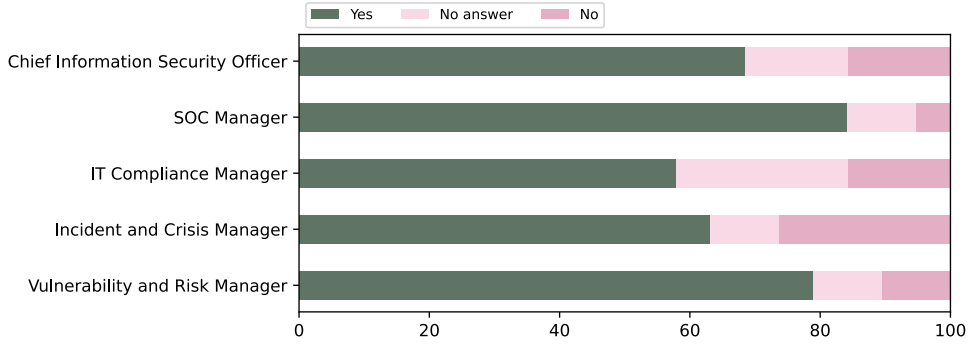

FIGURE 5. CLASSIFICATION OF MANAGEMENT SOC ROLES.

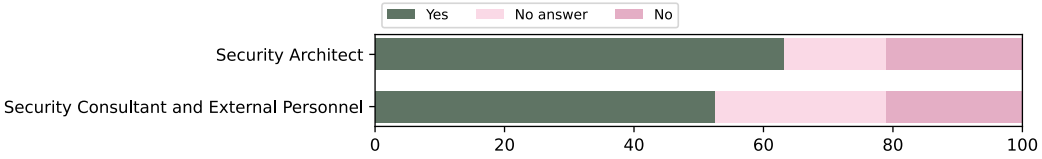

FIGURE 6. CLASSIFICATION OF CONSULTING SOC ROLES.

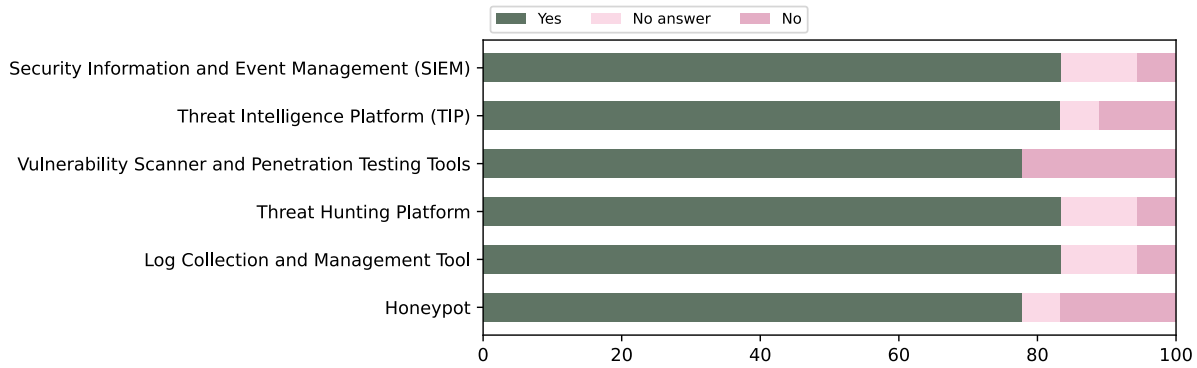

FIGURE 7. CLASSIFICATION OF DATA COLLECTION AND MANAGEMENT SOC TOOLS.

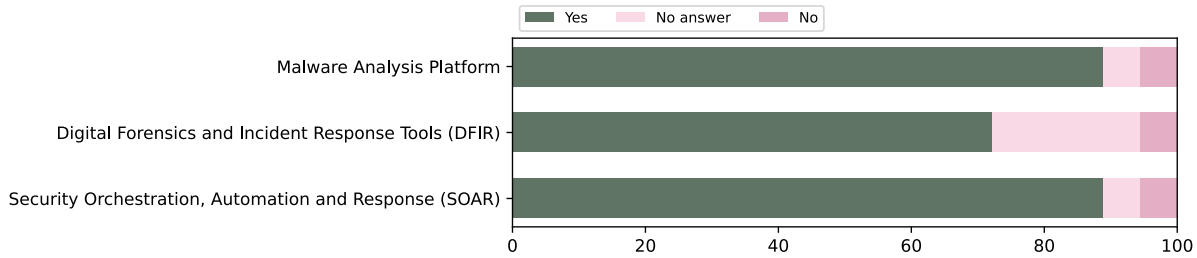

FIGURE 8. CLASSIFICATION OF INCIDENT ANALYSIS SOC TOOLS.

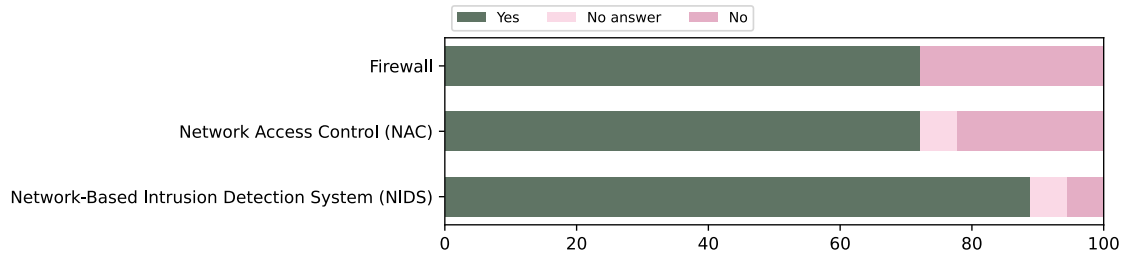

FIGURE 9. CLASSIFICATION OF NETWORK SECURITY SOC TOOLS.

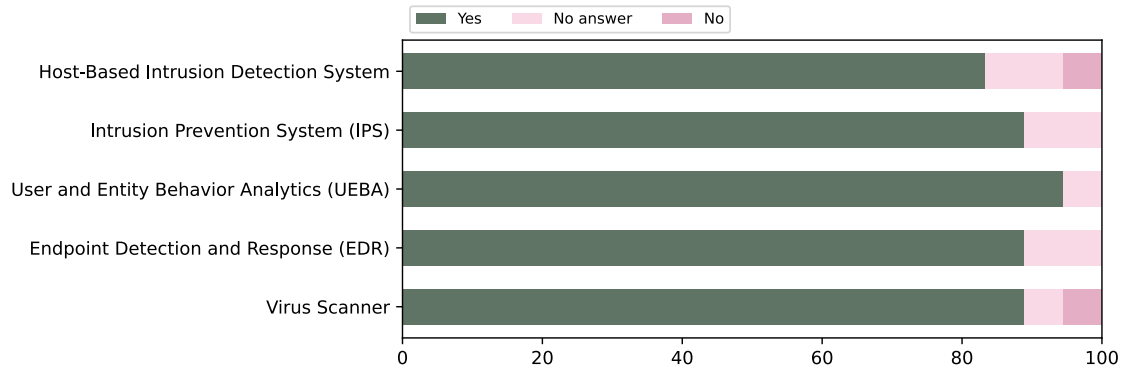

FIGURE 10. CLASSIFICATION OF ENDPOINT SECURITY SOC TOOLS.

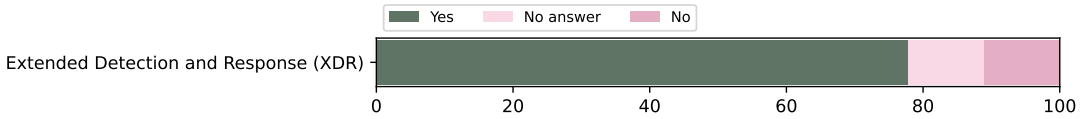

FIGURE 11. CLASSIFICATION OF INFRASTRUCTURE SECURITY SOC TOOLS.

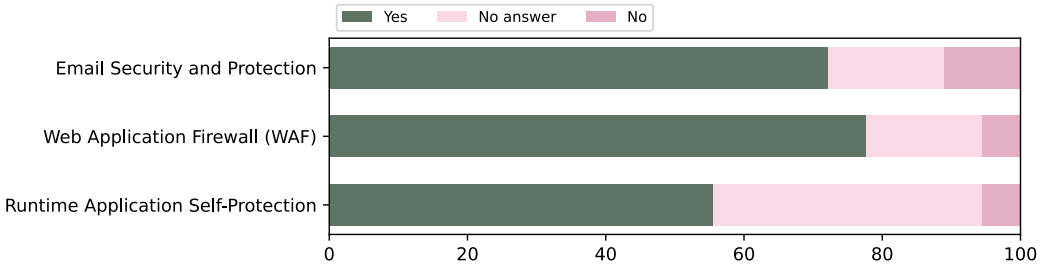

FIGURE 12. CLASSIFICATION OF APPLICATION SECURITY SOC TOOLS.

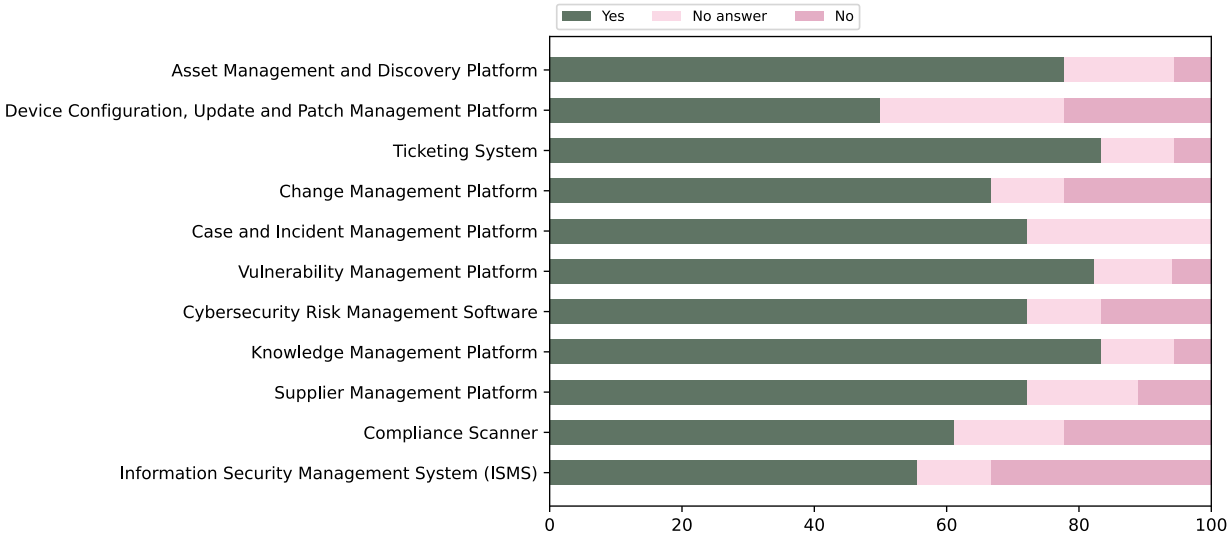

FIGURE 13. CLASSIFICATION OF MANAGEMENT PLATFORM SOC TOOLS.

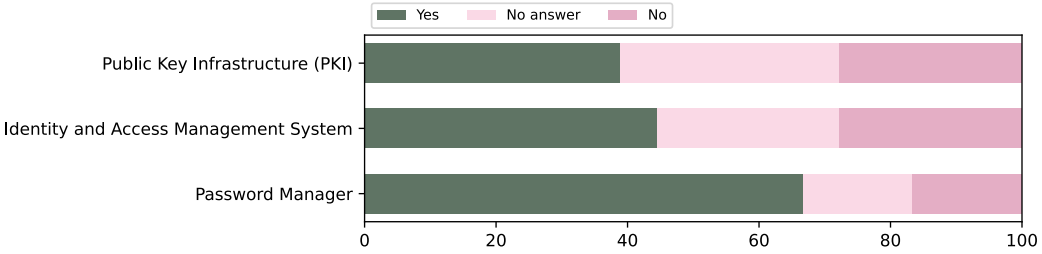

FIGURE 14. CLASSIFICATION OF IDENTITY ATTESTATION SOC TOOLS.

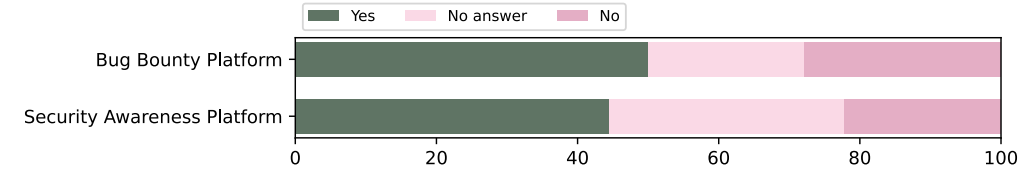

FIGURE 15. CLASSIFICATION OF SECURITY AWARENESS SOC TOOLS.