IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Security Operations Center: A Systematic Study and Open Challenges

MANFRED VIELBERTH, FABIAN BÖHM, INES FICHTINGER, AND GÜNTHER PERNUL, (Member, IEEE)

Chair of Information Systems, University of Regensburg, 93053 Regensburg, Germany

Corresponding author: Manfred Vielberth (e-mail: manfred.vielberth@ur.de).

ABSTRACT Since the introduction of Security Operations Centers (SOCs) around 15 years ago, their importance has grown significantly, especially over the last five years. This is mainly due to the paramount necessity to prevent major cyber incidents and the resulting adoption of centralized security operations in businesses. Despite their popularity, existing academic work on the topic lacks a generally accepted view and focuses mainly on fragments rather than looking at it holistically. These shortcomings impede further innovation. In this paper, a comprehensive literature survey is conducted to collate different views. The discovered literature is then used to determine the current state-of-the-art of SOCs and derive primary building blocks. Current challenges within a SOC are identified and summarized. A notable shortcoming of academic research is its focus on the human and technological aspects of a SOC while neglecting the connection of these two areas by specific processes (especially by non-technical processes). However, this area is essential for leveraging the full potential of a SOC in the future.

INDEX TERMS Security Management, Security Operations Center, Security Operations, SOC

I. INTRODUCTION

According to a recent report, the average number of security breaches reported by organizations has risen by 11% from 130 in 2017 to 145 incidents in 2018 [1]. Over the last five years, this number has risen by a total of 65%. However, this report only covers detected and reported incidents, and the number of unreported incidents is probably much higher. The total annual cost of any type of cyber-attack is also growing at a steady pace [1]. Unfortunately, many attacks go undetected for a surprisingly long time. The mean time to detect an incident was 196 days in 2018, and it took another 69 days on average to contain the breach [1]. This detection time demonstrates how ineffective companies are at detecting and mitigating cyber-attacks. The reasons for this inefficiency include but are not limited to companies (1) not having an overview of their devices, systems, applications, and networks, (2) not knowing which assets to protect, (3) not knowing which tools to use and how to integrate them with the existing infrastructure, or (4) being overwhelmed by the speed technology and the ever-evolving threat landscape.

Security Operations Centers (SOCs) can provide an overarching solution for detecting and mitigating an attack if implemented correctly. They incorporate a mixture of people, processes, technologies, and governance and compliance, to effectively identify, detect, and mitigate threats, ideally before any damage occurrs. However, there are a few research gaps and challenges associated with SOCs. The biggest issue is the lack of a precise definition of a SOC and its components. For some researchers, a SOC is solely an entity responsible for monitoring the network. For others, it is an organizational unit encompassing all security operations, like incident management and threat intelligence. This lack of consensus hinders companies from deploying efficient SOCs and researchers from further adding to the innovation of SOCs. Therefore, this work's main contribution is to close this research gap by establishing a ground truth for a state-of-the-art SOC. We conduct a structured literature review to identify and subsume the current state-of-the-art.

The remainder of this paper is structured as follows. We identify related work in Section II. We describe the methodology applied to carry out this literature survey throughout Section III. Section IV is the first part of the main contribution of this work. Therein we summarize relevant work for the definition of a SOC and other more general aspects. The second main contribution is formulated in Section V, which distills the building blocks of a SOC from literature. To highlight a roadmap for future research, we identify a series of open challenges within Section VI. We conclude our work

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3045514, IEEE Access

TABLE 1. Review protocol.

Research questions	– What is the state-of-the-art of SOC as seen in research? – Which challenges need to be solved to advance the field?
Dates	January 1st, 1990 - December 31st, 2019
Databases	IEEE Xplore Digital Library[1], ACM Digital Library[2], SpringerLink[3], EBSCO Host[4], Wiley Online Library[5], Web of Science[6], Dimensions[7]
Search criteria	English; Search keywords in Title, Abstract and Keywords
Search keywords	*Security Operation Center* **OR** *Security Operations Center* **OR** *Security Operations Centers* **OR** *Security Operation Centre* **OR** *Security Operations Centre* **OR** *Security Operations Centres*
Search methods	Keyword search, Backward search, Forward search
Inclusion criteria	Addresses SOC in general or part of it; Is available as a full version; Is not superseded by an included paper; Evaluates a paper included by a previous criterion

in Section VII summarizing the review.

II. RELATED WORK

A fundamental problem within a significant part of SOC literature is that it is very fragmented and widespread. Only a limited body of work has attempted to define holistic, architectural SOC frameworks so far [2]–[6]. Although researchers agree on most of the necessary capabilities, there is no clear consensus of what constitutes a SOC. Furthermore, most academic work focuses on particular characteristics of a SOC without paying much attention to the overall picture.

We identified some work partially relevant to our approach which is trying to get a more hands-on understanding of SOCs. The authors of the respective publications use semi-structured interviews [2], [7]–[11], on-site visits [2], [12], case studies [13], or ethnographic fieldwork [14]–[17]. These publications derive their definition of SOCs following a bottom-up approach leading to a limited understanding of SOCs. Interviews and on-site visits provide insight into a small fraction of specific SOC elements but do not allow conclusions upon a general state-of-the-art. We see a lack of general overview and identification of the status-quo in the field of SOC research. There is a need for a commonly agreed-upon terminology to advance the field further. We take the first step to fulfill this need.

III. METHODOLOGY

Our work aims to identify, evaluate, and synthesize relevant academic literature in the field of SOCs. Despite the real, practical significance of the topic, there is a lack of academic research, especially regarding a commonly agreed, holistic definition of SOCs. This issue makes it hard for researchers and organizations to identify relevant literature, and as a result, impedes future research and innovations in this field.

We aim to provide a guided tour through existing literature and establish a common ground truth. To conduct the review, we follow the three stages proposed by Tranfield et al. [18] based on well-established guidelines [19]–[21]. The review protocol in Table 1 specifies research questions, information sources, search criteria, and relevant keywords. After the first collection of papers, we apply predefined criteria for inclusion or exclusion of papers to decrease the amount of papers and increase the quality of the literature considered for further review.

Table 1 lists the used keywords to identify relevant literature. Only publications that had the exact search term in title, abstract, or keywords are considered. Searching for "Security" AND "Operations" AND "Center" results in an immense number of papers, from which only a very small fraction is relevant to this study. Therefore, only the full term is applied to identify relevant literature. The common abbreviation "SOC" is not used to search for papers because it also abbreviates System on a Chip (SoC) and, as a result, also produces a high number of false positives. The defined keywords are used to search in the databases defined in (Table 1). We chose these databases because of their reputation within information systems, computer science, and cybersecurity. Finally, *Dimensions* is included in the list of searched databases as it provides a holistic view over a wide variety of papers reflected by the number of search results.

TABLE 2. Search results per database.

Database	**Search Criteria**	$\sum$
IEEE Xplore	Document title, Abstract	34
ACM Digital Library	Title, Abstract, Keywords	18
SpringerLink	Title	18
EBSCO Host	AB Abstract, TI Title Only peer-reviewed	15
Wiley Online Library	Keywords, Title	4
Web of Science	Topic (Title, Abstract, Author keywords)	30
Dimensions	Title, Abstract	202
Total		**321**
After duplicate removal		**208**
After selection criteria		**158**

In total, 321 academic publications are identified using the keywords depicted in Table 2. From this set, we remove all duplicates, leaving 208 papers to analyze. Those papers are

extracted, and the selection (inclusion/exclusion) criteria are applied. All available remaining papers are downloaded and their abstracts are read to decide upon their relevancy for the study, leaving a total of 158 papers[8]. Figure 1 illustrates the publication dates of the remaining 158 papers after applying the exclusion criteria. The first paper included in the literature review was published in 2003. The number of publications about SOCs is skyrocketing since 2015, and we expect it to keep rising within the next years. Therefore, we see a strong necessity to establish a common baseline for SOC research.

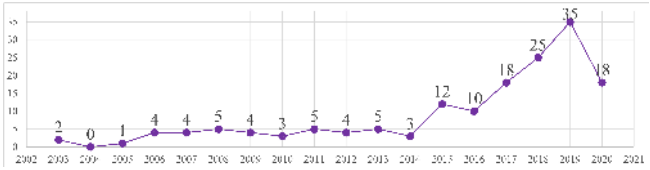

FIGURE 1. Relevant publications per year (until June 31st, 2020) identified in the structured review.

The identified literature can be categorized into two main categories *General Aspects* and *Building Blocks*. The first one summarizes the state-of-the-art regarding SOC definitions, operating models, and architectures. The second main category, *Building Blocks*, deals with the aspects which, based on literature, are comprising a SOC. Although we analyze scientific work to understand academia's current view, the topic of SOCs is highly driven by the industry as well. However, within the industry, the term *Security Operations Center* is used very ambiguously. Therefore, we only include a limited number of influential gray literature in this survey when appropriate. This literature is identified in the references used in scientific papers.

Besides the term "Security Operations Center", there is a wide variety of other, closely related terms used in the literature, e.g. Grid Security Operation Center (GSOC), Virtual Security Operation Center (VSOC), and many more. From here on, we will use the term SOC to abbreviate "Security Operations Center".

IV. GENERAL ASPECTS

This section introduces the first part of our main contribution. We subdivide this part of our work into the delimitation & definition of SOCs, their architecture, and operating models. Identified literature for these subtopics is summarized in Table 3.

A. DELIMITATION & DEFINITION

A SOC is an organizational unit operating at the heart of all security operations. It is usually not seen as a single entity or system but rather as a complex structure to manage and enhance an organization's overall security posture. Its function is to detect, analyze, and respond to cybersecurity threats and incidents employing people, processes, and technology [2], [22]–[25], [69]. Those activities can be formalized into seven dimensions or functional areas of a SOC [5], [26]. While widely accepted as utterly crucial for a company's security, SOCs are still considered a passive and reactive defense mechanism [27]–[29].

Research often describes operations within a SOC following the People, Processes, and Technologies (PPT) framework [3], [30]–[33]. This framework is used for various information technology topics like knowledge management [70] or customer relationship management [34]. Also, among SOC vendors, this framework is popular to summarize and structure their product. Although the *Governance and Compliance* aspect is often subordinated to processes, we consider it to be a category of its own due to the high importance within SOCs. It offers the framework in which people operate and according to which the processes and technologies are built. Therefore we extend the original PPT framework resulting in the People, Processes, Technology, Governance and Compliance (PPTGC) framework displayed in Figure 2.

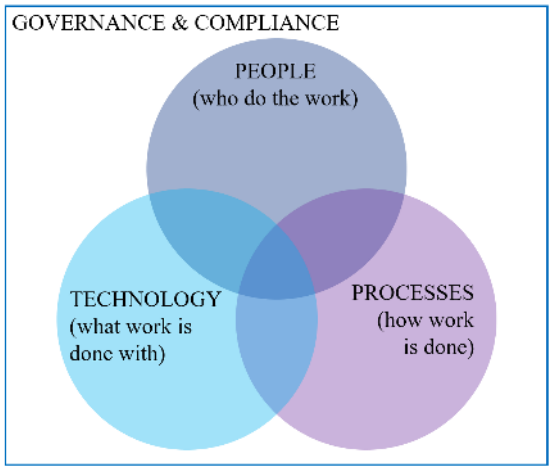

FIGURE 2. The People, processes and technology, governance & compliance (PPTGC) framework based on [70].

When implemented along with the PPTGC framework, a SOC can improve a company's security posture [36]. However, there is no clear terminology established describing a SOC. The following paragraphs delimit SOC from various other terms:

- **Computer Security Incident Response Team:** This term is often used interchangeably for a SOC although it mainly focuses on the response part once an attack has happened. A CSIRT is an organizational unit responsible for coordinating and supporting the response to a computer security incident [71]. A CSIRT is classified either as an independent team or part of a SOC [37].
- **Network Operations Center:** A Network Operations Center (NOC) oversees identifying, investigating, prioritizing, escalating, and resolving problems [17], [38]. However, in NOCs, the addressed problems are different as the NOC focuses on incidents impacting the performance and availability of an organization's net-

[8]For transparency reasons, the full list of 321 academic publications and the filtering steps are made available via https://go.ur.de/SOCLiterature

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3045514, IEEE Access

TABLE 3. Identified literature for the topic *General Aspects*.

General Aspects	References
Definition & Delimitation	[2], [3], [5], [17], [22]–[39]
Architecture	[3], [4], [6], [30], [34], [39]–[61]
Operating Models	[2], [3], [7], [25], [33], [46], [62]–[68]

work [36], [72]. As incidents can occur on all systems not just networks, it is beneficial for organizations when the NOC and SOC teams work together.

- **Security Intelligence Center:** The term Security Intelligence Center (SIC) was first used in 2017 to describe the successor of SOCs. It aims to provide a more holistic, integrated view than a SOC and can fully visualize and manage security intelligence in one place [24]. Therefore, several technologies (e.g. Information Security (IS) knowledge management, big data processing) are combined [39].
- **Security Information and Event Management:** SIEM is an integral part of many SOCs to cover a large part of the technological requirements. It is responsible for collecting security-relevant data in a centralized manner. Thereby, it provides security analytics capabilities by correlating log events. Further functionalities enable enrichment with context data, normalizing heterogeneous data, reporting, and alerting [73]. To allow the exchange of threat information, SIEM provides a connection to cyber threat intelligence exchange platforms, and it involves human security analysts by offering visual security analytics capabilities. It includes log management capabilities by long time storage of event data.

While analyzing literature for this section, we saw the lack of a commonly agreed-upon definition for a SOC. Definitions vary widely, making it quite hard to get a grasp of what a SOC is. Additionally, a SOC takes on different responsibilities depending on the technology landscape and maturity of the organization. To ensure a clear definition of the term SOC in our work, we define our understanding of a SOC stemming from and summarizing the analyzed literature in the following paragraph:

> The Security Operations Center (SOC) represents an organizational aspect of an enterprise's security strategy. It combines processes, technologies, and people to manage and enhance an organization's overall security posture. This goal can usually not be accomplished by a single entity or system but rather by a complex structure. It creates situational awareness, mitigates the exposed risks, and helps to fulfill regulatory requirements. Additionally, a SOC provides governance and compliance as a framework in which people operate and to which processes and technologies are tailored.

B. ARCHITECTURE

This section gives an overview of architectural design approaches for SOCs, which we identified within relevant SOC literature. The first part (Section IV-B1) summarizes three different general architectural approaches applied to SOC designs throughout the literature. The second part of this section (Section IV-B2) goes into more detail about specific architectures proposed throughout the years and describes the most influential ones.

1) Overall Architecture

SOCs can either be structured as centralized, distributed, or decentralized entities on a high and abstract level. In the case of SOCs, a centralized architecture describes the approach where all the data is sent from different locations or subsidiaries to one central SOC for further processing [4], [34].

A distributed SOC, on the other hand, resembles one single system operating across several subsidiaries [6], [40]. It appears for users as if they are dealing with one entity. The distributed system enables all entities to retrieve, process, combine and provide security information and services to other entities [41], [42]. It allows for spreading the workload and data evenly.

The third overall architectural design for SOCs is a decentralized system, a combination of the two system designs mentioned above [39]. A decentralized SOC comprises a few SOCs with possibly limited capabilities reporting to one or more central SOCs. A shift from having one central SOC to a more decentralized architecture is observed when comparing earlier research with more recent publications. The main reason for this seems to be to avoid a single point of failure.

2) Technological Architectures and Designs

A SOC is an organizational unit encompassing different functionalities and not just one single system. One of the first architecture models for SOCs is the SOCBox proposed by Bidou et al. [4], [34] and evaluated by Ganame et al. [43]. SOCBox defines a SOC as composed of five main modules: event generators, event collectors, message databases, analysis engines, and reaction management software.

Although the SOCBox architecture is still relevant regarding its main components, it has certain limitations as it was proposed almost 15 years ago, and technology has advanced considerably. SOCBox primarily focuses on data collection and incident management but fails to include digital forensics and reactive capabilities to prevent attacks. Moreover, the

proposed architecture describes a centralized system with numerous single points of failure. Due to the complexity of modern IT landscapes and technological developments, distributed architectures are often deemed to be more appropriate [6], [41]. Therefore, the SOCBox architecture has undergone several iterations and was improved throughout the years. Its direct successor is the Distributed SOC (DSOC) proposed by the same group of authors [6].

The DSOC architecture lays the basis for the distributed Grid SOC (GSOC) architecture for critical infrastructures, which again is developed by the research teams starting the work on the original SOCBox [40]–[42]. These three architectures highlight the shift from centralized to distributed SOC setup over time. The original SOCBox architecture [4] was also used by Miloslavskaya [39] to design a modern SOC for big data processing.

Radu [3] states that a SOC architecture consists of a generation layer, an acquisition layer, a data manipulation layer, and an output or presentation layer. This more abstract approach to defining a SOC's technological architecture using only very few building blocks can be found in several works [30], [44]–[46]. These publications conclude that a SOC consists of similar architectural blocks: a block that summarizes the data sources, followed by a block designed to collect the data from the sources and hand it to a third block responsible for analyzing the data. The last block describes the presentation of the data analysis results. None of these blocks makes any assumptions, whether done manually or automatically.

We also identified further proposals of SOC architectures within the relevant literature, focusing on SOCs for specific use cases. Settani et al. [47] describe the implementation of a SOC architecture for critical infrastructure providers. Tafazzoli and Grakani propose an architecture for processing events in an OpenStack environment to detect attacks in the cloud on a very superficial level [48]. There is a wide variety of other, very specific, and domain-tailored SOC architectures [49]–[61], [74].

C. OPERATING MODELS & INFLUENTIAL FACTORS

There are numerous ways of operating a SOC. Broadly speaking, a SOC can be operated internally or externally [7], [25], [62], [63]. However, various other and more specific classifications exist. Schinagl et al. [2] propose clustering the different operating models based on the SOC's organizational placement and its functionality, such as an integral, a technology-driven, a partly outsourced, and a specialized SOC. A different approach to classify SOC operating models is taken by Zimmerman et al. [75] and adapted by Radu et al. [3]. They use a combination of size, authority, and the organizational model and propose to divide SOCs into five different operating models: virtual SOC, small SOC, large SOC, tiered SOC, and national SOC. Another clustering of SOC operating models applies four main categories: dedicated, virtual, outsourced, and hybrid SOC [76]. Independently of the operating model of a SOC, it has to be secured itself. A failing SOC leaves the whole rest of a company vulnerable as attacks might spread undetected. Therefore, special attention must be paid to the security of a SOC [65], [66].

Each operating model has certain advantages and disadvantages, and it is essential to come to a decision upfront. Changing the SOC structure after setting it up will require a considerable amount of time and resources [64], [77], [78]. However, the choice between SOC operating models is not a trivial task, and the implications of this choice should be thoroughly considered. The literature identifies various factors which influence this choice:

- **Company strategy:** The overall business and IT strategy should be consulted to determine which operating model fits best [76]. A SOC strategy should be defined before selecting the respective operating model [75].
- **Industry sector:** The industry sector in which a company mainly operates largely influences the scope of the SOC required [7], [76].
- **Size:** The size of a company also has an impact on the decision, since a small company might not be able to set up and run a SOC on their own [67], [68] or might not even require a rigorously defined SOC [3], [25].
- **Cost:** The costs of internally implementing and maintaining a SOC must be compared with the costs of outsourcing security operations [64]. Initially, deploying an in-house SOC might be more expensive [78], but such an option might turn out to be more cost-effective in the long term. Costs of finding, hiring, and training SOC staff constitute a significant factor, especially since they might increase due to growing skill-shortage and increasing market demand [3].
- **Time:** It takes a considerable amount of time to set up a SOC. Therefore, alignment with organizational plans and timelines is necessary. Additionally, the time to set up a SOC should be compared to the time needed for outsourcing it.
- **Regulations:** Depending on the industry sector, different regulations must be considered. Some might enforce the implementation of an operational SOC [25], others might forbid the outsourcing of SOC operations altogether, or at least to specific providers who do not comply with the respective regulations [64].
- **Privacy:** Privacy also falls under regulation and must be respected whenever dealing with personal data [3].
- **Availability:** Availability requirements should be considered [68]. Most of the time, the goal is to have a SOC operational 24/7, 365 days a year [46], [78].
- **Management support:** Management support is of crucial importance when setting up a dedicated SOC. If management is not committed and benefits of a SOC are not communicated to upper management, the team might not get the resources needed [33].
- **Integration:** The capabilities of an internal SOC need to be integrated with other IT departments [7], [63], whereas, in an external SOC, the provider needs to be

integrated to get all the data needed.

- **Data loss concerns:** The SOC is most often a central place where a substantial amount of sensitive data is processed. Internal SOCs need to be highly secured, while for external SOC a trusted provider must be selected, who can ensure that the data is secured against intellectual property theft as well as accidental loss [64], [78].
- **Expertise:** It takes time and money to build up expertise. The required skills for operating a SOC are not very easy to find [63], [64]. Recruitment and retention (see also Section V-A2) of personnel is a crucial factor for internal SOCs. However, the necessary skills are already present for external SOC providers. Especially in the context of SOCs, having an insight into different companies might give SOC providers a knowledge advantage [67], [68]. However, companies should be aware that outsourcing reduces in-house knowledge [3].

With this list of important factors influencing a specific SOC's operating model decision, we conclude the *General Aspects* of SOCs identified in academic literature.

V. BUILDING BLOCKS

The second part of our main contribution now focuses on the main building blocks of a SOC. We structure this part of the work following the previously described PPTGC framework. The framework translates into defining processes to optimize operations, implementing the right technology to make work more efficient, and hiring the right people with the right skills to run the processes. Therefore, the framework allows us to define a SOC and its components cohesively. We also include a dedicated section to the aspect of governance and compliance within the SOC.

A. PEOPLE

Following the PPTGC framework, we first look at the people involved in a SOC. Literature allows us to derive the various roles and responsibilities involved in running a SOC. Another important aspect discussed in related literature is the recruitment of personnel and various retention methods. Third, the importance of training and awareness programs is outlined, and fourth, collaboration and communications procedures within a SOC are identified. The relevant literature for each of these subtopics can be found in Table 4.

1) Roles & Responsibilities

Just like in every other organizational unit, there are several different roles and responsibilities within a SOC. Depending on scope and size, different teams are needed in different numbers. Typical core roles in a SOC are different tiers of analysts as well as dedicated managers. Based on the identified work, we derive three roles with respective responsibilities [8], [54], [66], [75], [80], [81], [100], [101]:

- **Tier 1 (Triage Specialist):** Tier 1 analysts are mainly responsible for collecting raw data as well as reviewing alarms and alerts. They need to confirm, determine, or adjust the criticality of alerts and enrich them with relevant data. For every alert, the triage specialist has to identify whether it is justified or a false positive. An additional responsibility at this level is the identification of other high-risk events and potential incidents. All these need to be prioritized according to their criticality. If occurring problems cannot be solved at this level, they are escalated to tier 2 analysts. Furthermore, triage specialists are often managing and configuring the monitoring tools.
- **Tier 2 (Incident Responder):** At tier 2 level, analysts review the more critical security incidents escalated by triage specialists and do a more in-depth assessment using threat intelligence (Indicators of Compromise, updated rules, etc.). They need to understand the scope of an attack and be aware of the affected systems. The raw attack telemetry data collected at tier 1 is transformed into actionable threat intelligence at this second tier. Incident responders are responsible for designing and implementing strategies to contain and recover from an incident. If a tier 2 analyst faces major issues with identifying or mitigating an attack, additional tier 2 analysts are consulted, or the incident is escalated to tier 3.
- **Tier 3 (Threat Hunter):** Tier 3 analysts are the most experienced workforce in a SOC. They handle major incidents escalated to them from the incident responders. They also perform or at least supervise vulnerability assessments and penetration tests to identify possible attack vectors. Their most important responsibility is to proactively identify possible threats, security gaps, and vulnerabilities that might be unknown. As they gain reasonable knowledge about a possible threat to the systems, they also should recommend ways to optimize the deployed security monitoring tools. Also, any critical security alerts, threat intelligence, and other security data provided by tier 1 and tier 2 analysts need to be reviewed at this tier.
- **SOC Manager:** SOC managers supervise the security operations team. They provide technical guidance if needed, but most importantly, they are in charge of adequately managing the team. This includes hiring, training, and evaluating team members, creating processes, assessing incident reports, and developing as well as implementing necessary crisis communication plans. They also oversee the financial aspects of a SOC, support security audits, and report to the Chief Information Security Officer (CISO) or a respective top-level management position.

Each of these core roles is required to have a specific skill set. We summarize the identified skill sets very briefly within Figure 3. The core roles can be found in SOCs independent of their size. However, in a smaller SOC, each role's responsibilities are broader, and they are narrowed down to

TABLE 4. Identified literature for the topic *People*.

People	References
Roles & Responsibilities	[8], [14], [46], [54], [66], [79]–[81]
Recruitment & Retention	[10], [15], [32], [82]–[93]
Training & Awareness	[14], [88], [89], [93]–[96]
Collaboration & Communication	[8], [11], [12], [17], [23], [47], [97]–[99]

be more specific when the SOC grows. For example, in a small SOC with only a few analysts, everyone needs to be knowledgeable on several skills because a few employees need to cover all the arising tasks. In a bigger SOC, roles can be more specific as, for example, some analysts might be focused on network monitoring while others are experts for Windows or Linux specifics. This comes with many advantages, such as a better and faster response to threats or better separation of tasks.

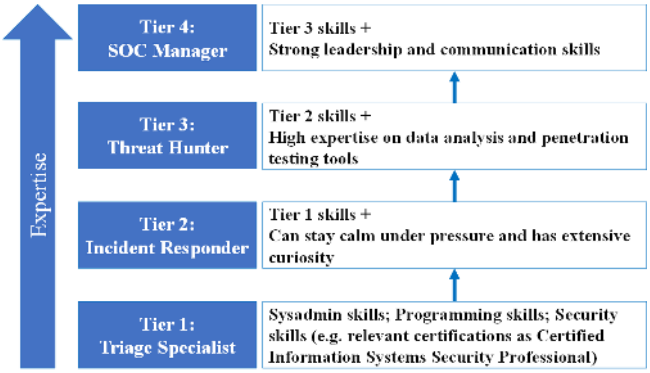

FIGURE 3. Necessary skills among SOC roles [54], [66], [75], [100], [101].

Besides the four already described essential roles, we identified additional roles that are at least to some extent involved in the daily business of a SOC [14], [46], [75], [79]. Because of the wide variety of identified roles, it is important to attempt to structure them. We have derived a list of different roles and possible interconnections between them. Figure 4 depicts those based on Olt [79]. These additional roles need to lead, work together, or cooperate with the previously described core SOC roles, which are also included in the figure. However, substantial overlap between roles and additional roles might be included in running a specific SOC. This is why we decided to group the roles into five main groups indicated through different colors in Figure 4. These groups can be adapted or expanded with additional roles when necessary:

- **Management roles:** In the context of a SOC, we identify three critical managerial roles. First of all, the *Chief Information Security Officer* defining strategies, goals, and objectives of an organization's overall security operations. A *SOC Manager* leads the SOC itself. We already described this role upfront. Inside of the SOC, the literature includes one additional high-level management role: the *Incident Response Coordinator*, which coordinates all activities related to incident response.
- **Technical roles:** There is a wide variety of additional security specialists who need to collaborate with the SOC analysts to allow for efficient and effective SOC operations. *Malware Analysts* help with responding to sophisticated threats by performing malware reverse engineering and creating crucial results for incident response activities. To be aware of possibly ongoing attacks, *Threat Hunters* actively look for threats inside the organization, for example, by reviewing logs or outside of the organization by analyzing available TI data. This TI data is also explicitly analyzed by *Threat Intelligence Analysts* or researchers. They analyze threat intelligence from various sources and produce input for the SOC team. If parts of an attack have succeeded, *Forensic specialists* conduct detailed investigations into them. They collect and analyze forensic evidence in a legally sound manner. *Red Teams* and *Blue Teams* actively try to attack or respectively defend the organization's systems to identify vulnerabilities, and both test as well as increase the effectiveness and resilience of security mechanisms. Finally, *Vulnerability Assessment Experts* perform research to identify new, previously unknown vulnerabilities and manages known vulnerabilities with respect to business risk. These experts create detailed technical reports with their findings and support SOC analysts or incident response teams in specified vulnerability discoveries. Another vital role of this group is the *Security Engineer (SE)*. The SE develops, integrates, and maintains SOC tools. Security Engineers also define requirements for new tools. They ensure the appropriate access to tools and systems. Additional tasks are the configuration and installation of firewalls and intrusion detection/prevention systems. Furthermore, they assist in writing and updating detection rules for Security Information and Event Management (SIEM) systems.
- **Consulting roles:** The two most important roles of this group are the *Security Architect (SA)* and the *Security Consultant*. The SA plans, researches, and designs a robust security infrastructure within a company. SAs conduct regular system and vulnerability tests and implement or supervise the implementation of enhancements. They are also in charge of establishing recovery

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3045514, IEEE Access

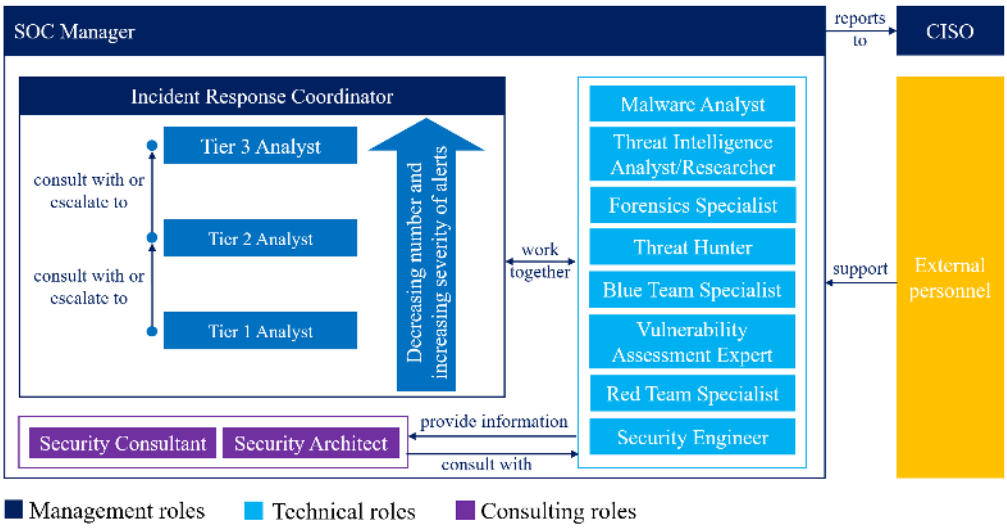

FIGURE 4. Interaction of different roles within a SOC [79].

procedures. Security consultants often research security standards, security best practices, and security systems. They can provide an industry overview for an organization and compare current SOC capabilities with competitors. They can help to plan, research, and design robust security architectures.

- **External personnel:** External personnel can be included in any SOC operation, and therefore, depending on the architecture and operating model of a SOC, more or less external personnel are involved in the different SOC roles and groups.

Besides technical skills, soft skills are becoming more and more important. Desired skills include communication skills, continuous learning abilities, analytical mindset, ability to perform under stress, commitment, teamwork, curiosity, and practical organizational skills [75]. The significance of relevant soft skills grows with the level of responsibility an individual has within a SOC. Besides hard and soft skills, there is a number of useful certifications for SOC employees depending on their level, which are summarized by DeCusatis et al. [80].

2) Recruitment & Retention

The people working in a SOC are the last line of defense and responsible for detecting and successfully mitigating attacks. Thus, having skilled human resources in an adequate quantity is imperative for the success of a SOC [32]. However, finding and retaining the right staff is not an easy task. The International Information System Security Certification Consortium ((ISC)^2) puts the current cybersecurity workforce gap at roughly four million people on a worldwide scale, and it is still growing [102]. Therefore, recruiting new, skilled staff for SOCs is getting increasingly difficult. There is little to no literature about how to specifically recruit SOC staff. Most of the relevant papers focus on retaining SOC staff and closing the skills gaps with automation.

Working in a SOC is very demanding and can be extremely stressful. Anthropological studies found that SOC analysts are often not satisfied with their job [15], [16]. They are overloaded with mundane, tedious tasks, and the currently deployed tools are not sophisticated enough to automate these tasks [82]–[84]. SOC analysts' primary responsibility, especially at tier 1, is to follow Standard Operating Procedures (SOPs), also called playbooks. This negatively impacts their creativity, growth, skills, and empowerment. Literature reveals a vicious cycle, which ultimately causes analyst burnout in a noticeable number of cases [15], [16]. Therefore, companies should take action to increase the job satisfaction of their SOC staff. Several methods to counteract staff burnout and increase job satisfaction can be determined:

Increase Automation: Increasing automation helps decrease the amount of mundane and boring tasks [83], [84]. This can be achieved with more efficient and helpful tools deployed within the SOC. Analysts should be consulted before buying and implementing tools, and they should be engaged in the development of new tools. New possibilities for automation can be discovered by analysts themselves if they have time to reflect on their daily work [16], [85]. Technology should amplify the human capacity to be creative and apply critical thinking to solve problems. Examples are studies analyzing data triage tasks and trying to optimize the process [86]–[89].

Increase Operational Efficiency: Automating specific tasks can also help to increase operational efficiency. Additional improvements can be made by streamlining processes, ensuring that analysts have access to the data they need, and providing team communication and collaboration possibilities. An example is the preferably optimal prioritization of alerts, so analysts can focus on the most critical ones [90], or the adaptive reallocation

of analysts based on the current needs [91].

Invest in Human Capital: Security professionals working in a SOC need to possess the right skills to perform their job correctly, as described above. Investing in their skills will not only contribute to their personal well-being but also benefit the company itself [92]. Skills can be enhanced by in-house or outsourced training, conference participation, observation of more senior staff, or even learning-by-doing. The more skills employees master, the more likely they are to be empowered. This empowerment enables employees to do their job efficiently and increases their morale [16]. Gaining skills and feeling empowered, in turn, has a positive effect on the creativity of analysts. Ultimately, employees grow and increase their intellectual capacity, are empowered, and more likely to be creative. If a positive causality among the personal development factors exists, SOC staff will be gratified [16], [93]. Unfortunately, it is not always possible to exactly meet employees' expectations. Technological limitations require personnel to sometimes do tedious tasks, and budget restraints might hinder staff from going on training. Other incentives, like a competitive salary, monetary bonus, team-building or after-work activities, flexible and competitive working hours, respect, and recognition, can also play a role in keeping up the SOC staff's morale.

3) Training & Awareness

Well-trained employees are more productive because they understand their responsibilities and tasks. Training strengthens their skills and addresses potential knowledge gaps. The quality and consistency of the work also increases [93]. Furthermore, training benefits an organization itself because employees are less likely to make mistakes. A study conducted by Accenture and the Ponemon Institute revealed that employee training could decrease the total cost of a cyber breach by about 270.000 USD [1].

For junior staff members, training is a means to equip them with the technical and soft skills required to perform well in their job. Training for juniors has a broader scope and aims to provide them with an overview of various security-related topics. For example, for a SOC tier 1 analyst, training could be given in real-time analysis, incident analysis and response, scanning and assessment, alert correlation, and many more. For more senior staff, training should be more tailored to their specific role in the SOC as employees working in a SOC are very likely specialized in specific tasks.

In general, training should consist of a mix of formal training, internal training, vendor-specific training, and on-the-job learning. Formal training is a form of structured training with predefined goals and objectives. Internal training is often taught by other team members and of a more informal nature. Thus, there is a less strict plan and internal training is more dynamic.

Vendor-specific training is used to familiarize SOC staff with deployed software (e.g. a specific SIEM system). On-the-job learning or shadowing more experienced team members is another form of acquiring the necessary skills [14]. As this type of learning is very unstructured, it is following a steep learning curve. However, it might be overwhelming for new SOC employees to deal with the flood of incoming alerts without more formal training [94]. To support them, Zhong et al. [88], for example, developed a system that traces and models the data triage actions of senior analysts to the present actions done in a similar context. All different training approaches have several advantages as well as disadvantages. There is only very little scientific work on SOC-specific training methods. Further research is necessary to show how different training methods can be applied in the context of SOCs and measure their effectiveness. An interesting approach to improve on-the-job learning and training is pursued by Applebaum et al. [95] by developing playbooks that provide analysts with an overview of tasks and actions based on the experience of other analysts. Also, knowledge graphs representing the domain knowledge and experience of SOC analysts enable better learning and training for others [89], [95]. A relatively exotic use case is considered by Sanchez et al. [96]. They present particular challenges for a SOC within the space domain and emphasize employee training's unique challenges.

4) Collaboration & Communication

Especially in high-pressure environments like a SOC, collaboration amongst the various team members is essential [17], [47]. A few academic resources are focusing on collaboration in SOCs. Hàmornik and Krasznay [8] emphasize the need for further research about computer-supported collaborative work (CSCW) to see how computer systems can support collaborative activities. The AOH-Map developed by Zhong et al. [97] is a collaborative analysis report system capturing and displaying the analytical reasoning process of analysts. Afterward, analysts can look at the captured process, review past decisions, share their results with others, and divide their tasks effectively. Additionally, work between analysts needs to be divided equally depending on their skills [98]. Crémilleux et al. [11] propose a collaboration process to create a feedback loop between tier 1 and tier 2 SOC analysts.

An upcoming trend is the operative use of visualization platforms with collaboration features, e.g., the 3D CyberCOP platform [12], [99] distinguishes explicit collaboration through the platform and implicit collaboration through oral communication and logging every user's actions. It is imperative for the SOC team's success to have constant interaction and communication with other business units, for example, the help desk, network administrators, or even the legal team. This requires ensuring the other departments that the SOC staff is not there to watch their every move but to help [23].

B. PROCESSES

This section features academic work focusing on the processes related to a SOC. We aim for a high-level perspective, as there are different, very specific processes happening in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3045514, IEEE Access

TABLE 5. Identified literature for the topic *Processes*.

Processes	References
Preparation	[22], [55], [67], [103]–[113]
Detection & Analysis	[4], [67], [80], [83], [114]–[118]
Containment, Eradication & Recovery	[80], [83], [97], [103], [104], [114], [117]–[122]

operations. Since the goal of a SOC is to respond to or prepare for incidents, one way to structure the underlying processes is through the Incident Response Lifecycle [103], [114], [119], [120] or similar frameworks such as presented in ISO/IEC 27035:2016 [123]. According to the NIST Computer Security Incident Handling Guide [124], the Incident Response Lifecycle comprises the four steps "preparation", "detection and analysis", "containment, eradication and recovery" and "Post-incident activity", which also form the structure of the following chapter.

At this point, we would like to emphasize that, in our view, the literature only allows an incomplete picture regarding processes. For example, technical processes are treated very intensively, whereas most surrounding processes are only dealt with sporadically. These aspects are to be regarded as research gaps and are presented in the following chapter accordingly incomplete, in order to go into the gaps in more detail in chapter VI. This is especially true for "post-incident activity" since no SOC specific scientific publication deals with this topic. Therefore, it will not be considered in the following descriptions.

1) Preparation

The analyzed literature mainly focuses on data collection within the topic of preparation; however, it does not give a uniform picture of which steps the data collection process is composed. However, as illustrated in Figure 5, the steps normalization with time synchronization [22], [55], [104]–[107], filtering [22], [55], [105], [106], [108], reduction [22], [109], aggregation [22], [55], [106], [109], [113] and prioritization [22], [55], [67], [103] or risk evaluation [110] were most frequently mentioned. The order of process steps is not uniform in literature, as this can vary depending on the application used. However, it is mostly described in the presented sequence. The identified process steps are explained in more detail to provide a general understanding:

Normalization: It is vital to translate the heterogeneous data formats into a uniform representation to conduct further processing. It is also essential to change all time data to one standard time zone and format [22], [77]. Synchronization helps avoid confusion in the timeline of the security events and reduces the likelihood that erroneous conclusions are made on inconsistently measured network activity. In literature, normalization is often referred to as log parsing or pre-processing.

Filtering: Since systems typically generate enormous amounts of data, it is essential to filter for data elements that are likely to contain important information from a security perspective [125].

Reduction: Reduction is like filtering, with the difference that individual, unimportant data fields are sorted out to reduce the amount of data.

Aggregation: Similar events are combined into one single data element. For example, three log entries, which indicate a log attempt to a host, could be aggregated to one single log, which states the type and number of login attempts [125].

Prioritization: Each log data should be classified according to importance to facilitate further processing. For example, to decide how to react to events or how long the logs should be stored, it is useful to prioritize incoming data.

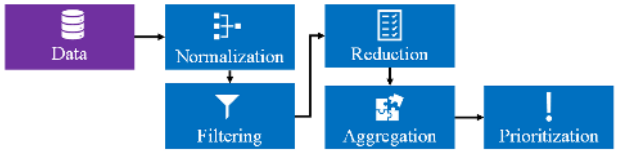

FIGURE 5. The data collection process.

Considering literature about data collection specifically for SOCs, there are only two notable papers: [111] and [22]. This is probably because most SOCs deploy a software solution responsible for collecting, processing, analyzing, and displaying events and alerts [112] and thus data collection is addressed in a more technical context. Bridges et al. [111] conduct interviews with 13 professionals from five different SOCs to discover the current state-of-the-art and future directions for host-based data collection. They evaluate what and how host data is collected, which tools are used, and whether dynamic collection (dynamically decide how much and which data is collected depending on factors such as security posture) is used. Their major takeaway is that analysts desire a wider, less manual collection of data, but only with the right toolset to understand and work with the data. Madani et al. [22] propose a logging architecture for SOCs. Their architecture contains log generators, a collection server, a storage server, and a log database. The authors list SIEM vendors incorporating log management in their SIEM solution and outline their weaknesses. Normalization, filtering, reduction, rotation, time synchronization, aggregation, and integrity check are the most important functionalities. Madani et al. [22] underline the importance of log collection and management. However, since the paper was published in

2011, there have been no SOC specific advances in the field.

2) Detection and Analysis

The sheer amount of data collected in previous steps can be overwhelming, even for seasoned security practitioners and researchers. Turning this data into useful information is done through data analysis and is essentially a means to make sense of what is collected. Regarding automatic analysis and detection, the identified literature mainly focuses on specific analysis and detection methods and technologies. However, only a few papers look at the subject area from an abstract, process-driven perspective. The following process steps were identified by merging available processes [73], [114] and by sequencing individually named steps within the stated literature. This results in a process which is comprised of the steps *Detection* [83], [114], *Analysis* [4], [115], [116], and *Alert Prioritization/Triage* [67].

- **Detection:** Incidents are detected with the help of humans or by automatic procedures. Thereby, it must be decided if the collected data indicates a security incident [114]. A more technical description of the identified detection approaches can be found in Section V-C2.
- **Analysis:** Regarding the techniques used for analysis, one can distinguish between source and target correlation, structural analysis, functional analysis, and behavior analysis [4]. Thereby, the authors describe the purpose of correlation as to enable the analysis of complex sequences by producing simple, synthesized, and accurate events.
- **Alert Prioritization/Triage:** Alert prioritization, also known as triage, can be seen as a link to containment, eradication, and recovery. It serves two primary purposes. First, to ensure that the most severe incidents are treated with priority, and second, to ensure that incidents are distributed for further processing according to available resources [67].

3) Containment, Eradication, and Recovery

The activities in containment, eradication, and recovery are described by Bhatt et al. [104] on a high level. This step aims to decide whether an incident is an unharmful event (e.g., during penetration testing), or a harmful event. In the case of a harmful incident, it is passed on to appropriate stakeholders to take further steps. In this context, Security Orchestration, Automation, and Response (SOAR) is of great importance and can be identified as a very active research area of the last two years [83], [118], [122]. According to Islam et al. [122] the key purpose of SOAR is the automation of processes through orchestration. The functionalities of SOAR are mainly categorized into integration, orchestration and automation. Security orchestration is a prerequisite of security automation, which is the process of automatic detection [117]. Therefore, SOAR integrates available information about security incidents (Cyber Threat Intelligence) [121] to automatically take appropriate measures to limit the damage as quickly as possible. Islam et al. [122] conducted a detailed survey on this topic.

A straightforward framework to tackle incidents is the Observe, Orient, Decide, Act (OODA) loop, which is a well-known analytical framework for decision-making developed by John Boyd [126]. It can be applied to incident management in the context of a SOC, as demonstrated in research [80], [97] (or similar to the Plan, Do, Check, Act loop [120]). In SOC literature [103], [114], incident management is mentioned mostly related to the incident handling lifecycle. Thus, the Alert and Incident Management process presented in Figure 6 comprises the process steps identified by two primary standards for information security incident management [123], [124].

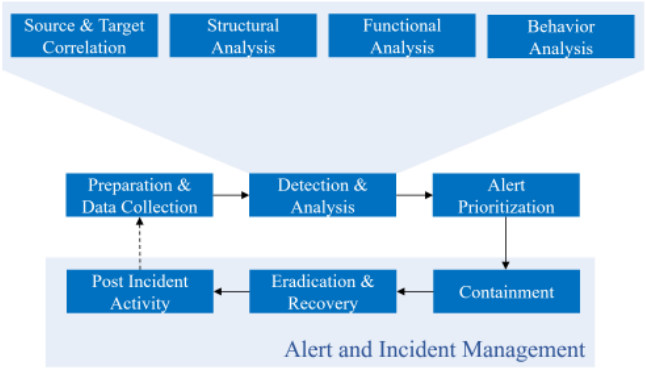

FIGURE 6. The SOC incident analysis, detection and management process.

A more detailed description of these process steps concerning SOC cannot be found in the analyzed literature, which is why the standards mentioned above must be referred to if necessary. The reason for this could be that employees know which tasks they have to carry out, but this has not been specified explicitly, which can cause problems, e.g., when staff changes. Therefore, Cho et al. [119] conducted a study where they show how it is possible to capture SOC staff's tacit knowledge on how they perform their tasks as processes.

C. TECHNOLOGY

This section discusses the technologies combined in a SOC. It covers the process steps from Section V-B from a technical point of view, whereby Containment, Eradication, and Recovery is not considered, as we did not find any literature dealing with SOC-specific technology covering this process step (see Table 6).

We first take a look at data collection technologies which support the preparation process mentioned in Section V-B1. Every organization should determine which devices should be monitored, what data needs to be collected, and in which format it should be stored. Moreover, depending on the data, the retention period of the data needs to be set. We then shed light on the applied methodologies and approaches to analyse data, detect threats and present the results, which can be mapped to the process detection & analysis (Section

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3045514, IEEE Access

TABLE 6. Identified literature for the topic *Technology*.

Technology	References
Data Collection	[37], [47], [80], [103], [104], [107], [111], [127]–[132]
Analysis & Detection	[13], [35], [41], [43], [55], [56], [84], [133]–[157]
Presentation	[9], [12], [13], [80], [97], [99], [112], [127], [158]–[170]

V-B2). As the interface between people and machines, the presentation of data and analysis results is of particular interest in a SOC context.

1) Data Collection

Various data collection techniques exist and can generally be classified into four categories: push/pull, distributed/centralized, real-time/historical and partial/full collection. Data can either be pulled by the data collector or pushed onto the data collector from the data source itself [77]. Furthermore, it can be collected in a centralized log collector (e.g. [171]) or in a distributed topology (e.g. [172]) over different subnodes. Thereby, data can either be captured fully or partially.

Within the identified literature, data collection mainly relates to identifying data sources that capture relevant security-related information. While new data sources are continuously being created, the most common sources, its classification [127], [173], [174], and corresponding examples are:

- **Security software:** SIEM systems [80], intrusion detection/prevention systems [37], [103], [107], [128], [162], [173], [174], firewalls [37], [104], [127], [128], [174], anti-virus software [37], [111], [127], vulnerability scanners [173], identity and access management [104]
- **Network assets:** Switches [104], [173], routers [104], [128], [173], servers [104], [127], [173], hosts [104], [173], proxies [174]
- **Virtualization environments:** Hypervisor, virtual machine introspection, cloud environments [80]
- **Operational technology:** Sensors, actuators, PLCs
- **Other Software:** Open-Source Big Data Analytics [80], databases [173], identity and access management [173], mailserver [174], operating systems [111], [174]
- **Physical security assets:** Security cameras, access control
- **External (Threat) Intelligence:** Geolocation and DNS lookup [80], open source intelligence (OSINT) [47], [129], intelligence from threat sharing platforms or other organizations [130]–[132]
- **People:** Employees (Human-as-a-Security-Sensor [175]), external users.

Each of these data sources can deliver a vast amount of information, of which not all is relevant. Capturing everything may help in spotting malicious activity, but it can also negatively impact system performance. Conversely, if fewer data sources are used to collect data, an attack might go undetected. Thus, finding the right balance between capturing too much and capturing too little data is essential when designing a SOC's technological capabilities. However, as a rule of thumb, it is generally better to capture data from as many sources as possible (under performance constraints) and then rely on well established data normalization, correlation, and analysis mechanisms.

Depending on the data source, the data type collected may vary as illustrated in Figure 7. All collected data can be broadly classified into either log data or intelligence. Logs document the current state of the system and usually record all the changes occurring within the system. Logs are generally divided into operating system/application logs and security software logs [125]. Network logs proposed by Zhiguo et al. [176] can be added since they have unique features and cannot be categorized perfectly into log categories. Operating systems and applications often provide data in the form of logs. These logs give the user information on system events such as the shutdown or start-up of a service, audit records, client requests and server responses, account information, usage information, etc. Security logs instead display suspicious activities, results of virus scans, etc. [125]. Intelligence provides additional context for threat analysis.

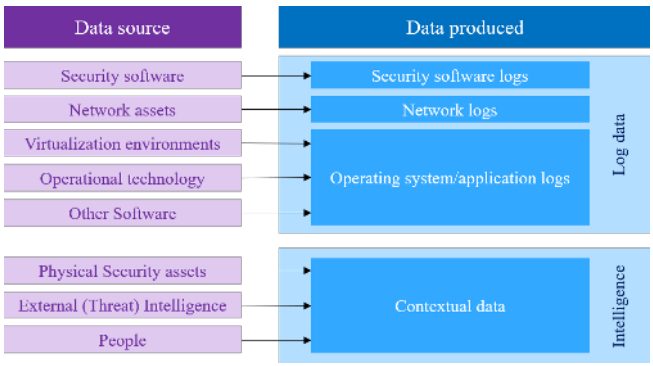

FIGURE 7. Data sources and the type of data they produce.

2) Analysis & Detection

Attack detection is performed either automatically or manually. Manual detection is the detection of an incident through an internal or external person. Thereby, the detection can be performed by security experts such as analysts within the SOC or by security novices. The different roles and tasks of security experts are further discussed in Section V-A.

TABLE 7. Classification of literature with respect to applied detection methodologies and approaches.

	Detection methodologies			Detection approach classes				
	Anomaly	**Signature**	**Specification**	**Statistics**	**Pattern**	**Rule**	**Heuristic**	**State**
[13]	✓			✓				
[35]	✓			✓				
[41]		✓			✓	✓		
[43]	✓	✓			✓	✓		
[55]		✓			✓			
[56]	✓			✓		✓		
[84]		✓					✓	
[134]		✓			✓		✓	
[135]		✓		✓		✓		
[136]	✓	✓		✓	✓	✓	✓	
[137]		✓			✓	✓		
[138]		✓		✓	✓		✓	
[139]	✓			✓		✓		
[140]		✓		✓			✓	
[141]		✓		✓		✓	✓	
[142]		✓				✓		✓
[143]	✓			✓		✓		
[144]		✓			✓	✓		✓
[145]		✓		✓				✓
[146]	✓				✓			
[147]		✓					✓	
[148]	✓					✓	✓	
[149]	✓	✓				✓		✓
[150]		✓		✓		✓		
[151]	✓	✓		✓	✓			
[152]	✓					✓		
[153]	✓	✓		✓				
[154]		✓				✓		
[155]		✓		✓			✓	
[156]	✓			✓			✓	
∑	14	21	0	16	10	16	10	4

An example of manual detection through security novices would be if an employee receives a phishing mail and then reports it, so the security team can take appropriate measures. The concept of integrating employees into the detection process was introduced as "human-as-a-security-sensor" [175], [177] and means that employees are enabled to detect and report security incidents. Therefore, awareness training plays a crucial role as further discussed in Section V-A3. All in all, manual detection is necessary, because not all attacks can be detected through technology, especially when it comes to advanced attacks. However, automated detection cannot be neglected, because the sheer amount of data would overstrain humans. The topics of manual detection related to presentation are discussed in Section V-C3.

Regarding automatic analysis and detection, the identified literature mainly focuses on specific analysis and detection methods and technologies. To show the state-of-the-art analytical methods, those mentioned in the literature are classified in Table 7. Therefore, a well-accepted classification scheme of Liao et al. [178] was used. It distinguishes between detection methodologies and detection approaches.

Anomaly-based or behavior-based methodologies use the system's normal behavior as a foundation and try to detect deviations. *Signature-based* or also knowledge-based methods use accumulated knowledge of attacks and is very useful to detect known attacks or exploitation of known system vulnerabilities. Therefore, it is important to regularly update the knowledge base. *Specification-based* methodologies focus on detecting incidents based on predefined profiles or protocols. Hybrid methodologies use a mixture of the three described detection methodologies.

Concerning detection approaches, *statistics-based* detection is one of the oldest methods used for intrusion detection and uses statistical properties and statistical tests like mean, median or variance, to detect deviation between the normal behavior and observed behavior. Threshold metrics, hidden Markov models and multivariate models are examples of statistical based detection approaches. *Pattern-based* and *Rule-based* approaches use either predefined patterns, learned patterns or rules for detection. An example for rule-based detection are support vector machines. *Heuristic-based* approaches are inspired by biological concepts as for example artificial neural networks. *State-based* approaches try to infer the behavior of attacks within the network for example by

utilizing finite state machines.

Table 7 shows, that all used detection methodologies are either anomaly- or signature-based. In none of the analyzed papers, the potential of specification-based incident detection was leveraged. In contrast, each detection approach class can be assigned an approach described in the literature, whereby a focus on statistics- and rule-based approaches is recognizable. To enhance detection independent of the utilized approach Karacy et al. [133] propose a principle that allows intrusion detection even when end-to-end encryption was used and Smith [157] suggests that user behaviour analytics (UBA) should be used more intensively, since misused credentials are a great threat.

3) Presentation

From a technological view, most identified publications focus on specific visualization tackling problems related to SOCs. They are briefly outlined in the following. DeCusatis [80] describes an attack visualization based on force diagrams and hive plots. Settani et al. [158] shows how a map and dashboard-based visualization of incidents and a mobile visualization enables on-site personnel to make qualified decisions. Besides, Erola et al. [159] present an approach that combines machine learning and information from business processes with visual analytics to guide SOC employees through the decision-making process. Similarly, Sopan et al. [9] aim at visually supporting SOC analysts by automating decision-making using a machine learning model. However, they also present the model visually to enable the machine learning model's decisions to be understood. The Situ platform [13] has the goal to visualize the context of an incident for leveraging the experience of security experts. In contrast to the approaches described above, the CyberCOP [12], [99], [160] platform relies on three-dimensional visualization. The VISNU project [112], [161], [162] takes a similar approach, which improves the collaboration of multiple SOCs in different organizations by displaying network data in three dimensions. Thereby, they aim at the collaboration of multiple analysts in one environment by providing different views on the same incident. The concept of mind maps is leveraged by the AOH-Map [97] software, which visualizes all the identified traces of an attack to exchange it with collaborating analysts. Hassell et al. [163] combine network simulation with its visualization for optimizing its resilience against threats. Payer et al. [164] rely on Virtual Reality (VR) to analyze threats, allowing new types of interactions. To enhance tactical situational awareness within a SOC Mullins et al. [170] describe three suitable visualizations.

Starting 2018, increasing interest in sonification and its potential for SOCs can be identified [165] as it was implemented within the SIEM system of a SOC [166]. This showed that humans can detect attacks by listening to network traffic [127], [167] in specific contexts [168].

A fairly new approach to SOC is data presentation using storytelling presented by Afzaliseresht et al. [169]. This involves translating the analysis results into a narrative story containing more or less details depending on the users' level of knowledge. In a SOC setting within a research institution, this approach is advantageous in terms of cognitive load.

D. GOVERNANCE AND COMPLIANCE

The following section discusses the governance and compliance aspect of a SOC (see Table 8). IT governance is responsible for ensuring the effective and efficient use of IT systems by providing a strategic direction, developing standards, policies and procedures, and implementing them. Compliance ensures that companies adhere to external rules, for example standards and regulations and internal rules, for example policies and procedures. Additionally, compliance is essentially the feedback loop of security governance, because it shows how governance rules are applied in practice. The following section will look at three aspects of governance and compliance: how security audits are performed, current metrics in a SOC and standards and guidelines related to SOCs. It should be noted that metrics play a major role in maturity assessment, so the two sections partly overlap.

1) Standards & Guidelines

Today, many organizations are struggling to decide whether they need a SOC, which kind of SOC they need, and what components their SOC should have. There are no renowned holistic SOC standards or industry specific guidelines to help companies with their decisions [3]. However, a SOC can help to ensure that certain compliance regulations are met [30], [179] and many of the standards focus on one domain or task within a SOC. We provide a list of these standards in Table 9.

Another noteworthy standard is provided by the European Telecommunications Standards Institute (ETSI) [187] providing guidelines for building and operating a secured SOC. It mainly focuses on requirements to be met by the service provider operating a SOC for the telecommunication industry. Some private organizations have started to provide companies with best practices and recommendations, for example by conducting a survey [188]. There is only very little work on establishing best practices for a SOC [36], [60].

2) Security Audits & Maturity Assessments

A SOC can help companies in conducting internal and external IT (security) audits. In an IT audit, the IT infrastructure, policies, and procedures are examined and evaluated. Independent and unbiased parties usually perform external audits. An example would be a typical year-end audit in the banking sector, which assesses the compliance of its IT capabilities against relevant standards. Depending on the type and scope of the audit, different IT capabilities are assessed. Because a SOC collects valuable log data from almost all systems, and hosts some relevant capabilities itself, it is an invaluable source of data for IT auditors. Advanced SIEM tools aggregate security information from across the company and generate reports for compliance audits. This information can be used to prove compliance with laws and

TABLE 8. Identified literature for the topic *Governance & Compliance*.

Governance & Compliance	References
Standards & Guidelines	[3], [30], [36], [60], [179]
Security Audits & Maturity Assessments	[2], [5], [63]
Metrics	[23], [30], [46], [57], [68], [81], [85], [163], [180]–[186]

regulations. Additionally, the SOC team can help determine the IT risks for the company.

Of course, the SOC itself should have controls in place, which should be audited regularly. An example for an internal SOC audit and its findings is given by NASA [189]. Due to the lack of widely accepted standards and guidelines, external assessments are not offered by independent parties. However, there is literature proposing methods to assess the current maturity of the SOC capabilities as well as the overall effectiveness of the SOC [63]. Common maturity models are compared and summarized into five capability maturity stages: non-existent, initial, repeatable, defined process, reviewed and updated, and continuously optimized [63]). In practice a similar maturity assessment approach is presented in an industry guideline from IBM [190]. Schinagl et al. [2] assess the effectiveness of a SOC by identifying the degree to which identified building blocks have been implemented. These approaches enable SOC owners to uniformly assess the maturity of their capabilities and to spot the areas which still need to be improved. It also allows various companies to compare their SOC operations and benchmark against each other, if the data is made available, enabling the collaboration between SOCs. To locate collaboration areas of SOCs, a questionnaire-based approach is proposed by Kowtha et al. [5]. The authors describe a model for characterizing SOCs by the seven dimensions of scope, activities, organizational dynamics, facilities, process management and external interactions.

3) Metrics

Metrics are quantifiable measures used to track and assess the status of a process or system. Metrics are mainly used to support strategic decisions, to assure the quality, or to gain tactical oversight [191]. A considerable body of literature exists in the field of security metrics [192], [193], and many of those metrics can be directly applied to a SOC. However, there is very little scientific literature on how those security metrics can be used in a SOC, let alone metrics specifically covering SOCs. Ganame and Bougeois [180] propose metrics to assess the security level of different sites in a multi-site network in real-time. Their goal is to see whether threats are occurring in a network or not. Aiming to improve the resiliency of networks, Hassell et al. [163] test their simulation software using resiliency metrics. They criticize the lack of standardized metrics to evaluate resiliency techniques. Ganesan et al. [181], [194] propose an optimization model to dynamically schedule analysts and dynamically assign them to sensors to decrease total time for alert investigation and increase the Level of Operational Effectiveness (LOE). Some literature, however, comes from SOC vendors [188], [195]. Typical metrics used in a SOC include:

- **General SOC metrics:**
  - **Coverage [188]:** A SOC can only monitor a limited amount of assets due to resource constraints, which raises the question of how many of them are covered. *Examples:* Number of monitored assets, coverage (number of monitored assets vs. number of assets)
  - **Performance metrics:** Measurement of the performance is crucial for managing and improving a SOC. Historical performance metrics enable comparability between work-shifts or longer time periods [68].

TABLE 9. Standards related to SOC domains or tasks.

Domain or task	Standards
Cyber Security in general	ISO/IEC 27001 and 27002, IEC 62443, ANSI/ISA 62443, NIST Cybersecurity Framework, NIST Special publication 800-12, NIST Special publication 800-14, NIST Special publication 800-26
Data Logging	DCID, FFIEC, ISO 17799, DISA, NIST SP 800-92, NIST SP 800-53, PCI DSS, FDA GXP
Incident Management	SANS Incident Handler's Handbook, ISO/IEC 27035:2016, NIST Special publication 800-83, NIST Special publication 800-61, ITIL
Business Continuity Management	ISO 22301:2012, ISO 22313:2012, ISO/FDIS 22313, BSI-Standard 100-4
Digital Forensics	ISO/IEC 27037:2012, ISO/IEC JTC 1 SC 27, ISO/IEC 27041:2015, ISO/IEC 27042:2015, NIST SP 800-86
IT Governance	COBIT, ITIL, Information Security Assurance - Capability Maturity Model (ISA-CMM)
Vulnerability Management	SANS Implementing a Vulnerability Management Process, NIST SP 800-40, ISACA Vulnerability Management
Privacy	EU-GDPR

Agyepong et al. [85] conducted an extensive survey about performance metrics for SOCs and proposed a consecutive framework [186]. *Examples:* False positive rate [30], [68], average analysis time [68], readiness level [81], [181], Mean Time to Detect [185]

- **People metrics:** To improve the performance of security analysts inside a SOC it is necessary to measure human activities and workflows [68]. *Examples:* Security analyst performance [68], number of incidents closed in one shift [188], workload [195]
- **Technical metrics:**
  - -- **Threat metrics:** A threat is the potential damage posed by vulnerabilities. Thus, these metrics are closely related and, in most cases, based on vulnerability and threat metrics. *Examples:* Security level [180], threat actor attribution [188]
  - -- **Vulnerability metrics:** In general, vulnerabilities can be exploited by attackers or can cause a security incident. Thus, it is particularly important for SOCs to be aware of possible weak spots. *Examples:* Vulnerability exposure [182], time-to-vulnerability remediation [182], vulnerability severity [182], incidents due to known vs. unknown vulnerabilities [188]
  - -- **Risk metrics:** Risks are in most cases assessed in real time, which is also summarized under the term situational awareness [46]. The evaluation of risks is especially important, when it comes to choosing appropriate security measures. *Examples:* Risk posture [23], [46], [183], [184], [188], risk per system [81], [180], key risks [195]
  - -- **Alert metrics:** Alerts are in most cases generated automatically by technologies such as SIEM systems or intrusion detection systems, based on the analysis of sensor data [181]. Each alert should go through an alert analysis process [194] in order to decide upon possible measures. *Examples:* Time per alert investigation [181], alert generation rate [181], number of alerts that remain un-analyzed [81], criticality of an alert [180]
  - -- **Incident metrics:** An incident is an occurrence, that causes harm to an organization and a SOC aims at averting incidents or reducing the caused harm. As incidents are a very central element of SOCs, appropriate metrics are essential. *Examples:* Incident priority [23], number of incidents [68], [183], [188], number of successful attacks [163], recovery time [181], costs per incident [188], mitigation success [195]
  - -- **Resiliency metrics:** Cyber resilience is crucial, if an environment is compromised in order to continue operations with as little damage as possible [163]. *Examples:* Time spent per attack [163], defensive efficiency [163], attack noise [163], number or time of disruptions [163], [188].
- **Governance and Compliance metrics:**
  - -- **Compliance metrics:** Since compliance to all regulatory guidelines and standards is hardly possible, it is useful to define compliance goals and accordingly appropriate metrics. Additionally, it can be of value to provide measures for compliance audits. *Examples:* Number of policy violations [30], [57], percentage of systems with tested security controls
  - -- **Maturity metrics:** Usually refers to the level of maturity as described in Section V-D2

The classification is not always strict and lines are blurry. For example, some people metrics might be classified as governance and compliance metrics.

To overcome the many problems with current security metrics, a few things should be considered. It is important to clearly define what the objectives of the metrics are and how their success/failure can be measured. Some SOC vendors use the S.M.A.R.T. management objectives framework developed by Doran [196], as a guide to develop metrics [195], [197].

VI. CHALLENGES

Throughout Sections IV and V, we focused on our first research question in terms of the state-of-the-art of a SOC. We already mentioned a series of challenges that impose the development and improvement of SOCs. Within the following paragraphs, we now briefly describe these challenges in response to our second research questions regarding the challenges needing to be solved to advance the field of SOC research. Every SOC naturally faces different challenges depending on its operating model, architecture, scope, or size. However, we derive several challenges applicable to most SOCs. Although many of the challenges are somewhat related, we try to describe them as independently as possible and along with the PPTGC framework, which we followed throughout this work. Figure 8 gives an overview of these challenges and highlights some relevant dependencies between them.

A. PEOPLE

1) Monotonous and demotivating tasks

As mentioned earlier, there is a vast number of alerts coming into the SOC every second. Even though tools are trying to display only true positive alerts, the number of false positives is still very high. Every incoming alert needs to be manually investigated by an analyst, most of the time at tier 1 level. The analysts need to open the alert and determine whether it is a false positive or not. Sometimes it takes seconds to come to a decision, sometimes minutes or even hours. Performing this task over and over again is very repetitive and monotonous as several works have shown previously [8], [11], [16], [32]. Additionally, this task is very demanding on a security analysts' capability of information processing and analytical reasoning due to the vast amount of data [94]. Although doing a very monotonous task, the analysts are working under high pressure and have high responsibility. Any incorrect decision can lead to unpredictable consequences for the company if

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3045514, IEEE Access

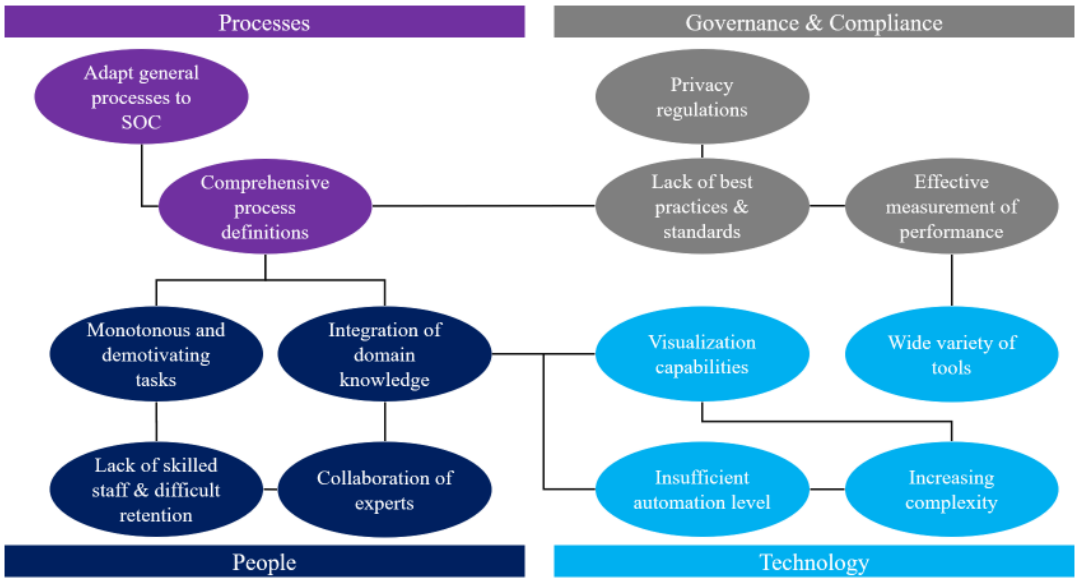

FIGURE 8. Challenges for SOC research.

an incident unfolds. This issue, combined with time pressure faced in a SOC and the lack of creativity needed to solve the tasks causes analyst boredom, which finally could lead to burnout [8], [16]. Additionally, the non-challenging nature of tasks and the fact that most analysts need to follow predefined procedures all the time limits their ability to react to new and innovative threats in the future [11]. An exciting direction for retaining SOC analysts' motivation might be the inclusion of gamification aspects into the SOC operations. When the tasks become too mundane and frustrating for the SOC employees, it is tough to retain skilled staff [30], [32]. This amplifies the next challenge in the context of people within SOCs.

2) Lack of skilled staff and difficult retention

A very severe challenge companies will continue to face is the lack of skilled security staff [3], [8], [80]. In addition to that, the nature of the work as highlighted in the previous chapter leads to a high turnover rate of personnel. This means companies have to spend many resources on training new staff, unless they are willing to spend their resources on retaining the staff. We identified some options in literature to retain staff like training or after-work activities (Section V-A2). However, the lack of job-related security training is still apparent [6], [32]. Practical experience is required to perform data triage, but it is considered hard to get the practical training and experience in the first place [98]. Tier 1 analysts are not always empowered to perform more challenging tasks to improve their knowledge and experience. A lack of feedback from senior analysts intensifies the challenge and can cause frustration [11]. Some technological solutions are trying to overcome the problem by capturing past activities and decisions from experienced staff so the more junior can profit and learn from this data. However, capturing the tacit knowledge involved in the decision-making is a challenging task [98]. Despite this fact, some approaches, especially from Human-Computer Interface (HCI) and respective communities, have been trying to capture the reasoning behind analytical decisions for quite some time [198]. These aspects can help to improve SOCs' working conditions.

3) Collaboration of experts

Collaboration between analysts is still rare, and analysts usually work on a problem independently [12]. This challenge might either stem from the time pressure the staff is facing or the lack of appropriate collaboration platforms. The same applies to communication, which is mostly carried out directly between analysts. This type of communication is necessary but also time-consuming and inefficient [97]. Once again, the absence of an appropriate communication platform for SOC-specific requirements reduces the staff's interactions overall. Only with the appropriate means to collaborate and communicate SOC analysts from any tier can learn from each other and, therefore, improve their efficiency and motivation.

4) Integration of domain knowledge

Identifying threats and incidents gets increasingly harder as IT infrastructures grow and expand from the cyberspace into the physical world, for example through the use of cyber-physical systems [83]. Current automated threat detection tools work pretty well for detecting well-known attacks, as they operate based on signatures and attack patterns [13], [159]. Therefore, unknown situations remain undetected as no rule is defined for them yet. To detect unknown attacks, it is inevitable to include domain knowledge of security experts and even non-security experts. Security experts are valuable as they have a deep understanding of security routines, requirements and have already taken countermeasures. However, non-security experts (e.g. engineers) become more

and more indispensable as they have the knowledge which is often necessary to decide whether an alert or the reported behavior is malicious or benign, especially in the context of cyber-physical systems.

Additionally, it is necessary to communicate knowledge of automated analyzes like machine learning models to the SOC staff to understand and comprehend what their analyses algorithms learned. Tying human experts and machines closer together and providing them processes and technologies to transfer knowledge in either direction is a crucial challenge for SOCs. Only when we succeed in leveraging both domain knowledge from humans and explicit knowledge from machines, we face the next generation of cyber threats.

B. PROCESSES

1) Comprehensive process definitions

The review showed that there is only very little literature on the processes within a SOC. As these processes are the core of understanding SOCs and deploying them effectively, the lack of precisely defined processes hinders academia from entirely comprehending what organizations are doing within a SOC. Thus, room for small improvements, let alone innovations, are very hard to identify on an abstract level. This might be the reason for the imbalanced results regarding processes and technology. As there is no abstract, high-level understanding of a SOC's processes, many researchers focus on trying to improve technologies that might be useful with no clear understanding of which specific process or task of a SOC needs improvement. Also, having a clear understanding of a SOC's processes, tasks, and interfaces requires the integration with other business processes. This blind spot needs to be closed by academia to understand the processes running in SOCs. Only then will it be possible to advance the current proliferation that is imminent in SOCs in a sustainable manner. Especially "post-incident activity" is barely mentioned in SOC literature, although it is of great importance as it mainly deals with learning and iterative improvement.

2) Adapt general processes to SOC

Several security standards, regulations, and frameworks [123], [124] define general security-related processes that give rise to the assumption that these can be related at least partially to SOC. These can therefore serve as a basis for a SOC specific process landscape. However, our analysis has not identified any academic literature dealing with how these processes can be related to SOCs. Further research should aim to identify the aspects that apply to SOCs, adapt those to SOC, and extend them by SOC specifics. This could lead simply to a more comprehensive definition and understanding of the processes.

C. TECHNOLOGY

1) Increasing complexity

We see three major challenges for SOCs resulting from the increased complexity of the IT and OT environment in a company: First, the infrastructure is becoming more complicated and intertwined, making it difficult to maintain situational awareness and a cohesive overview. Managers and analysts have poor visibility into the network because they cannot keep track of all the devices in the network [7]. Second, the data captured from the infrastructure is as heterogeneous as its sources [22], [32], [94], making it hard to process, analyze, understand, and link. It also impedes the discovery of whether an event is part of a bigger attack [11]. Third, having more data sources increases the overall number of events and, in many cases, the number of false-positive alerts. It is often mentioned that there is too much (useless) data in general [22], and too many (false positive) alerts [9], [25], [32], [159], [164]. Analysts are overloaded with a high volume of such alerts and face a typical "needle in a haystack" problem when trying to filter the noise [12], [159]. There is not much discussion about the negative impact of false positives on SOCs, although there are controversial opinions like Kokulu et al. [7].

2) Wide variety of tools

In many SOCs, the previous problem is approached by implementing and deploying various SOC tools, for example, a SIEM system. However, deploying a variety of tools does not solve the overall problem, at least not immediately. Tools need to be configured and maintained, which is a time- and resource-consuming process [159]. If tools are not maintained properly, they increase the amount of data and false positives to be dealt with for the analysts. Different tools are necessary because most of them only offer a solution to a specific problem. Therefore, a variety of tools is needed to cover all capabilities within a SOC. Integrating them so that they can run smoothly together poses a further challenge [4], [23]. For example, tools typically only cover the standard IT technologies and have no visibility into operational technology. Some tools also suffer from poor usability and regular malfunctioning [7]. This makes the job for analysts much more complicated than it should be and has a negative effect on the detection rate of a SOC. Lastly, tools might be chosen for compliance or budget reasons, not because they are helpful or practical [15].

3) Visualization capabilities

Having the right visualization capabilities is another challenge. Generally, there is too much data to be able to visualize it properly [173]. Visualizations need to be simple and easily accessible, as well as precise and informative [12]. However, there is no perfect solution, and a trade-off between these two requirements is necessary. Selecting the right visualization technique is rigid and very dependent on the context and tasks that should be solved with the visualization.

Nonetheless, appropriate visualizations are crucial for an efficient and effective SOC team. Additionally, visualizations are a great deal to support the transfer of knowledge between humans and machines. They can serve as an intermediary allowing analysts to understand machine learning models and

improve automated analyses by implicit human input and domain knowledge [199].

4) Insufficient level of automation

There is also an insufficient level of automation of SOC components [7]. Many of the tasks carried out in a SOC, e.g. threat hunting, scanning alerts, or responding to incidents, still require a significant portion of manual work in a context where human resources are scarce. The insufficient level of automation is caused by the fact that analysts' tasks are hard to automate. However, automation is needed to reduce the manual and repetitive tasks many SOC analysts have to perform today. There is already a considerable body of literature focusing on the applicability of machine learning techniques to automate the detection of attacks. Unfortunately, many techniques prove to only be successful under certain conditions or for specific types of attacks. These techniques and their comprehensiveness and effectiveness in detecting attacks need to be compared. More user studies should be conducted to evaluate their usability. Additionally, machine learning approaches produce a high number of false positives. Determining whether an alert is real requires further investigation by the analysts based on tacit knowledge.

D. GOVERNANCE AND COMPLIANCE

1) Effective measurement of SOC performance

Even though measuring a SOC's performance and effectiveness is one of the most important governance tasks, many of the currently established metrics are considered inefficient [7], [171]. Additionally, if the metrics are too focused on performance, analysts might be incentivized to work for general statistics [16], [200], as described in Section V-D3. This fuels the need for uniform metrics proving the value of a SOC to management.

2) Lack of best practices & standards

Some SOC capabilities, like incident management, are already very advanced. Consequently, many standards and industry best practices can be implemented for these specific capabilities. They can then be audited to see whether they adhere to the standard. Other capabilities are less advanced and have no universal standard. Unfortunately, there is no holistic SOC standard or framework, making it hard to audit a cohesive and complex SOC. The lack of best practices also means that there is no actual decision support for organizations. Decision-makers struggle to choose the right operating model, the right scope, the right capabilities, and even the right tools to support the capabilities. Best practices, either from academia or industry, are needed to enable companies to set up SOCs fitted to their needs. Currently, many guidelines on SOCs are written by security vendors [77], [190]. Despite their valuable contributions to the development of SOCs, they are biased to a certain extent, which further highlights the need for independent standards and impartial industry guidelines. Researchers alone cannot solve this problem. They need to collaborate with regulators, standardization entities, and industry expertise.

3) Privacy regulations

Existing privacy standards and regulations leave many questions regarding collecting and analyzing data unanswered. The company needs to determine if they capture sensitive information, if they could avoid it, and how they can anonymize or at least pseudonymize the data without losing their value. However, there is not much work providing guidelines to decide whether data contains sensitive information or not and even less work giving practical advice on the anonymization of data and still detecting incidents using the anonymized data. Another challenge on the rise is to define the right policies and procedures.

VII. CONCLUSION

The main objective of this work is to identify and compile the current state-of-the-art of SOCs. To thoroughly achieve this goal, we needed to explore the frontiers of academic literature on the topic. This work's central part consists of a comprehensive literature review on SOCs from a pure research viewpoint. Its objective is to take a close look at SOCs in general but also include their components. The survey is conducted systematically to avoid the exclusion of any relevant information. We planned the review, meaning that the used search terms included various keywords and terms relevant to SOCs. This work includes as many aspects of SOCs as possible. Using the PPTGC framework, various components of a SOC are generally classified into either people, processes, technology, or governance and compliance. We describe these SOC components as currently defined in the literature.

We use the relevant literature and the defined state-of-the-art to identify major challenges that hinder further development and innovation for SOCs. The challenges can also serve as a guideline for future research aiming to improve SOCs. Regarding the people working in a SOC, we see a major challenge in recruiting and retaining staff. Training and Awareness play an essential role in addressing this challenge while also helping to increase the company's overall security posture. When looking at the various processes in a SOC, it is imperative to integrate them with other processes across the whole organization. Analyzing processes regarding SOCs, we can also see that academia and practice lack a thorough and comprehensive definition of the specific processes included in a SOC and their interactions. Without a proper definition of processes, it might not be possible to advance the current state-of-the-art. Technologies promise relief from many repetitive tasks in a SOC; however, most of them are not advanced enough to deliver on the expectations and hype they have created. To maximize the potential of deployed technological solutions, they need to be aligned with and integrated with the rest of an organization's technological infrastructure. Lastly, an immaturity of SOC governance and compliance aspects has been identified. Compared to

people or technological components of a SOC, comprehensive standards and industry-specific guidelines are lacking. This kind of immaturity generally impedes security audits and overall SOC assessments. The lack of standards also prevents various SOC components from advancing since a common baseline of the status-quo has not yet been agreed upon. As we have mainly analyzed academic literature, to provide a more comprehensive picture we aim to include a more practical view by considering information such as case studies in future research.

Concluding, SOCs surely help companies to be prepared for cyber-attacks. However, they need to be planned thoroughly, implemented, and integrated very carefully, assessed regularly, and improved continually to unveil their full potential. If done correctly, they improve companies' ability to prevent hacks, financial losses, and personal data breaches.

REFERENCES

[1] Accenture and Ponemon Institute LLC. The cost of cybercrime, 2018.

[2] 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, pages 2253–2262, Kauai, 2015. IEEE.

[3] S. Radu. Comparative analysis of security operations centre architectures; proposals and architectural considerations for frameworks and operating models. In Innovative Security Solutions for Information Technology and Communications, volume 10006 of Lecture Notes in Computer Science, pages 248–260. Springer International Publishing, Cham, 2016.

[4] R. Bidou, J. Bourgeois, and F. Spies. Towards a global security architecture for intrusion detection and reaction management. In Information Security Applications, volume 2908 of Lecture Notes in Computer Science, pages 111–123. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[5] S. Kowtha, L. Nolan, and R. Daley. Cyber security operations center characterization model and analysis. In 2012 IEEE Conference on Technologies for Homeland Security (HST), pages 470–475, Waltham, 2012. IEEE.

[6] A. Ganame, J. Bourgeois, R. Bidou, and F. Spies. A global security architecture for intrusion detection on computer networks. Computers & Security, 27(1-2):30–47, 2008.

[7] F. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G. Ahn. Matched and mismatched socs. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security - CCS '19, pages 1955–1970, New York, New York, USA, 2019. ACM Press.

[8] B. Hámornik and C. Krasznay. A team-level perspective of human factors in cyber security: Security operations centers. In D. Nicholson, editor, Advances in Human Factors in Cybersecurity, volume 593 of Advances in Intelligent Systems and Computing, pages 224–236. Springer International Publishing, Cham, 2018.

[9] A. Sopan, M. Berninger, M. Mulakaluri, and R. Katakam. Building a machine learning model for the soc, by the input from the soc, and analyzing it for the soc. In 2018 IEEE Symposium on Visualization for Cyber Security (VizSec), pages 1–8, Berlin, 2018. IEEE.

[10] V. Rooney and S. Foley. What you can change and what you can't: Human experience in computer network defenses. In N. Gruschka, editor, Secure IT Systems, volume 11252 of Lecture Notes in Computer Science, pages 219–235. Springer International Publishing, Cham, 2018.

[11] 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, volume 11391 of Lecture Notes in Computer Science, pages 136–142. Springer International Publishing, Cham, 2019.

[12] A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, and C. Ponchel. 3d cybercop: A collaborative platform for cybersecurity data analysis and training. In Y. Luo, editor, Cooperative Design, Visualization, and Engineering, volume 11151 of Lecture Notes in Computer Science, pages 176–183. Springer International Publishing, Cham, 2018.

[13] J. Goodall, E. Ragan, C. Steed, J. Reed, G. Richardson, K. Huffer, R. Bridges, and J. Laska. Situ: Identifying and explaining suspicious behavior in networks. IEEE transactions on visualization and computer graphics, 25(1):204–214, 2018.

[14] S. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann. A tale of three security operation centers. In Proceedings of the 2014 ACM Workshop on Security Information Workers - SIW '14, pages 43–50, New York, New York, USA, 2014. ACM Press.

[15] S. Sundaramurthy, M. Wesch, X. Ou, J. McHugh, S. Rajagopalan, and A. Bardas. Humans are dynamic - our tools should be too. IEEE Internet Computing, 21(3):40–46, 2017.

[16] S. Sundaramurthy. An Anthropological Study of Security Operations Centers to Improve Operational Efficiency. Dissertation, University of South Florida, 2017.

[17] J. Brown, S. Greenspan, and R. Biddle. Incident response teams in it operations centers: the t-tocs model of team functionality. Cognition, Technology & Work, 18(4):695–716, 2016.

[18] D. Tranfield, D. Denyer, and P. Smart. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3):207–222, 2003.

[19] J. Webster and R. Watson. Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, 26(2):13–23, 2002.

[20] Y. Levy and T. J. Ellis. A systems approach to conduct an effective literature review in support of information systems research. Informing Science: The International Journal of an Emerging Transdiscipline, 9:181–212, 2006.

[21] C. Okoli. A guide to conducting a standalone systematic literature review. Communications of the Association for Information Systems, 37(43):879–910, 2015.

[22] A. Madani, S. Rezayi, and H. Gharaee. Log management comprehensive architecture in security operation center (soc). In 2011 International Conference on Computational Aspects of Social Networks (CASoN), pages 284–289, Salamanca, 2011. IEEE.

[23] M. Mutemwa, J. Mtsweni, and L. Zimba. Integrating a security operations centre with an organization's existing procedures, policies and information technology systems. In 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), pages 1–6, Plaine Magnien, 2018. IEEE.

[24] N. Miloslavskaya. Analysis of siem systems and their usage in security operations and security intelligence centers. In Biologically Inspired Cognitive Architectures (BICA) for Young Scientists, volume 636 of Advances in Intelligent Systems and Computing, pages 282–288. Springer International Publishing, Cham, 2018.

[25] N. Miloslavskaya, A. Tolstoy, and S. Zapechnikov. Taxonomy for unsecure big data processing in security operations centers. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pages 154–159, Vienna, 2016. IEEE.

[26] C. Han, S. Park, and S. Lee. The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. International Journal of Critical Infrastructure Protection, 26:100312, 2019.

[27] J. Kaplan, T. Bailey, C. Rezek, D. O'Halloran, and A. Marcus. Engage attackers with active defense. In Beyond Cybersecurity, pages 123–139. John Wiley & Sons, Inc, Hoboken, NJ, USA, 2015.

[28] G. Wang, Z. Yan, and J. Chen. A method for software trusted update on network security equipment. IOP Conference Series: Materials Science and Engineering, 569, 2019.

[29] A. Shah, K. Farris, R. Ganesan, and S. Jajodia. Vulnerability selection for remediation: An empirical analysis. Journal of Defense Modeling & Simulation, 21(4):154851291987412, 2019.

[30] C. Onwubiko. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pages 1–10, London, 2015. IEEE.

[31] C. Onwubiko and K. Ouazzane. Cyber onboarding is 'broken'. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pages 1–13, Oxford, 2019. IEEE.

[32] S. Mansfield-Devine. Creating security operations centres that work. Network Security, 2016(5):15–18, 2016.

[33] M. Majid and K. Ariffi. Success factors for cyber security operation center (soc) establishment. In Proceedings of the Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology, INCITEST 2019, 18 July 2019, Bandung, Indonesia, pages 1–11, Bandung, 2019. EAI.

[34] J. Bourgeois, A. Ganame, I. Kotenko, and A. Ulanov. Software environment for simulation and evaluation of a security operation center. In

Information Fusion and Geographic Information Systems, Lecture Notes in Geoinformation and Cartography, pages 111–127. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[35] A. Bialas, M. Michalak, and B. Flisiuk. Anomaly detection in network traffic security assurance. In Engineering in Dependability of Computer Systems and Networks, volume 987 of Advances in Intelligent Systems and Computing, pages 46–56. Springer International Publishing, Cham, 2020.

[36] D. Kelley and R. Moritz. Best practices for building a security operations center. Information Systems Security, 14(6):27–32, 2006.

[37] L. Aijaz, B. Aslam, and U. Khalid. Security operations center — a need for an academic environment. In 2015 World Symposium on Computer Networks and Information Security (WSCNIS), pages 1–7, Hammamet, 2015. IEEE.

[38] O. Podzins and A. Romanovs. Why siem is irreplaceable in a secure it environment? In 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), pages 1–5, Vilnius, 2019. IEEE.

[39] N. Miloslavskaya. Security intelligence centers for big data processing. In 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pages 7–13, Prague, 2017. IEEE.

[40] J. Bourgeois and R. Syed. Managing security of grid architecture with a grid security operation center. In Proceedings of the International Conference on Security and Cryptography, pages 403–408, Milan, 2009. Science and and Technology Publications.

[41] R. Syed, J. Pazardzievska, and J. Bourgeois. Fast attack detection using correlation and summarizing of security alerts in grid computing networks. The Journal of Supercomputing, 62(2):804–827, 2012.

[42] R. Syed, M. Syrame, and J. Bourgeois. Protecting grids from cross-domain attacks using security alert sharing mechanisms. Future Generation Computer Systems, 29(2):536–547, 2013.

[43] A. Ganame, J. Bourgeois, R. Bidou, and F. Spies. Evaluation of the intrusion detection capabilities and performance of a security operation center. In Proceedings of the International Conference on Security and Cryptography, pages 48–55, Setúbal, 2006. Science and and Technology Publications.

[44] X. Hu and C. Xie. Security operation center design based on d-s evidence theory. In 2006 International Conference on Mechatronics and Automation, pages 2302–2306, Luoyang, 2006. IEEE.

[45] S. Yuan and C. Zou. The security operations center based on correlation analysis. In 2011 IEEE 3rd International Conference on Communication Software and Networks, pages 334–337, Xi'an, 2011. IEEE.

[46] E. Amoroso. Cyber attacks: awareness. Network Security, 2011(1):10–16, 2011.

[47] G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, M. Carolan, D. Conroy, K. Boettinger, M. Gall, G. Brost, C. Ponchel, M. Haustein, H. Kaufmann, K. Theuerkauf, and P. Olli. A collaborative cyber incident management system for european interconnected critical infrastructures. Journal of Information Security and Applications, 34:166–182, 2017.

[48] T. Tafazzoli and H. Gharaee Garakani. Security operation center implementation on openstack. In 2016 8th International Symposium on Telecommunications (IST), pages 766–770, Tehran, 2016. IEEE.

[49] J. Li, C. Hsieh, and H. Lin. A hierarchical mobile-agent-based security operation center. International Journal of Communication Systems, 26(12):1503–1519, 2013.

[50] J. Li and C. Hsieh. Implementation of the distributed hierarchical security operation center using mobile agent group. In 2010 International Symposium on Computer, Communication, Control and Automation (3CA), pages 79–82, Tainan, 2010. IEEE.

[51] G. Chamiekara, M. Cooray, L. Wickramasinghe, Y. Koshila, K. Abeywardhana, and A. Senarathna. Autosoc: A low budget flexible security operations platform for enterprises and organizations. In 2017 National Information Technology Conference (NITC), pages 100–105, Colombo, 2017. IEEE.

[52] E. Falk, S. Repcek, B. Fiz, S. Hommes, R. State, and R. Sasnauskas. Vsoc - a virtual security operating center. In 2017 IEEE Global Communications Conference, pages 1–6, Singapore, 2017. IEEE.

[53] U. Glasser, P. Jackson, A. Araghi, and H. Shahir. Intelligent decision support for marine safety and security operations. In 2010 IEEE International Conference on Intelligence and Security Informatics, pages 101–107, Vancouver, 2010. IEEE.

[54] B. AlSabbagh and S. Kowalski. A framework and prototype for a socio-technical security information and event management system (st-siem). In 2016 European Intelligence and Security Informatics Conference (EISIC), pages 192–195, Uppsala, 2016. IEEE.

[55] F. Sailhan and J. Bourgeois. Log-based distributed intrusion detection for hybrid networks. In Proceedings of the 4th annual workshop on Cyber security and informaiton intelligence research developing strategies to meet the cyber security and information intelligence challenges ahead - CSIIRW '08, page 1, New York, New York, USA, 2008. ACM Press.

[56] P. Bienias, G. Kolaczek, and A. Warzynski. Architecture of anomaly detection module for the security operations center. In 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pages 126–131, Napoli, 2019. IEEE.

[57] A. Chowdhary, D. Huang, G. Ahn, M. Kang, A. Kim, and A. Velazquez. Sdnsoc: Object oriented sdn framework. In Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization - SDN-NFVSec '19, pages 7–12, New York, New York, USA, 2019. ACM Press.

[58] D. Crooks and L. Valsan. Wlcg security operations centre working group. Proceedings of Science, 1(1):1–25, 2017.

[59] D. Crooks, L. Vâlsan, K. Mohammad, S. McKee, P. Clark, A. Boutcher, A. Padée, M. Wójcik, H. Giemza, and B. Kreukniet. Operational security, threat intelligence & distributed computing: the wlcg security operations center working group. EPJ Web of Conferences, 214, 2019.

[60] D. Crooks and L. Vâlsan. Building a minimum viable security operations centre for the modern grid environment. In Proceedings of International Symposium on Grids & Clouds 2019 — PoS(ISGC2019), page 010, Trieste, Italy, 2019. Sissa Medialab.

[61] Paul Danquah. Security operations center: A framework for automated triage, containment and escalation. Journal of Information Security, 11(04):225–240, 2020.

[62] D. Forte. An inside look at security operation centres. Network Security, 2003(5):11–12, 2003.

[63] P. Jacobs, A. Arnab, and B. Irwin. Classification of security operation centers. In 2013 Information Security for South Africa, Johannesburg, 2013. IEEE.

[64] D. Forte. State of the art security management. Computer Fraud & Security, 2009(10):17–18, 2009.

[65] N. Miloslavskaya. Security operations centers for information security incident management. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pages 131–136, Vienna, 2016. IEEE.

[66] D. Feher and H. Nguyen. Security concerns towards security operations centers. In 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), pages 000273–000278, Timisoara, 2018. IEEE.

[67] A. Shah, R. Ganesan, and S. Jajodia. A methodology for ensuring fair allocation of csoc effort for alert investigation. International Journal of Information Security, 18(2):199–218, 2019.

[68] M. Khalili, M. Zhang, D. Borbor, L. Wang, N. Scarabeo, and M. Zamor. Monitoring and improving managed security services inside a security operation center. ICST Transactions on Security and Safety, 5(18):157413, 2019.

[69] C. Crowley and J. Pescatore. Sans 2018 security operations center survey, 2018.

[70] G. Bhatt. Knowledge management in organizations: Examining the interaction between technologies, techniques, and people. Journal of Knowledge Management, 5(1):68–75, 2001.

[71] R. Ruefle. Defining computer security incident response teams, 2007.

[72] D. Robb. How to manage a security operations center, 2019.

[73] M. Vielberth and G. Pernul. A security information and event management pattern. In 12th Latin American Conference on Pattern Languages of Programs (SLPLoP). 2018.

[74] F. Alruwaili and T. Gulliver. Socaas: Security operations center as a service for cloud computing environments. International Journal of Cloud Computing and Services Science, 3(2):87–96, 2014.

[75] C. Zimmerman. Ten strategies of a world-class cybersecurity operations center, 2014.

[76] Huntsman Security. Choosing a soc service model: The key considerations, 2018.

[77] J. Muniz, G. McIntyre, and N. AlFardan. Security operations center: Building, operating, and maintaining your SOC. Cisco Press, Indianapolis, Indiana, 2015.

[78] LINKBYNET. Outsourced soc vs. internal soc: How to choose?, 2018.

[79] C. Olt. Establishing security operation centers for connected cars. ATZelectronics worldwide, 14(5):40–43, 2019.

[80] C. DeCusatis, R. Cannistra, A. Labouseur, and M. Johnson. Design and implementation of a research and education cybersecurity operations center. In Cybersecurity and Secure Information Systems, volume 33 of Advanced Sciences and Technologies for Security Applications, pages 287–310. Springer International Publishing, Cham, 2019.

[81] R. Ganesan, A. Shah, S. Jajodia, and H. Cam. Optimizing alert data management processes at a cyber security operations center. In Adversarial and Uncertain Reasoning for Adaptive Cyber Defense, volume 11830 of Lecture Notes in Computer Science, pages 206–231. Springer International Publishing, Cham, 2019.

[82] C. Zhong, J. Yen, P. Liu, and R. Erbacher. Learning from experts' experience: Toward automated cyber security data triage. IEEE Systems Journal, 13(1):603–614, 2019.

[83] C. Islam, M. Babar, and S. Nepal. Automated interpretation and integration of security tools using semantic knowledge. In Advanced Information Systems Engineering, volume 11483 of Lecture Notes in Computer Science, pages 513–528. Springer International Publishing, Cham, 2019.

[84] Y. Kanemoto, K. Aoki, M. Iwamura, J. Miyoshi, D. Kotani, H. Takakura, and Y. Okabe. Detecting successful attacks from ids alerts based on emulation of remote shellcodes. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), pages 471–476, Milwaukee, 2019. IEEE.

[85] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap. Challenges and performance metrics for security operations center analysts: a systematic review. Journal of Cyber Security Technology, 76(3):1–28, 2019.

[86] C. Zhong, J. Yen, P. Liu, R. Erbacher, C. Garneau, and B. Chen. Studying analysts' data triage operations in cyber defense situational analysis. In Theory and Models for Cyber Situation Awareness, volume 10030 of Lecture Notes in Computer Science, pages 128–169. Springer International Publishing, Cham, 2017.

[87] C. Zhong, J. Yen, P. Liu, and R. Erbacher. Automate cybersecurity data triage by leveraging human analysts' cognitive process. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pages 357–363, 2016.

[88] C. Zhong, T. Lin, P. Liu, J. Yen, and K. Chen. A cyber security data triage operation retrieval system. Computers & Security, 76:12–31, 2018.

[89] A. Pingle, A. Piplai, S. Mittal, A. Joshi, J. Holt, and R. Zak. Relext: Relation extraction using deep learning approaches for cybersecurity knowledge graph improvement, 2019.

[90] A. Shah, R. Ganesan, S. Jajodia, and H. Cam. Adaptive reallocation of cybersecurity analysts to sensors for balancing risk between sensors. Service Oriented Computing and Applications, 12(2):123–135, 2018.

[91] A. Shah, R. Ganesan, S. Jajodia, and H. Cam. A two-step approach to optimal selection of alerts for investigation in a csoc. IEEE Transactions on Information Forensics and Security, 14(7):1857–1870, 2018.

[92] S. Sundaramurthy, A. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and R. Rajagopalan. A human capital model for mitigating security analyst burnout. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), pages 347–359, Ottawa, 2015. USENIX Association.

[93] T. Sander and J. Hailpern. Ux aspects of threat information sharing platforms. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security - WISCS '15, pages 51–59, New York, New York, USA, 2015. ACM Press.

[94] T. Lin, C. Zhong, J. Yen, and P. Liu. Retrieval of relevant historical data triage operations in security operation centers. In From Database to Cyber Security, volume 11170 of Lecture Notes in Computer Science, pages 227–243. Springer International Publishing, Cham, 2018.

[95] A. Applebaum, S. Johnson, M. Limiero, and M. Smith. Playbook oriented cyber response. In 2018 National Cyber Summit (NCS), pages 8–15, Huntsville, 2018. IEEE.

[96] Salvador Llopis Sanchez, Robert Mazzolin, Ioannis Kechaoglou, Douglas Wiemer, Wim Mees, and Jean Muylaert. Cybersecurity space operation center: Countering cyber threats in the space domain. In Kai-Uwe Schrogl, editor, Handbook of Space Security, pages 921–939. Springer International Publishing, Cham, 2020.

[97] C. Zhong, A. Alnusair, B. Sayger, A. Troxell, and J. Yao. Aoh-map: A mind mapping system for supporting collaborative cyber security analysis. In 2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), pages 74–80, Las Vegas, 2019. IEEE.

[98] A. Shah, R. Ganesan, S. Jajodia, and H. Cam. Optimal assignment of sensors to analysts in a cybersecurity operations center. IEEE Systems Journal, 13(1):1060–1071, 2019.

[99] A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, and C. Ponchel. From cyber security activities to collaborative virtual environments practices through the 3d cybercop platform. In Information Systems Security, volume 11281 of Lecture Notes in Computer Science, pages 272–287. Springer International Publishing, Cham, 2018.

[100] Alien Vault. How to build a security operations center (on a budget), 2017.

[101] O. Cassetto. Security operations center roles and responsibilities, 2019.

[102] International Information System Security Certification Consortium. Strategies for building and growing strong cybersecurity teams: Cybersecurity workforce study, 2019.

[103] A. Lin, H. Wong, and T. Wu. Enhancing interoperability of security operation center to heterogeneous intrusion detection systems. In Proceedings of the 39th Annual 2005 International Carnahan Conference on Security Technology, pages 216–221, Las Palmas, 2005. IEEE.

[104] S. Bhatt, P. Manadhata, and L. Zomlot. The operational role of security information and event management systems. IEEE Security & Privacy, 12(5):35–41, 2014.

[105] D. Zhang and D. Zhang. The analysis of event correlation in security operations center. In 2011 Fourth International Conference on Intelligent Computation Technology and Automation, pages 1214–1216, Guangdong, 2011. IEEE.

[106] Z. Qu and L. Wang. The design of a correlation analysis engine model based on carma_ve algorithm. In 2009 IEEE International Symposium on IT in Medicine & Education, pages 1267–1270, Jinan, 2009. IEEE.

[107] B. Bösch. Approach to enhance the efficiency of security operation centers to heterogeneous ids landscapes. In Critical Information Infrastructures Security, volume 7722 of Lecture Notes in Computer Science, pages 1–9. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[108] F. Sailhan, J. Bourgeois, and V. Issarny. A security supervision system for hybrid networks. In R. Lee, editor, Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, volume 149 of Studies in Computational Intelligence, pages 137–149. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[109] M. Verma and R. Bridges. Defining a metric space of host logs and operational use cases. In 2018 IEEE International Conference on Big Data (Big Data), pages 5068–5077, Seattle, 2018. IEEE.

[110] M. Alam, S. Malik, Q. Javed, A. Khan, S. Khan, A. Anjum, N. Javed, A. Akhunzada, and M. Khan. Formal modeling and verification of security controls for multimedia systems in the cloud. Multimedia Tools and Applications, 76(21):22845–22870, 2017.

[111] R. Bridges, M. Iannacone, J. Goodall, and J. Beaver. How do information security workers use host data? a summary of interviews with security analysts, 2018.

[112] B. Song, J. Choi, S. Choi, and J. Song. Visualization of security event logs across multiple networks and its application to a csoc. Cluster Computing, 22(S1):1861–1872, 2019.

[113] David Weissman and Anura Jayasumana. Integrating iot monitoring for security operation center. In 2020 Global Internet of Things Summit (GIoTS), pages 1–6, Dublin, 2020. IEEE.

[114] M. Nabil, S. Soukainat, A. Lakbabi, and O. Ghizlane. Siem selection criteria for an efficient contextual security. In 2017 International Symposium on Networks, Computers and Communications (ISNCC), pages 1–6, Marrakech, 2017. IEEE.

[115] Y. Cheng, C. Chen, C. Chiang, J. Wang, and C. Laih. Generating attack scenarios with causal relationship. In 2007 IEEE International Conference on Granular Computing (GRC 2007), page 368, Fremont, 2007. IEEE.

[116] G. Gonzalez Granadillo, M. El-Barbori, and H. Debar. New types of alert correlation for security information and event management systems. In 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pages 1–7, Larnaca, 2016. IEEE.

[117] Chadni Islam, Muhammad Ali Babar, and Surya Nepal. A multi-vocal review of security orchestration. ACM Computing Surveys, 52(2):1–45, 2019.

[118] Kieran Hughes, Kieran McLaughlin, and Sakir Sezer. Dynamic countermeasure knowledge for intrusion response systems. In 2020 31st Irish Signals and Systems Conference (ISSC), pages 1–6, Letterkenny, Ireland, 2020. IEEE.

[119] Selina Y. Cho, Jassim Happa, and Sadie Creese. Capturing tacit knowledge in security operation centers. IEEE Access, 8:42021–42041, 2020.

[120] Masoud Hayeri Khyavi. Isms role in the improvement of digital forensics related process in soc's.

[121] Wenzhuo Yang and Kwok-Yan Lam. Automated cyber threat intelligence reports classification for early warning of cyber attacks in next generation soc. In Jianying Zhou, Xiapu Luo, Qingni Shen, and Zhen Xu, editors, Information and Communications Security, volume 11999 of Lecture Notes in Computer Science, pages 145–164. Springer International Publishing, Cham, 2020.

[122] Chadni Islam, Muhammad Ali Babar, and Surya Nepal. Architecture-centric support for integrating security tools in a security orchestration platform. In Anton Jansen, Ivano Malavolta, Henry Muccini, Ipek Ozkaya, and Olaf Zimmermann, editors, Software Architecture, volume 12292 of Lecture Notes in Computer Science, pages 165–181. Springer International Publishing, Cham, 2020.

[123] International Organization for Standardization. Iso/iec 27035-1:2016: Information technology - security techniques - information security incident management - part 1: Principles of incident management, 2016.

[124] P. Cichonski, T. Millar, T. Grance, and K. Scarfone. Computer security incident handling guide: Special publication 800-61 revision 2, 2012.

[125] K. Kent and M. Souppaya. Guide to computer security log management: Recommendations of the national institute of standards and technology, 2006.

[126] F. Osinga. Science, Strategy and War: The Strategic Theory of John Boyd. Routledge, London, 2007.

[127] C. Falk and J. Dykstra. Sonification with music for cybersecurity situational awareness. In Proceedings of the 25th International Conference on Auditory Display (ICAD 2019), pages 50–55, Newcastle upon Tyne, United Kingdom, 2019. Department of Computer and Information Sciences, Northumbria University.

[128] D. Ambawade, P. Kedar, and J. Bakal. A comprehensive architecture for correlation analysis to improve the performance of security operation center. In Innovations in Computer Science and Engineering, volume 8 of Lecture Notes in Networks and Systems, pages 205–216. Springer Singapore, Singapore, 2017.

[129] M. Almukaynizi, E. Marin, E. Nunes, P. Shakarian, G. Simari, D. Kapoor, and T. Siedlecki. Darkmention: A deployed system to predict enterprise-targeted external cyberattacks. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), pages 31–36, Miami, 2018. IEEE.

[130] R. Graf and R. King. Neural network and blockchain based technique for cyber threat intelligence and situational awareness. In 2018 10th International Conference on Cyber Conflict (CyCon), pages 409–426, Tallinn, 2018. IEEE.

[131] R. Graf and R. King. Secured transactions technique based on smart contracts for situational awareness tools. In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), pages 81–86, Cambridge, 2017. IEEE.

[132] D. Tsai, W. Chen, Y. Lu, and C. Wu. A trusted security information sharing mechanism. In 43rd Annual 2009 International Carnahan Conference on Security Technology, pages 257–260, Zurich, 2009. IEEE.

[133] Leyli Karaçay, Erkay Savaş, and Halit Alptekin. Intrusion detection over encrypted network data. The Computer Journal, 9:1, 2020.

[134] M. Baskaran, T. Henretty, J. Ezick, R. Lethin, and D. Bruns-Smith. Enhancing network visibility and security through tensor analysis. Future Generation Computer Systems, 96:207–215, 2019.

[135] K. Berlin, D. Slater, and J. Saxe. Malicious behavior detection using windows audit logs. In Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security - AISec '15, pages 35–44, New York, New York, USA, 2015. ACM Press.

[136] P. Burnap, R. French, F. Turner, and K. Jones. Malware classification using self organising feature maps and machine activity data. Computers & Security, 73:399–410, 2018.

[137] Q. Chen, Sheikh Rabiul Islam, H. Haswell, and R. Bridges. Automated ransomware behavior analysis: Pattern extraction and early detection. International Conference on Science of Cyber Security, 2019.

[138] K. Demertzis, N. Tziritas, P. Kikiras, S. Sanchez, and L. Iliadis. The next generation cognitive security operations center: Adaptive analytic lambda architecture for efficient defense against adversarial attacks. Big Data and Cognitive Computing, 3(1):6, 2019.

[139] H. Farooq and N. Otaibi. Optimal machine learning algorithms for cyber threat detection. In 20th International Conference on Computer Modelling and Simulation (UKSim), pages 32–37, Cambridge, 2018. IEEE.

[140] C. Feng, S. Wu, and N. Liu. A user-centric machine learning framework for cyber security operations center. In 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pages 173–175, Beijing, 2017. IEEE.

[141] W. Feng, S. Wu, X. Li, and K. Kunkle. A deep belief network based machine learning system for risky host detection, 2017.

[142] J. Hernandez Guillen, M. del Rey, and R. Casado-Vara. Security countermeasures of a sciras model for advanced malware propagation. IEEE Access, 7:135472–135478, 2019.

[143] S. Hiruta, S. Ikeda, S. Shima, and H. Takakura. Ids alert priority determination based on traffic behavior. In Advances in Information and Computer Security, volume 11689 of Lecture Notes in Computer Science, pages 189–206. Springer International Publishing, Cham, 2019.

[144] K. Hong, C. Chen, Y. Chiu, and K. Chou. Ctracer: Uncover c&c in advanced persistent threats based on scalable framework for enterprise log data. In 2015 IEEE International Congress on Big Data, pages 551–558, New York, 2015. IEEE.

[145] C. Mao, H. Pao, C. Faloutsos, and H. Lee. Sbad: Sequence based attack detection via sequence comparison. In Privacy and Security Issues in Data Mining and Machine Learning, volume 6549 of Lecture Notes in Computer Science, pages 78–91. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[146] H. Mao, C. Wu, E. Papalexakis, C. Faloutsos, K. Lee, and T. Kao. Malspot: Multi2 malicious network behavior patterns analysis. In Advances in Knowledge Discovery and Data Mining, volume 8443 of Lecture Notes in Computer Science, pages 1–14. Springer International Publishing, Cham, 2014.

[147] Y. Niu and Y. Peng. Application of radial function neural network in network security. In 2008 International Conference on Computational Intelligence and Security, pages 458–463, Suzhou, China, 2008. IEEE.

[148] Y. Niu, Q. Zhang, Q. Zheng, and H. Peng. Security operation center based on immune system. In 2007 International Conference on Computational Intelligence and Security Workshops (CISW 2007), pages 97–103, Heilongjiang, 2007. IEEE.

[149] A. Oprea, Z. Li, T. Yen, S. Chin, and S. Alrwais. Detection of early-stage enterprise infection by mining large-scale log data. In 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pages 45–56, Rio de Janeiro, 2015. IEEE.

[150] A. Oprea, Z. Li, R. Norris, and K. Bowers. Made: Security analytics for enterprise threat detection. In Proceedings of the 34th Annual Computer Security Applications Conference on - ACSAC '18, pages 124–136, New York, New York, USA, 2018. ACM Press.

[151] H. Pao, C. Mao, H. Lee, C. Chen, and C. Faloutsos. An intrinsic graphical signature based on alert correlation analysis for intrusion detection. In 2010 International Conference on Technologies and Applications of Artificial Intelligence, pages 102–109, Hsinchu, 2010. IEEE.

[152] R. Vaidyanathan, A. Ghosh, Y. Cheng, A. Yamada, and Y. Miyake. On the use of bgp as numbers to detect spoofing. In 2010 IEEE Globecom Workshops, pages 1606–1610, Miami, Florida, USA, 2010. IEEE.

[153] S. Wu, J. Fulton, N. Liu, C. Feng, and L. Zhang. Risky host detection with bias reduced semi-supervised learning. In W. Hubei, editor, Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science - AICS 2019, pages 34–40, New York, New York, USA, 2019. ACM Press.

[154] T. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels, and E. Kirda. Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks. In C. N. Payne, editor, Proceedings of the 29th Annual Computer Security Applications Conference on - ACSAC '13, pages 199–208, New York, New York, USA, 2013. ACM Press.

[155] N. Yi, Z. Qi-Lun, and P. Hong. Network security management based on data fusion technology. In 2006 7th International Conference on Computer-Aided Industrial Design and Conceptual Design, pages 889–892, Hangzhou, 2006. IEEE.

[156] Paweł Dymora and Mirosław Mazurek. An innovative approach to anomaly detection in communication networks using multifractal analysis. Applied Sciences, 10(9):3277, 2020.

[157] Matthew Smith. The soc is dead, long live the soc! ITNOW, 62(1):34–35, 2020.

[158] G. Settanni, Y. Shovgenya, F. Skopik, R. Graf, M. Wurzenberger, and R. Fiedler. Acquiring cyber threat intelligence through security information correlation. In 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), pages 1–7, Exeter, 2017. IEEE.

[159] A. Erola, I. Agrafiotis, J. Happa, M. Goldsmith, S. Creese, and P. Legg. Richerpicture: Semi-automated cyber defence using context-aware data

analytics. In 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pages 1–8, London, 2017. IEEE.

[160] A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, and C. Ponchel. Why should we use 3d collaborative virtual environments for cyber security? In 2018 IEEE Fourth VR International Workshop on Collaborative Virtual Environments (3DCVE), pages 1–2, Reutlingen, Germany, 2018. IEEE.

[161] T. Kwon, J. Song, S. Choi, Y. Lee, and J. Park. Visnu: A novel visualization methodology of security events optimized for a centralized soc. In 2018 13th Asia Joint Conference on Information Security (AsiaJCIS), pages 1–7, Guilin, 2018. IEEE.

[162] B. Song, S. Choi, J. Choi, and J. Song. Visualization of intrusion detection alarms collected from multiple networks. In Information Security, volume 10599 of Lecture Notes in Computer Science, pages 437–454. Springer International Publishing, Cham, 2017.

[163] S. Hassell, P. Beraud, A. Cruz, G. Ganga, S. Martin, J. Toennies, P. Vazquez, G. Wright, D. Gomez, F. Pietryka, N. Srivastava, T. Hester, D. Hyde, and B. Mastropietro. Evaluating network cyber resiliency methods using cyber threat, vulnerability and defense modeling and simulation. In MILCOM 2012 - 2012 IEEE Military Communications Conference, pages 1–6, Orlando, 2012. IEEE.

[164] G. Payer and L. Trossbach. The application of virtual reality for cyber information visualization and investigation. In M. Blowers, editor, Evolution of Cyber Technologies and Operations to 2035, volume 63 of Advances in Information Security, pages 71–90. Springer International Publishing, Cham, 2015.

[165] L. Axon, B. Alahmadi, J. Nurse, M. Goldsmith, and S. Creese. Sonification in security operations centres: What do security practitioners think? In Proceedings 2018 Workshop on Usable Security, pages 1–12, Reston, VA, 2018. Internet Society.

[166] L. Axon, J. Happa, A. van Janse Rensburg, M. Goldsmith, and S. Creese. Sonification to support the monitoring tasks of security operations centres. IEEE Transactions on Dependable and Secure Computing, pages 1–17, 2019.

[167] L. Axon, J. Happa, M. Goldsmith, and S. Creese. Hearing attacks in network data: An effectiveness study. Computers & Security, 83:367–388, 2019.

[168] Louise Axon, Bushra A. AlAhmadi, Jason R. C. Nurse, Michael Goldsmith, and Sadie Creese. Data presentation in security operations centres: exploring the potential for sonification to enhance existing practice. Journal of Cybersecurity, 6(1), 2020.

[169] Neda Afzaliseresht, Yuan Miao, Sandra Michalska, Qing Liu, and Hua Wang. From logs to stories: Human-centred data mining for cyber threat intelligence. IEEE Access, 8:19089–19099, 2020.

[170] Ryan Mullins, Ben Nargi, and Adam Fouse. Understanding and enabling tactical situational awareness in a security operations center. In Isabella Corradini, Enrico Nardelli, and Tareq Ahram, editors, Advances in Human Factors in Cybersecurity, volume 1219 of Advances in Intelligent Systems and Computing, pages 75–82. Springer International Publishing, Cham, 2020.

[171] Z. Wang and Y. Zhu. A centralized hids framework for private cloud. In 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pages 115–120, Kanazawa, 2017. IEEE.

[172] R. Gad, M. Kappes, and I. Medina-Bulo. Monitoring traffic in computer networks with dynamic distributed remote packet capturing. In 2015 IEEE International Conference on Communications (ICC), pages 5759–5764, London, 2015. IEEE.

[173] H. Shiravi, A. Shiravi, and A. Ghorbani. A survey of visualization systems for network security. IEEE transactions on visualization and computer graphics, 18(8):1313–1329, 2012.

[174] R. Marty. Applied Security Visualization. Safari Tech Books. Addison-Wesley, Boston, 2009.

[175] M. Vielberth, F. Menges, and G. Pernul. Human-as-a-security-sensor for harvesting threat intelligence. Cybersecurity, 2(1):35, 2019.

[176] G. Zhiguo, X. Luo, J. Chen, F. L. Wang, and J. Lei, editors. Emerging Research in Web Information Systems and Mining. Communications in Computer and Information Science. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[177] R. Heartfield, G. Loukas, and D. Gan. You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. IEEE Access, 4:6910–6928, 2016.

[178] H. Liao, C. Richard Lin, Y. Lin, and K. Tung. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1):16–24, 2013.

[179] N. Miloslavskaya. Soc- and sic-based information security monitoring. In Recent Advances in Information Systems and Technologies, volume 570 of Advances in Intelligent Systems and Computing, pages 364–374. Springer International Publishing, Cham, 2017.

[180] A. Ganame and J. Bourgeois. Defining a simple metric for real-time security level evaluation of multi-sites networks. In 2008 IEEE International Symposium on Parallel and Distributed Processing, pages 1–8, Miami, 2008. IEEE.

[181] R. Ganesan and A. Shah. A strategy for effective alert analysis at a cyber security operations center. In From Database to Cyber Security, volume 11170 of Lecture Notes in Computer Science, pages 206–226. Springer International Publishing, Cham, 2018.

[182] K. Farris, A. Shah, G. Cybenko, R. Ganesan, and S. Jajodia. Vulcon: A system for vulnerability prioritization, mitigation, and management. ACM Transactions on Privacy and Security, 21(4):1–28, 2018.

[183] T. Sadamatsu, Y. Yoneyama, and K. Yajima. Practice within fujitsu of security operations center: Operation and security dashboard. Fujitsu scientific & technical journal, 52(3):52–58, 2016.

[184] L. Allodi and F. Massacci. Security events and vulnerability data for cybersecurity risk estimation. Risk analysis : an official publication of the Society for Risk Analysis, 37(8):1606–1627, 2017.

[185] Cyril Onwubiko and Karim Ouazzane. Soter: A playbook for cybersecurity incident management. IEEE Transactions on Engineering Management, pages 1–21, 2020.

[186] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete 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), pages 1–8, Dublin, 2020. IEEE.

[187] G. Gaudin, H. Debar, A. Fillette, J. deMeer, A. Rennoch, P. Saadé, and J. Saugeot. Etsi gs isi 007: Guidelines for building and operating a secured security operations center (soc), 2018.

[188] C. Crowley and J. Pescatore. Common and best practices for security operations centers: Results of the 2019 soc survey, 2019.

[189] National Aeronautics and Space Administration. Audit of nasa's security operations center: Report no. ig-18-020, 2018.

[190] IBM. Strategy considerations for building a security operations center: Optimize your security intelligence to better safeguard your business from threats, 2013.

[191] W. Jansen. Directions in Security Metrics Research. Diane Publishing, Gaithersburg, 2010.

[192] R. Savola. Towards a taxonomy for information security metrics. In Proceedings of the 2007 ACM Workshop on Quality of Protection, pages 28–30, 2007.

[193] P. Black, K. Scarfone, and M. Souppaya. Cyber security metrics and measures. Wiley Handbook of Science and Technology for Homeland Security, pages 1–15, 2008.

[194] R. Ganesan, S. Jajodia, and H. Cam. Optimal scheduling of cybersecurity analysts for minimizing risk. ACM Transactions on Intelligent Systems and Technology, 8(4):1–32, 2017.

[195] J. Moran. Key performance indicators (kpis) for security operations and incident response: Identifying which kpis should be set, monitored and measured, 2019.

[196] G. Doran. There's a smart way to write management's goals and objectives. Management review, 70(11):35–36, 1981.

[197] R. Cambra. Metrics for operational security control, 2004.

[198] K. Xu, S. Attfield, T. Jankun-Kelly, A. Wheat, P. Nguyen, and N. Selvaraj. Analytic provenance for sensemaking: a research agenda. IEEE computer graphics and applications, 35(3):56–64, 2015.

[199] M. Wagner, A. Rind, N. Thür, and W. Aigner. A knowledge-assisted visual malware analysis system: Design, validation, and reflection of kamas. Computers & Security, 67:1–15, 2017.

[200] M. Hummer, S. Groll, M. Kunz, L. Fuchs, and G. Pernul. Measuring identity and access management performance - an expert survey on possible performance indicators. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, pages 233–240, Funchal, 2018. SCITEPRESS.

MANFRED VIELBERTH studied Management Information Systems at the University of Regensburg. His major fields of study were Financial Computing and Information Security during his Bachelor´s degree and IT-Security during his Master's degree. Since February 2017, he is a Ph.D. candidate and research assistant at the Chair of Information Systems at the University of Regensburg. His research interests include human aspects in the security analytics domain. On the expert side, this mainly comprises improving processes for better integrating security analysts within a Security Operations Center. In terms of security novices, this primarily covers capturing reports about security incidents in the context of the Human-as-a-Security-Sensor paradigm.

FABIAN BÖHM received his master's degree in Management Information Systems within the Honors Elite Program at the University of Regensburg and the Polytechnic University of Catalonia in Barcelona in 2016. Since early 2017, he is a Ph.D. candidate and research assistant at the Chair of Information Systems at the University of Regensburg. His research interests cycle around the application of Visual Analytics for cybersecurity. His primary focus within this topic is to leverage Visual Analytics approaches to integrate human domain knowledge into different cybersecurity areas. The core research results show the possibilities offered by Visual Analytics in crucial security domains as Cyber Threat Intelligence, Identity and Access Management, Security Analytics, and Digital Forensics.

INES FICHTINGER received her B.Sc. and M.Sc degree in Management Information Systems with a specialisation in Cyber Security from the University of Regensburg (Germany). She is currently working at Deloitte Belgium as a Senior Cyber Security Consultant. Her main areas of interests are Security Operations and SOC-as-a-service, as well as evaluating the current cyber security posture of companies and helping them design a strategy to reach their desired security posture.

GÜNTHER PERNUL is a professor in the Department of Information Systems at the University of Regensburg, Germany. Pernul received his diploma and Ph.D. (with honors) in business informatics from the University of Vienna, Austria. Previously, he held positions at the University of Duisburg–Essen, Germany; University of Vienna; University of Florida, Gainesville; and College of Computing at the Georgia Institute of Technology, Atlanta. His research interests focus on data and information-security aspects, data protection and privacy, data analytics, and advanced datacentric applications. He is a Member of the IEEE. Contact him at guenther.pernul@ur.de.