Security Operations Centers: A Holistic View on Problems and Solutions

Matthew Shutock
The University of Texas at San Antonio
matthew.shutock@gmail.com

Dr. Glenn Dietrich
The University of Texas at San Antonio
glenn.dietrich@utsa.edu

Abstract

Since Security Operations Centers (SOCs) were first implemented, they have strived to protect the organization and constituency they serve from all manner of Information Technology (IT) security threats. As SOCs have evolved over time to become as effective and efficient at this as possible, they have struggled with changes and upgrades to their foundational elements of people, processes, and technology in pursuit of this mission. While most relevant literature focuses on one challenge a SOC faces, or one aspect of one problem, the authors of this paper performed a literature review to identify and discuss the top current and future challenges that SOCs face in addition to the top current and future solutions to these problems.

1. Introduction

While much has been written on what SOCs are, what they do, how they function, etc., there is an interest in determining what problems SOCs face both now and in the future in addition to how they plan to combat these problems.

Most research that has been conducted in this area focuses either on broad descriptions and/or implementations of SOCs [1]–[3] or on one specific issue facing a SOC such as personnel and staffing issues [4], big data integration and analysis [5], or securing cloud-based SOC infrastructure [6]. This paper attempts to combine relevant literature and identify the most common current problems faced by a typical SOC today, problems they anticipate having in the future, solutions currently implemented by SOCs today to combat these problems, and planned future solutions.

This paper will focus on both the qualitative and quantitative aspects of issues SOCs are facing. The qualitative aspects are based on academic and industry articles for specific topics. The quantitative statistics will stem from survey-based statistics from the SANS Institute where each survey collected and analyzed hundreds to thousands of SOC employee responses from a variety of sectors to help provide a well-rounded understanding of the SOC community.

In the following section, a general overview of what SOCs are, what they are comprised of, how they function, and what they are capable of will be discussed to give contextual understanding to the ensuing challenge/solution discussion.

2. SOC overview

Since their earliest official establishment in the 1990s [1], there have been many terms used to describe SOCs. Some of these include Security Operations Center (SOC), Cybersecurity Operations Center (CSOC), Network Operations and Security Center (NOSC), and even more holistic terms such as a Fusion Center [1], [7]. These monikers closely relate to the physical SOC facility and the services it provides. In this paper, the term "SOC" will be used when referring to a security operations center while the term "organization" will refer to the entities the SOC is charged with protecting.

Regardless of the official nomenclature chosen, all SOCs serve a similar purpose as shown in their definition. The most holistic definition for a SOC may be provided by SANS, according to Crowley and Pescatore, as "A combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects" [7]. In other words, SOCs operate in real-time to help monitor and maintain the entirety of an enterprise's information technology security through source aggregation, automatic alert generation/prioritization based on the data collected, and the ability to execute remediation solutions [1].

Hidden within the definition for a SOC is the concept of Computer Network Defense (CND). CND is defined as "The practice of defense against unauthorized activity within computer networks, including monitoring, detection, analysis (such as trend and pattern analysis), and response and

URI: https://hdl.handle.net/10125/80249
978-0-9981331-5-7

restoration activities" [1]. Essentially, CND is what the SOC does and is the SOC's overall purpose and objective. In pursuit of the SOC's mission to provide CND, a strong foundation of people, processes, and technologies must be in place for a SOC to succeed.

2.1. SOC foundational elements

People, Processes, and Technology (PPT) are the foundational triad a SOC operates on. All three components are required for a SOC to function effectively while the synergy between them allows a SOC to function efficiently. As Zimmerman states: "The key to effective CND is having the people, process, and technology that enable the SOC to maintain parity with the adversary" [1].

People are arguably the most important part of this triad as they are ultimately what construct a SOC and are often the last line of defense and interpretation of both data and events. Although processes and technology are integral to a SOC's function, people are the most critical element as it is extremely difficult to technologically emulate human thought processes for analyzing and remediating threats [1], [3]. Vielberth, Böhm, Fichtinger, and Pernul state that, although automation technologies are necessary for SOC operations, automation is difficult to implement and only works under the correct conditions which leads to the conclusion that "Determining whether an alert is real requires further investigation by the analysts based on tacit knowledge" [8].

Processes are the standardized workflows that SOCs and incident response teams follow to investigate and remediate alerts which should be documented in the SOC's procedures [2]. Procedures often come in the form of Standard Operating Procedures (SOPs) that contain the "specific technical processes, techniques, checklists, and forms" [9] used by SOC staff and are often geared toward junior staff such as Tier 1 personnel [1]. The most important aspects of processes are that they are both standardized and repeatable to help ensure no tasks are missed [10].

Technology involves all the hardware and software necessary for the proper functioning of the SOC and the ability to provide its designated services. The central theme around all SOC technologies is that they collect, aggregate, and analyze data from across an enterprise's entire infrastructure in addition to detection and prioritization of this data which later assists in remediation [2].

2.2. SOC operation and layout

SOC functionality varies widely based on several factors including budget, size and complexity of an organization, size of the SOC and services provided, maturity (i.e. how long the SOC has been operating), and where a SOC lies on the centralized vs. distributed spectrum [1], [7], [8]. According to the 2019 SANS SOC survey, 37% of SOCs utilize a single centralized SOC followed by 25% with no defined architecture, and 16% that were centralized but regionally distributed [7]. Due to this, this paper will explore the functionality of single centralized SOCs as it is the most common type.

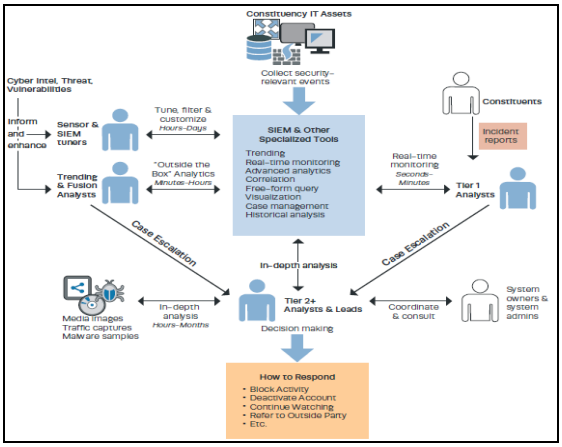

Figure 1. SOC roles and escalation [1]

A visualization of a single centralized SOC is shown in Figure 1. In this SOC configuration, data (e.g. logs) is collected from all IT assets across an organization's entire infrastructure and stored in collection databases. Additionally, threat intelligence, such as vulnerabilities and tactics, techniques, and procedures of threat actors, is collected and stored in separate databases for correlation between what possible/expected threats and vulnerabilities exist compared to what the organization has collected and is currently seeing. This combined data is analyzed and filtered by a correlation engine to produce alerts that are displayed by the SIEM (Security Information and Event Manager).

Through a combination of information displayed by the SIEM, supporting tools and processes, and alerts reported by the human constituency of an organization, alerts generated at this point are observed by human analysts which begin review, investigation, and/or remediation procedures.

Based on the size, capabilities, requirements, and geographic disbursement of both a SOC and the organization it serves, the organizational structure of a SOC can vary widely. This ranges from having a small, five-person SOC (or less) where all staff

typically cross-train and serve in all functions to large SOCs with hundreds of people in its employ where staff are separated into tiers with defined responsibilities for their respective positions. Torres provides a consolidated layout of a three-tier structure in regard to incident remediation as follows [2]:

- Tier 1 (Alert Analyst): continuous monitoring, triage, and remediation of incoming alerts
- Tier 2 (Incident Responder): investigates complex alerts elevated from tier one personnel
- Tier 3 (Threat Hunter): uses intelligence-led procedures to proactively identify and investigate threats before a SOC encounters them
- SOC Manager: responsible for administrative procedures and acts as a communication point between the SOC and the organization

Some of these tiers and capabilities can overlap depending on the specifics of a SOC, especially if a SOC is smaller in size or does not have the requirements or resources to implement this type of system [8].

To better serve their constituency, SOCs extend the capabilities of tiered staff members and help provide additional services based on the needs of the organization including, but not limited to, forensic investigation, auditing, and training for non-security staff [1].

3. Current problems/challenges

With an understanding of what SOCs are, how they operate, and who they serve, this discussion arrives at the problems/issues/challenges commonly faced by SOCs as of 2019. As with the design, requirements, services, organization, and staff of SOCs, problems vary from SOC to SOC. Therefore, not all SOCs will face all the problems described in the following sections.

Table 1 details the top challenges faced by SOCs based on SANS industry surveys. Table 1 compares the results of the same survey conducted in 2018 and 2019 with little change year to year for each individual challenge.

Table 1. Top SOC challenges [7]

Table 4. Challenges to Full Integration and Utilization of a Centralized SOC Service Model Year-over-Year

	2019		2018	
Lack of skilled staff	57.7%	157	61.9%	148
Lack of automation and orchestration	49.6%	135	52.7%	126
Too many tools that are not integrated	43.0%	117	47.7%	114
Lack of management support	37.1%	101	37.2%	89
Lack of processes or playbooks	36.8%	100	42.7%	102
Lack of enterprisewide visibility	36.0%	98	41.8%	100
Too many alerts that we can't look into (lack of correlation between alerts)	32.0%	87	33.9%	81
Silo mentality between security, IR and operations	30.2%	82	30.1%	72
Lack of context related to what we are seeing	25.4%	69	18.8%	45
High staffing requirements	25.0%	68	27.2%	65
Regulatory or legal requirements	9.2%	25	12.6%	30
Other	4.8%	13	8.8%	21
Answered		**272**		**239**

3.1. Staffing issues

Topping the list of current challenges is the lack of skilled staff employed by SOCs [7]. This means that there is both a lack of SOC staff and, consequently, a skill shortage in all areas necessary for the proper functioning of a SOC. As human analysts are arguably the most important portion of the PPT triangle, this can lead to a detrimental decrease in the protection, detection, and remediation provided by a SOC as no technology or process can or should completely replace them.

The results of the SANS 2018 survey revealed that 61% of SOC respondents felt the lack of skilled staff hampered SOC operations while the 2019 survey showed 57% felt the same [7], [11]. This correlates to the current need for people in the cybersecurity workforce as the 2020 International System Security Certification Consortium (ISC2) workforce study shows there is a shortage of 3.1 million people in the cybersecurity field globally [12].

This challenge can be viewed on two fronts as described below: one is the various training and academic curriculums for those entering the cybersecurity field while the other is the SOC/organization itself involving recruiting, hiring, training, and maintaining its workforce.

For academic curriculums, Hoffman, Burley, and Toregas discuss how traditional university programs do not match up with the time-critical nature of the rapidly evolving cybersecurity field, a lack of standardization in certificate programs, and a lack of networks to connect recent graduates to employers as major impediments in this area [4]. These reasons, among others, can create bottlenecks for organizations when seeking new people. Even if an organization were willing and financially able to hire new employees, it may be difficult to find those with the right skills in a timely manner.

From the organization's standpoint, time and funding must be set aside with management's support for hiring, recruiting, and training. A lack of upper-level opportunities, including managerial and advanced technical positions (e.g. forensics, penetration testing, etc.) requiring new and/or advanced training, can stifle the skill set of current employees preventing them from promotion and acquiring necessary knowledge [4].

Even when an organization finds individuals that are formally educated in this field, a dissonance exists between this education and technical knowledge, skills, and abilities required of the position [13]. This is especially true in cases of using detection, response, and remediation tools as these

are not typically part of a traditional education program [13].

As Crowley and Pescatore point out, many new employees simply know the fundamentals of security theory and lack analytical and critical thinking skills stemming from being unable to amalgamate the various skillsets they have been taught [11]. It is here that organizations rarely have the time and/or funding to properly train and hone the skills of these new hires.

3.2. Lack of automation

Automation, in a general sense, refers to the execution of tasks without human intervention [14]. In SOCs, this refers to "software tools that aid analysts' job and improve operational efficiency" [15]. Essentially, automation reduces the number of repetitive tasks that would normally have to be performed manually such as automatic ticket generation, system reimaging, data ingestion from multiple sources, and tool configuration.

If tasks are not automated within a SOC, the more time it will take to manually process them thus reducing the effectiveness and efficiency within a SOC [16]. Additionally, a lack of automation contributes to increased analyst fatigue and a decreased ability to focus on more important tasks [15].

A common response to mitigating problems caused by staff shortages described earlier is through automation. However, many SOCs see automation as a problem area as well [7].

To this end, Table 1 shows that around 50% of SOCs list lack of automation as an impediment to making their SOC effective. Additionally, 46.3% of organizations report using only a low level of automation for key security and IR processes [14]. For specific automation functions, SANS reported that only 18% of SOCs rely on an automation/orchestration platform to correlate and analyze data for events, Indicators of Compromise (IoCs) and other security threat data [11]. In the same study, 50% of SOCs only partially automate data extraction and calculation with substantial manual effort required for reporting SOC metrics.

There are many reasons for this lack of effective automation. While budget and management support are reported as the top reason with 61.7% of respondents reporting that this is a contributing factor, the following two, amount of staff and skill level, are factors in only around half of SOCs [14]. These issues result in a continuous predicament for SOCs where difficulty exists in hiring enough skilled staff and/or training them to accomplish "x" (automation in this case).

Although automation is becoming more essential to a SOC's core functions, it is important to note that automation should not become a replacement for human analysts. The purpose of automation should be to assist a SOC analyst in retrieving and processing information rather than all processes being completely automated. This leads to an additional problem where SOCs must strive for a balance between automated functions versus those analyzed by humans. While those alerts that can be automated with minimal impact should be implemented, higher-risk and more complex alerts should be dealt with by the analysts themselves [17].

3.3. Lack of tool integration

A lack of tool integration is closely tied to the current lack of automation in many SOCs. Integration is the capability for an automated platform to access, process, and communicate data from a variety of separate sources [14].

SOCs use a variety of tools to generate, collect analyze, store and present vast amounts of information [1]. Relevant data from both non-security and security-specific devices, especially log data, must be collected and processed for the effective operation of a SOC. As this data comes in different formats potentially containing different types of data (or at least the data being arranged in a different order based on the format), it is imperative that it be integrated in a way that it can be read and displayed by the appropriate technologies [8].

The number of devices in an organization can potentially number into the millions [1]. Additionally, new technologies and processes are constantly called for in support of an expanding organization therefore adding to the number of devices.

Without proper tool integration, SOCs will lack complete and detailed data from across the entirety of its organization [14]. Therefore, as each tool produces its own data, this reduces the context of an incoming alert and stifles an analyst's ability to react as they must spend more time manually investigating and rendering a solution.

Besides the 43% of organizations responding that a lack of tool integration is a major concern [7], 21.3% of organizations/SOCs report not currently using any automation or orchestration tools while 34% report they are currently undergoing integration of existing tools through in-house integration and orchestration efforts [14].

A lack of tool integration not only means a SOC cannot aggregate data properly from different sources but, consequently, that portions of the infrastructure are not visible [14]. This includes both not seeing the devices themselves and the context that this data provides (i.e. not only can we not collect data from subnet "x", but also that we cannot see/interpret what those users are doing).

One major cause of this lack of tool integration is a lack of integration between the SOC and Network Operations Center (NOC) [11]. SOCs and NOCs serve two separate but related functions: while the NOC exists to maintain an organization's IT infrastructure and network communications, the SOC monitors the security of the same [18]. Resultingly, overlap with tools and functions exists between these two departments. While NOC tools exist from a maintenance and diagnostic perspective, SOC tools stem from a security perspective. Although both sets of tools can perform similar functions, they are typically not integrated well.

To maintain separation of duties, it is imperative that these two departments remain separate. However, they should work together closely to help improve and provide a more complete picture of an organization's security. Unfortunately, only around 33% of SOCs integrate their functions with the NOC by either being an integral part of SOC operations or by being well informed and communicative of each other's activities [7].

Another issue with integration is that the myriad devices managed by a SOC, or at least device categories, come from different vendors [19]. As Clarke and Knake explain, security tool manufacturers often only want to design a product to solve one, narrow problem without concern for the larger picture of device integration as it is not a concern when trying to sell products [19]. This is due in part to SOCs lacking an understanding of their architectural needs and/or their desire to purchase tools that appear to be the most current solution to an issue which, resultingly, cause SOCs to increase their capability to react to some security problems but at the cost of the capability to resolve the more core issue of device integration [19].

4. Anticipated problems/challenges

As we move beyond 2019, there is no way to predict with absolute certainty what the future will hold. However, the types of issues SOCs will face in the coming years can be foreseen to some degree. With that, the issues described in the previous current problems/challenges section can easily transfer here as the speed at which SOCs and the entire security community remediate these issues depends on a variety of factors including money, time, and staffing levels.

Referring to Figure 2, we can see the top areas SOCs plan to focus future monetary investment in. Although this can be viewed as future solutions to current problems, it provides insight into what the future problems of SOCs will be.

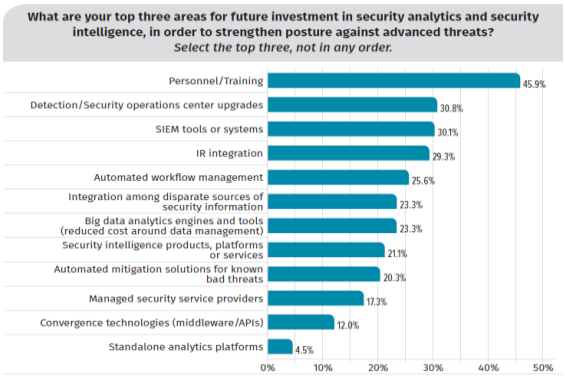

Figure 2. Future SOC investments [20]

4.1. Leveraging machine learning and big data

Machine learning is a derivative of the broader study of artificial intelligence [21]. According to Tantawy, this up-and-coming solution to many SOC problems incorporates algorithms to gather, process, and generalize both historical and current data for a SOC in order to learn from this over time [21]. By information mining, pattern correlation, and drawing inferences from this processed data, machine learning can predict, to some degree, future outcomes and assist SOC analysists in detecting and reacting to threats more quickly [21].

With machine learning, not only are the detection and response capabilities of a SOC automated more effectively and efficiently, the learning aspect is as well [21]. This represents a developing trend in cybersecurity with the convergence of data science and analytics.

Large amounts of unstructured data fed to a machine learning solution is a major component of machine learning effectiveness [5]. Although comprehensive big data can aid in machine learning, it has uses by itself such as being fed into log aggregation tools like the Elasticsearch, Logstash, and Kibana (ELK) platform or Splunk which help provide correlation, visualization, and therefore meaning to this seemingly limitless, unfiltered data.

As shown in Figure 2, almost a quarter of all SOCs predict they will invest in big data in the near

future. As of 2018, almost 52% of SOCs reported using AI/machine learning in some capacity [11] which increased from just under 40% from the previous year [22]. However, SOCs reported only a 34% satisfaction rating with the ability for machine learning to detect the occurrence of a threat in their organization in 2019 [7] which decreased from a 62% satisfaction rating for all machine learning capabilities from the previous year [10]. Overall, as machine learning becomes implemented to a greater degree, the satisfaction rating seems to decrease.

Several reasons help explain these satisfaction ratings, but the overarching cause is that the vendor-assured value of machine learning and big data are currently exaggerated [7]. With assertions that machine learning will eventually help with staffing problems, it requires skilled people to install, configure, and tune this technology as respondents in the 2019 SOC survey cited frequent false positives occurring as a result of implementing machine learning in their SOC [7].

Another source of dissatisfaction involves the previously discussed issues of integrated tools, visibility, and the ability to perform baselining [7]. For machine learning to be effective, a SOC must have visibility into their entire organization to gather data for machine learning to use and learn from. Without proper and accurate data, the conclusions derived by machine learning will remain unsatisfactory.

4.2. MSSP outsourcing

Although some SOCs have already begun outsourcing some or all aspects of their capabilities to Managed Security Service Providers (MSSPs), this will likely become more widespread in the future as the necessity for it will become more apparent with staff, skill, and resource shortages for the foreseeable future. According to a 2020 survey conducted by SANS concerning the use of external services, 23.5% of organizations reported they will maintain the same level of use for MSSP services as the previous year while 21.6% planned to increase the use of MSSPs by the end of 2021 [13].

MSSPs can be defined as paid entities that function as full-fledged SOCs completely external to an organization [1]. More specifically, MSSPs function similarly to a Software as a Service (SaaS) model even so far as to consider them a SOC as a Service (SOCaaS) in that they provide information security assurance and event management via log collection from both the SOC/infrastructure and their own cloud platform to help provide proactive and reactive defense [23].

When a lack of staff, specialized skills, and other resources exists for SOC operations, MSSPs are often considered and used to augment SOC capabilities as they can fill staffing and skill shortages required for in-house SOC functions [11]. Outsourcing SOC functionality in this way can allow a SOC to devote more time and resources to education/training of personnel they choose to keep.

With the benefits of MSSP use also come several challenges [11]. Outsourcing and the use of MSSPs are least likely to be successful when the provider must have a thorough understanding of business processes and/or active modification of internal systems is required [11]. A great deal of trust is also required between the organization/SOC and the MSSP as the MSSP requires knowledge of confidential business secrets that organizations are normally reluctant to provide to external parties to function effectively [11].

As mentioned previously for internal-only SOCs, device integration is a current and ongoing concern [14]. Even if a SOC uses different vendors for security and IT products that do not integrate well, they at least have the knowledge of what systems they have purchased. With an MSSP, an understanding of both the SOC's and the MSSP's technology and processes must be acquired and configured accordingly [24]. This can lead to a lengthy integration timeline (assuming it is successful) of typically six to nine months [7]. Although MSSPs may be a better option for some SOCs in the long run, SOCs may not be comfortable with the time and effort required in combination with the needed effectiveness of monitoring and detection.

4.3. Cloud-based infrastructures

Regardless of the use of MSSPs, organizations/SOCs are moving towards using cloud-based solutions [24]. An organization building and maintaining their own data centers for complete ownership of all equipment and technology can be an expensive proposition. As organizational requirements for new technologies to meet business needs is ever-growing, the border between on-premises environments and cloud infrastructure is beginning to erode.

74.2% of organizations currently use a mix of cloud and on-premise solutions for their infrastructure while 3% of organizations report using a cloud-only infrastructure for their operations [20]. This means that 19% use an on-premises only solution while over 77% of organizations use the cloud in some capacity. According to the SANS 2019 Cloud Security Survey, most organizations (32.5%)

use two to three cloud service providers [25]. With this continuing trend, respondents of the 2019 SOC survey show that the implementation of both informal ad hoc and single centralized SOCs are declining while the preference for both distributed and cloud-based SOCs is increasing [7].

With cloud-based providers, three organizations exist: the SOC using the services of the provider, the provider itself, and all other third parties affiliated with the SOC and/or the cloud provider. As integration will be required, this can result in a complex, heterogeneous technical coordination between all parties as there can be a significant lack of interoperability between both the overall infrastructure and security tools used by all parties [6]. 54.8% of SOCs report this lack of integration between security tools and the cloud as their top concern [20] while 28.2% of SOCs report a lack of employee skill/training with using public cloud services as their top realized issue [25].

Furthermore, just like an on-premises only solution, use of cloud resources leads to visibility issues from a lack of system/device integration [26]. For instance, with Amazon Web Services (AWS), while the customer is responsible for security in the cloud (i.e. their assets), AWS is responsible for security of the cloud itself [27]. For a SOC to be assured that both fronts are protected, this requires a great deal of coordination, integration, and configuration of both parties in addition to a high amount of trust as cloud providers may not fully disclose security vulnerabilities affecting themselves, and therefore the SOC, as they should.

Lastly, using cloud-based services leads to an expanded attack surface and should force a SOC to consider where threats may emerge from [28]. In addition to data being transferred between a SOC/organization, cloud systems are ultimately based on hardware and operating systems meaning they have inherent vulnerabilities just like traditional IT and security devices [28].

5. Current solutions

Some of the problems described in the previous section are solutions in and of themselves such as automation, using machine learning, MSSPs, and moving infrastructure into the cloud. As this discussion moves from current/future problems to current/future solutions, we will discuss how some of the most important issues for SOCs can be mitigated or resolved. Comparing Table 1 to Figure 2, we can see a comparison between SOC's overall concerns and areas of future investment. From this information, some of the top areas for current and future solutions can be seen.

5.1. Student and employee training

The overarching principle behind growing a skilled workforce for the cybersecurity field, and therefore qualified staff for a SOC, is a holistic approach to both education and training [4]. This involves the convergence of government, industry, and academic parties to communicate, identify, and define what education and training is necessary when compared against the complex and ever-evolving world of cybersecurity [4].

One such partnership is the National Initiative for Cybersecurity Education (NICE) framework which helps define and map required cybersecurity knowledge and skills for new entrants to the field thereby helping to address needed education and workforce challenges [29]. Universities can use this framework to better define programs, while employers can create applicable training programs, and policymakers can create laws and standards to better facilitate this convergence effort. Additionally, programs such as the DoD Cyber Scholarship Program and the National Science Foundation's Scholarship for Service enable better collaboration between government-driven support and focus, academic education, and industry-based skill refinement through cybersecurity conference attendance and internship opportunities [30], [31].

Based on insight and guidance provided from frameworks like NICE, two- and four-year academic institutions educating new entrants to the cybersecurity field should make the effort to merge cybersecurity education with their diverse range of schools and departments (e.g. business, engineering, science, etc.), adapt to the field and provide job-relevant skills, and take advantage of contemporary technological developments [4]. For example, Cyber Bit's Cyber Range mimics a SOC in a virtual environment for students thereby enabling them to train and respond to simulated alerts and incidents as if they were working in an actual SOC [32]. Solutions like Cyber Range allows students to not only integrate classroom instruction with real, marketable experience in a training environment, but also take a real-time, proactive approach to applied learning and problem solving instead of traditional reactive/historical assignments.

For employee training, especially for new hires, initial training should be a top priority that is included in an organization's processes [8]. Much of this should be focused on foundational skills acquired through documentation review and on-the-job

experience via observation and supervised tasking. For a SOC, this could mean forming a new employee pipeline where the person starts in a tier one position to become familiar with the technologies used, the overall environment, and issues typically seen in that SOC followed by periodic training. From here, as new hires gain experience and proficiency, they can move on to receive additional training in more specific areas of SOC operations.

5.2. Automation improvements

As most SOCs are suffering from the lack of skilled staff combined with large and ever-growing pools of data to analyze, they are constantly looking for new ways to automate tasks and implement orchestration and device/operations integration [8]. For a SOC to achieve effective and thorough monitoring and analysis, they must strive to automate to the largest extent possible without removing people entirely from the protection, detection, and remediation processes [1].

One relatively new and novel way of accomplishing this is with Dorkbot developed by the University of Texas at Austin which is currently used by over 2.350 educational institutions from 205 countries [33]. Dorkbot "automates the discovery and verification of web application vulnerabilities across entire domains at scale" and hunts for both uncommon and common web-based vulnerabilities such as cross-site scripting, local/remote file inclusion, operating system injection, and SQL injections by leveraging the power of publicly available sources such as the Google Hacking Database [33], [34]. Dorkbot was developed entirely in-house and is distributed freely to all academic institutions to include the source code if an institution wishes to deploy it locally. While the focus is toward academia, several state agencies in Texas use Dorkbot as well. The continued effort to improve the effectiveness and efficiency of Dorkbot has resulted from over 6,000 verified vulnerabilities reported in 2017 to over 26,000 in 2018 [34].

Other more common tools for automating aspects of a SOC's operations include log aggregation and big data analysis tools such as Splunk, ELK, and Sumo Logic [5]. With log aggregation tools like these, the process of analysts having to either manually parse logs from myriad devices of different types or parse these logs with relatively simplistic search mechanisms like grep are dramatically reduced. In addition to aggregating various log and data sources from across a SOC's environment, the ingestion of threat intelligence from sources internal and external to the SOC allow for the effective correlation of pertinent information to proactively determine the source of threats and how to respond to them more effectively and efficiently.

The combination and use of these various orchestration/automation processes and technologies have greatly aided SOCs, albeit with the challenges described earlier, in combating the truly foundational issues of time, money, and lack of skilled personnel. The challenge for SOCs and their respective management is to plan for the effective implementation and use of these tools and processes, decide on what is most appropriate for their operations, and dedicate resources towards fully integrating them.

6. Future solutions

As with the challenges described earlier (automation, MSSPS, cloud integration), we can see some of the solutions that SOCs may implement out of desire and/or necessity as we move beyond 2019. The current/future solutions described here are interchangeable to an extent. Although the solutions described in the next section are in use to some degree currently, they are not as well defined and/or implemented as the current solutions described previously.

6.1. Development security operations

A developing trend for organizations to undertake and for SOCs to monitor and integrate into their security solutions is that of Development Security Operations (DevSecOps) which stems from Development Operations (DevOps) [35].

DevOps strives to produce quality code through a streamlined process that incorporates automated testing on a continuous development and deployment cycle [36]. While there are advantages to producing code in this manner, security is mostly an afterthought as DevOps is often outsourced and/or deployed in the cloud through an Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) implementation thereby reducing the control and visibility that the parent organization has with respect to both the code itself and the external infrastructure it is created on [37].

DevSecOps functions as an extension of the Software Development Lifecycle (SDLC) that seeks to change the process that DevOps uses by enhancing the security of both the automation processes and the final code [38]. DevSecOps functions via continuous collaboration among development, IT operations, and information security teams with all three involved in

the continuous development and deployment cycle [28]. By integrating security controls and into the DevOps cycle, security tasks related to code building, such as security checking and testing, can be automated thus leading to secure code that does not interfere with the continuous nature of software development and deployment [36].

This new focus in software construction has led to the implementation of Continuous Integration and Continuous Delivery (CI/CD) pipelines [35]. With a CI/CD pipeline, often offered by major cloud and external service providers such as Amazon Web Services, Microsoft, and Atlassian, scalable continuous security becomes part of this cycle as well through various automated testing processes such as both static (tests owned and/or imported code) and dynamic code analysis (tests code externally while in a running state as an attacker would) [38].

While CI/CD pipelines add automated security verification and testing to code, they also create logs of every step in the process [36]. Logging in this way helps create continuous, verifiable feedback that can be ingested and analyzed by SOC tools to check for security issues both during development and after deployment. Combined with data gathered from threat intelligence sources, this can alert the SOC to the most up to date vulnerabilities created as a result of its constituency's software development whether internal or external to the organization.

6.2. Platform consolidation

Combining the previously discussed concepts of orchestration/automation, device integration, and the expanding nature of organizations (especially in the cloud), there is a prediction that the security tools used by SOCs will be consolidated under a handful of platform developers [19].

A security platform is the combination of four separate types of components: devices that sense, devices that understand and filter what the sensors collect, devices that make decisions based on the filtered data, and devices that carry out actions based on what the decision-making devices decide [19].

These components combined in this manner will allow SOCs to have all the features and capabilities of multiple tools from multiple vendors without the configuration and integration overhead.

Creating a platform does not mean that platform manufacturers will be required to buy out smaller companies, but rather that they integrate existing tools into the single platform they develop. Clarke and Knake provide an example of this when they describe how vendor A can have the sensing and actuating components of a platform installed in an organization's infrastructure while the sense- and decision-making devices belonged to vendor B housed in their separate infrastructure. Here, vendor B would be able to automatically pull information gathered by the sensors, process it, and send the decision back to the actuating devices owned by vendor A [19].

While the security platform concept itself relates more to the future of the cybersecurity industry, this would have tremendous benefits for SOCs as they would not have to coordinate and integrate with multiple vendors. A solution sometimes proposed by SOCs in response to this is for them to make their own tools. This is a massive undertaking that requires tremendous amounts of time, money, and expertise which many SOCs do not have as only 22.7% of SOCs report using Application Programming Interfaces (APIs) and dashboards developed entirely in-house for event data correlation and analysis [11].

7. Conclusion

SOCs, in their mission to provide CND for an organization through protection, detection, investigation, and remediation of alerts and incidents, rely on a combination of people, processes, and technology. Within each of these foundational components, there exists many challenges in achieving effective and efficient SOC operations. While SOCs are struggling through the growing pains of resolving these issues, there exists a constant stream of solutions from the motivation, ingenuity, and dedication of the most important aspect of a SOC: people.

8. References

[1] C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*, The MITRE Corporation, 2014.

[2] A. Torres, "Building a World-Class Security Operations Center: A Roadmap", SANS Institute Reading Room, SANS Institute, 2015.

[3] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A Tale of Three Security Operation Centers", *SIW '14: Proceedings of the 2014 ACM Workshop on Security Information Workers*, 2014, pp. 43–50.

[4] L. Hoffman, D. Burley, and C. Toregas, "Holistically Building the Cybersecurity Workforce", *IEEE Security & Privacy Magazine*, vol. 10, no. 2, 2012, pp. 33–39.

[5] R. Andrade and J. Torres, "Enhancing intelligence SOC with big data tools", *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, pp.

1076–1080.
[6] J. Meszaros, “Towards security management in the cloud utilizing SECaaS”, *WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering Series*, no. 7, 2012.
[7] C. Crowley and J. Pescatore, “Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey”, SANS Institute Reading Room, SANS Institute, 2019.
[8] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, “Security Operations Center: A Systematic Study and Open Challenges”, *IEEE Access*, vol. 8, 2020, pp. 227756-227779.
[9] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology”, *NIST Special Publication (SP) 800-61*, rev. 4, 2012.
[10] F. Janos and N. Dai, “Security concerns towards Security Operations Centers”, in *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, IEEE, 2018, pp. 000273–000278.
[11] C. Crowley and J. Pescatore, “The Definition of SOC-cess? SANS 2018 Security Operations Center Survey”, SANS Institute Reading Room, SANS Institute, 2018.
[12] $(ISC)^2$, “Cybersecurity Professionals Stand Up to a Pandemic”, *$(ISC)^2$ Cybersecurity Workforce Study 2020*, $(ISC)^2$, 2020.
[13] J. Pescatore and B. Filkins, “Closing the Critical Skills Gap for Modern and Effective Security Operations Centers (SOCs)”, SANS Institute Reading Room, SANS Institute, 2021.
[14] B. Filkins, “2019 SANS Automation and Integration Survey”, SANS Institute Reading Room, SANS Institute, 2019.
[15] S. Sundaramurthy, et al., “A Human Capital Model for Mitigating Security Analyst Burnout”, *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, 2015, pp. 347–359.
[16] D. Murdoch, “2020 SANS Automation and Integration Survey Integration Survey”, SANS Institute Reading Room, SANS Institute, 2021.
[17] E. Cole, “SOC Automation - Deliverance or Disaster", SANS Institute Reading Room, SANS Institute, 2017.
[18] J. Pescatore, “Maximizing SOC Effectiveness and Efficiency with Integrated Operations and Defense”, SANS Institute Reading Room, SANS Institute, 2019.
[19] R. A. Clarke and R. K. Knake, The Fifth Domain, Penguin Press, New York, 2019, pp. 63–83.
[20] M. Bromiley, “Effectively Addressing Advanced Threats”, SANS Institute Reading Room, SANS Institute, 2019.
[21] A. Tantawy, “Closing the Skills Gap with Analytics and Machine Learning”, SANS Institute Reading Room, SANS Institute, 2017.
[22] C. Crowley, “Future SOC: SANS 2017 Security Operations Center Survey”, SANS Institute Reading Room, SANS Institute, 2017.
[23] F. F. Alruwaili and T. A. Gulliver, “SOCaaS: Security Operations Center as a Service for Cloud Computing Environments”, *International Journal of Cloud Computing and services science*, vol. 3, no. 2, 2014, pp. 87–96.
[24] T. Banasik, “The State of Cloud Security : Results of the SANS 2020 Cloud Security Survey”, SANS Institute Reading Room, SANS Institute, 2021.
[25] D. Shackleford, “SANS 2019 Cloud Security Survey”, SANS Institute Reading Room, SANS Institute, 2019.
[26] Cloud Security Alliance, “Top Threats to Cloud Computing: The Egregious Eleven”, Cloud Security Alliance, 2018.
[27] Amazon, “Shared Responsibility Model”, Amazon Web Services, Inc., 2021, https://aws.amazon.com/compliance/shared-responsibility-model.
[28] D. Shackleford, “Automating Cloud Security to Mitigate Risk”, SANS Institute Reading Room, SANS Institute, 2019.
[29] W. Newhouse, S. Keith, B. Scribner, and G. Witte, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework”, *NIST Special Publication 800-181*, 2017.
[30] United States Department of Defense, “Cyber Scholarship Program (CySP)”, Department of Defense, 2021, https://dodcio.defense.gov/Cyber-Workforce/CySP/Scholarship.
[31] United States Office of Personnel Management, “CyberCorps: Scholarship for Service”, United States Office of Personnel Management, 2021, https://www.sfs.opm.gov.
[32] Cyberbit, “Cyber Range”, Cyberbit, 2021 https://www.cyberbit.com/platform/cyber-range.
[33] The University of Texas at Austin Information Security Office, “Dorkbot”, The University of Texas at Austin, 2021, https://security.utexas.edu/dorkbot.
[34] C. Beasley, “Dorkbot: A Managed Application Security Assessment Service for Higher Education”, Educause Review, 2019, https://er.educause.edu/blogs/2019/2/dorkbot-a-managed-application-security-assessment-service-for-higher-education.
[35] J. Bird and E. Johnson, “A SANS Survey: Rethinking the Sec in DevSecOps: Security as Code”, SANS Institute Reading Room, SANS Institute, 2021.
[36] D. Shackleford, “A Guide to Managing Cloud Security", SANS Institute Reading Room, SANS Institute, 2018.
[37] A. Robinson, “Continuous Security: Implementing the Critical Controls in a DevOps Environment", SANS Institute Reading Room, SANS Institute, 2016.
[38] J. Mukherjee, “DevSecOps: Injecting Security into CD Pipelines”, Atlassian, 2019, https://www.atlassian.com/continuous-delivery/principles/devsecops.