AARMS Vol. 16, No. 3 (2017) 73–92. **10.32565/aarms.2017.3.5**

Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics[1]

Balázs Péter HÁMORNIK,[2] Csaba KRASZNAY[3]

Cybersecurity is an emerging field of national security where usually the technical aspects of defense take first place. Cyberdefense is heavily relaying on teamwork where members of Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) or Security Operations Center (SOC) teams are often geographically dispersed. In cybersecurity teamwork, computer supported collaboration is crucial as the team functions virtually in many ways. In this paper we present the results of interviews that were conducted with SOC exerts and we summarize the reviewed relevant literature. We have reviewed knowledge, skills, abilities and other characteristics (KSAOs) that make a team of cybersecurity experts capable to perform as virtual teams. These results revealed that to treat the cybersecurity team as a socio-technical system and supporting to cope with challenges of virtual teams helps them to be more effective and enhances employee retention. This perspective may contribute to cyberdefense of both industry and military.

Keywords*: human factors, Security Operations Center, teamwork, KSAOs, virtual teams*

Introduction

As cybersecurity is getting one of the most important national security issues worldwide, nations began improving their ability to tackle this challenge successfully by setting up specialized forces for cyberdefence. One of the best-known setup for such groups is a Computer Emergency Response Team or a Computer Security Incident Response Team. A CERT or a CSIRT can support one organization or a set of organizations with the same interest. The basis of their success is the continuous flow and interpretation of security related information. This can be done in a Security Operations Center (SOC) that is the key element of modern incident management.

There are several CERTs or CSIRTs in Hungary, some of them support private companies, some of them were established by non-profit organizations, some of them came into being through the effects of a law. CERT-Hungary is responsible for the incident management of all governmental and municipal bodies, meanwhile Mil-CERT deals with the cyber incidents

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-entitled "Public Service Development Establishing Good Governance" in the Ludovika Cybersecurity Workshop.

[2] Ph.D., Assistant Professor, Budapest University of Technology and Economics, Department of Ergonomics and Psychology; e-mail: hamornik@erg.bme.hu

[3] Ph.D., Assistant Professor, National University of Public Service, Institute of E-government; e-mail: krasznay.csaba@uni-nke.hu

of Hungarian Defense Forces. Although cooperation is essential between such groups, they have to be built up as an operational internal team first. [1] Unfortunately, one of the major problems in information security is that there is a million-man strong manpower shortage in this profession worldwide. In military, this might be solved by simply reassigning some troops, but old traditions may not work in a modern age with knowledge workers. Therefore, it is worthwhile studying people related questions of cyber defense and highlighting the findings to support Hungary's national security efforts in the cyberspace.

Knowledge, skills, abilities and other characteristics (KSAOs) could be identified that make employees capable of working effectively in SOC teams. This includes both general and virtual teamwork approaches. This step should rely on the results of research on work-related stress in other high-risk industries, such as aviation or nuclear power-plant (NPP) where employee selection focuses on tolerance against monotony or on vigilance. [2] The application of the expected results from this latter step would contribute to better employee selection, retention, and development in SOCs even in the military, which in turn could help alleviate the serious lack of experts that, as mentioned previously, SOCs are facing nowadays.

Security Operations Centers (SOCs)

Security Operations Centers are defined as both a team and an organization unit, often operating in shifts around the clock. SOCs are also a facility dedicated to preventing, detecting, assessing and responding to cybersecurity threats and incidents, as well as to fulfilling and assessing regulatory compliance. This implies many aspects that invite closer examination: the team (in the first place), the organizational unit, and the external expectations that compliance requirements bring. It is important to emphasize that SOCs cover multiple security activities that require different skill sets when it comes to effective teamwork. A fully functional SOC running 24/7 requires a team of minimum eight to 10 people just to maintain two people per shift, working three days on, three days off, four days on and four days off in opposing, 12-hour shifts. [3] This requires effective teamwork and competent leadership of such teams. To maintain continuous high quality through the changes in shifts and people, a deep, shared understanding should be developed and kept up-to-date. In addition, the recruitment, selection, and retention of employees is crucial in SOCs: shift work, time pressure, monotony, and high risk all make demands on staff, as they induce stress and fatigue, and are a challenge to work-life balance.

The main activities that an SOC covers are monitoring functions, detection, triage of alerts, resolution of incidents (by taking actions or escalations), handling of issues (aligned with the internal or external processes required, e.g. ticketing system or reporting), threat hunting and threat intelligence (TI).

The last 15 years of the SOC landscape reveal four incremental generations of SOCs developed as responses to increasingly sophisticated attacks. [3] [4] [5] The generations distinguish different sets of tools used and ways of working, as well as more and more requirements to comply with. This evolution is visible throughout the research literature from the years 2000s. [4] SOC generations are as follows:

1. *First-generation SOC:* Security operations are not delivered by the establishment of a formal SOC, but in many cases by some IT operations individual or a team who focuses on a blend of tasks. They cover device and network monitoring, as well as antivirus operation. They rarely work proactively, and the security incident response is

not appreciated highly in the enterprise. This initial generation of SOCs does not usually use a centralized system such as a Security Information and Event Management (SIEM) tool. [3]

2. *Second-generation SOC:* At this stage, SOCs focus on security threat management and event management, which creates the need for SIEM tools. SIEMs aggregate log information from various sources to form events. Events are then correlated to discover the possible relationships between them to help identify a security incident. Incidents are reported and visualized as dashboard alerts to SIEM operators. At this level, SOC activities are integrated with company ticketing systems. The main activity while operating such second generation SOC systems is correlation rule setting and refinement to enable the SIEM tool to capture known or recently discovered threats. This is always a reactive way of working. [3]
3. *Third-generation SOC:* At this level of evolution, incident response tasks are formalized. Other security services, such as vulnerability management are linked to SOC operations. This shows a shift toward a more proactive strategy. [3]
4. *Fourth-generation SOC:* The latest generation is described by the manner SOCs treat data. They can analyze large amounts of data recorded over long periods of time to discover threats and visualize them. This volume of data could also mean big data analytics. The data is enriched using multiple external sources (e.g. geo IP, DNS, IP and Domain reputation service, threat intelligence feeds). Another key differentiator at this level is the automation of remediation measures (as opposed to manual rule setting processes). [3]

Regarding the models of SOCs, based on our knowledge of the market, five distinct models exist:

1. A virtual SOC, mostly found in small enterprises does not have a dedicated facility and consists of part-time members working in a reactive manner. The virtual SOC may be applied when most of the SOC operations are outsourced and the in-house security team is limited to this model.
2. A multifunction SOC/Network Operation Center (NOC) has a dedicated facility, however, it shares tasks and people with the NOC. It provides 24/7 operations and it is frequent in the case of low-risk large enterprises or small/mid-size companies aiming to save costs.
3. A distributed/co-managed SOC consists of dedicated and partly dedicated team members, typically in 5/8 operation times, co-managed with a Managed Security Service Provider (MSSP). It is most frequent in small/mid-sized enterprises.
4. A dedicated SOC has its own facility and team fully employed in-house, operating 24/7, covering all functions required. It is the best practice choice for large enterprises and companies facing high risks.
5. A command SOC is a coordinating, higher-level SOC that provides threat intelligence, threat awareness, and additional services to multiple local SOCs in very large enterprises. Command SOCs are rarely involved in day-to-day operations. Security operations can be outsourced to expert service providers (MSSPs) who run the SOC at their facility, using their own team. In this case, the MSSP's SOC team is shared among multiple clients.

An SOC facility's physical characteristics are inspired by the arrangements found in a network operating room. [3] The aim of the physical setting is to facilitate monitoring, the shared understanding of events, and the collaboration of experts. The analysts at the individual workstations with multiple displays are facing toward a large central screen, which shows a dashboard where alerts may appear and where network status is monitored in tables, logs, and charts. The analysts' displays show the same types of information in details. The individual workstations are grouped by roles of team members. *Level 1* analysts, who investigate alerts at the first step, usually sit closest to the central display. Then *level 2* and *level 3* come at increasing distances from the center. The adjunct functions of the SOC e.g. TI, forensics, malware analysis may sit separately or even in different facilities. The SOC manager as a team leader is positioned to overlook the whole team in the room to be able to orchestrate their work.

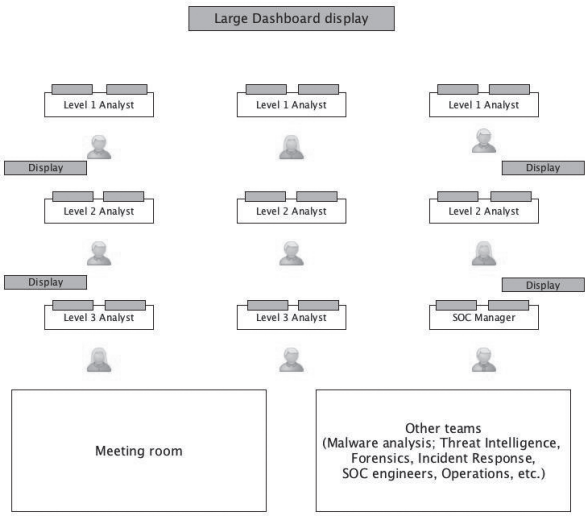

Figure 1. *SOC floor plan.* [Edited by the authors.]

As mentioned previously, the SOC is also defined as a team which has a leader and specialized employees. [3] SOCs are usually led by the SOC manager, who is responsible for the overall leadership. The majority of tasks in the team rely on analysts whose responsibilities can include security event monitoring, incident report investigation, incident handling, threat intelligence, vulnerability intelligence and reporting. They are organized in escalation levels (1–2–3) or tiers from juniors to seniors. The most advanced experts are doing forensics and malware analysis, which may be somewhat separated from the escalation levels. There are engineering roles (SOC engineers) too, who are responsible for the testing, staging, and deploying of new technology platforms or major releases/updates to those platforms. This also includes the setting and the refinement of correlation and detection rules. Operations roles also exist, focusing on the maintenance and operation of the SOC platforms. Beside these core roles, other support functions can also be represented in the SOC team: project managers, compliance and audit support experts, process/procedure developers, training specialists, communications specialists, etc.

SOC is a Field of Teamwork

Teams are groups of people working together toward reaching a common goal. They work in an interdependent way: every team member's performance contributes to the overall performance and they rely on each other. [6] Their activity is coordinated by a leader who orchestrates the processes and procedures they follow. These are especially valid in the case of high-risk industries—such as aviation, nuclear power-plants (NPPs) and information security—where an error can lead to fatalities, accidents, or data losses.

Teams are more than the sum of their members: interdependency and collaboration among members produce higher performance than can be reached by the individuals making up the team. This originates from the way knowledge is used and combined in a team. Mental representations that contain information that are applied in the team are named in multiple ways in the literature of psychology. A focused field of applied cognitive and social psychology studies team cognition in multiple industries. Team mental models [7] [8] contain the shared knowledge that a team has. This means the up-to-date representation of the internal and external reality, the knowledge that has to be applied during work. It contains the problems and tasks to be solved, the tools to be used, individual knowledge and its distribution (who knows what), the processes to follow on a team or individual level (roles in the team), and the future state that is the aim of the team's activities. The team's mental model functions as a common interpretative frame for the team, which enables them to react effectively to challenges. [8] The team mental model contains decision- and behavioral patterns that can be applied across the team and which enable them to behave coherently.

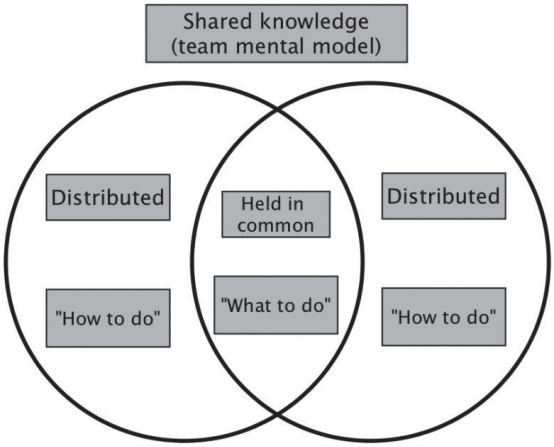

Figure 2. *Team mental model: What is shared and distributed?* [Edited by the authors.]

According to Banks and Millward [9] the procedural knowledge that dictates how to perform a task (a procedure [3]) usually does not have to be owned by every team member. It is not fully efficient to have the knowledge of procedures represented redundantly: a team should not be a group of one-man-armies as it is emphasized in case of SOCs. [3] The declarative

knowledge containing what to do has to be owned by every team member indeed. It enables the team to keep their focus on their aims, and act in a coordinated way toward the same goal.

The key to using team mental models effectively, as a team-level cognitive process, is communication. Explicit communication enables teams to build and update team mental models. [10] [11] [12] During periods of high pressure, there is often no room to communicate, to explain the background of actions or the context. Thus, communication before actions is crucial to a fully functional team mental model. During an emergency situation, teams perform with a limited communication capacity, coordinating their actions implicitly. This means that they presume that everyone knows what to do and how to perform their roles. The team mental model held in the minds of individuals enables the team to perform effectively. As we have previously reviewed information security teamwork in SOCs, this is one of the fields of teamwork in high risk where team mental models, communication, and coordination takes a crucial role in success.

Computer Supported Cooperative Work (CSCW)

Information security and security operations centers places where teams are using technology to collaboratively complete their tasks, reach their goals. This makes the research field of Computer Supported Cooperative Work (CSCW) highly relevant. According to Carstensen and Schmidt CSCW addresses: "how collaborative activities and their coordination can be supported by means of computer systems." Relying on the definition of Carstensen and Schmidt *"computer-based support for cooperative work can be provided by offering better communication facilities, providing improved monitoring and awareness possibilities to the actors, and by aiming at reducing the complexity of the coordination activities to be conducted by the involved actors"*. [13: 620] CSCW focuses on the study of tools and techniques of groupware, as well as their psychological, social, and organizational effects. [14] In order to use our concepts distinctively, we have to define what we mean by collaboration and cooperation. Collaboration is when people work together toward a single shared goal. Cooperation is slightly different: while cooperating, people perform together but also work on their own goals (goals that fit the common aim's direction).

The "CSCW matrix" (Figure 3) considers the work context along two dimensions: space features of collaboration (co-location or geographically distributed) and time features of collaboration (synchronous or asynchronous working). The resulting four cells cover most of the possible ways a team can collaborate or cooperate. [15]

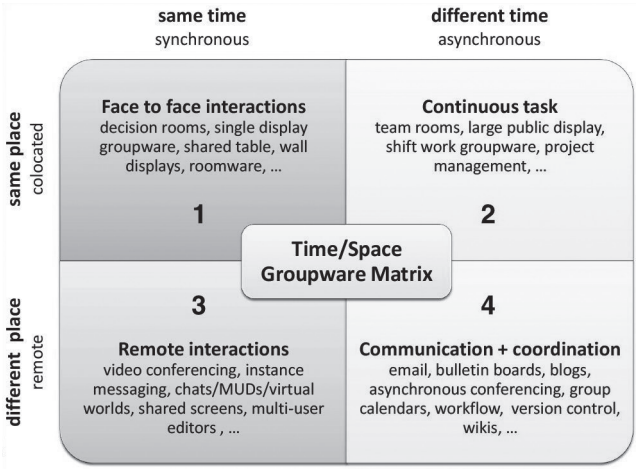

Figure 3. *The CSCW Matrix.* [16]

Previously we have defined SOC teamwork as where team mental models expected to be observed and identified expound the characteristics of it in the CSCW perspective. [17] In this study we are focusing on a mixture of synchronous and asynchronous tasks heavily relying on remote interactions, communication, and coordination.

Virtual Teams

Security Operations Centers are assumed to be a field of teamwork where technology plays a crucial role while more and more frequently geographical distributed experts are requested to collaborate using communication channels provided by information technology. These characteristics of teams fit what literature defines as virtual team. Traditionally virtual teams are defined as: *"a group of people who interact through interdependent tasks, guided by common purpose. Unlike conventional teams a virtual team works across space, time, and organizational boundaries with links strengthened by webs of communication technologies."* [18: 6] This definition fits the CSCW matrix cited above and integrates into the research paradigms of work and organizational psychology. Virtual teams are in the current focus of organizational psychology, since approximately 79% of knowledge workers work in dispersed teams so it became a standard form of working. [19] In the following section, we are examining collaborative aspect of security teamwork where virtual teamwork may appear.

Virtual Collaboration in SOCs

Information security work both in individual and team levels started emerging as a research topic in CSCW from the early 2000s. Hence the emphasis of supporting the effectiveness in this field remained on the technology side. The technology provides more and better data, indicators, anomalies, less false positive alerts which security experts are getting faced with. Focusing on the human factors Goodall, Lutters, Komlodi [20] [21] studied the analysts using intrusion detection system (IDS). In that time SOCs were not widespread and the activities

of IDS Analysts could be considered to be the ancestors of SOC Analysts. IDSs are pattern based alerting tools aiming to prevent attacks against the organizations computer network. Analysts handle alerts that are false positives in a very high percentage: however, they have to maintain their vigilance to look for alerts indicating real compromises. Considering the IDS analysts' work as a socio-technical system [20] three points can be highlighted: (1) understand the work-behavior of analysts, what effects both (2) the way to design technology that fits their tasks, and (3) the staffing of such teams. IDS Analysts work consists of monitoring, analysis, and response. These tasks are mostly identical to SOC analyst tasks. Especially since these have similarities in collaborative means: analysts do not work in isolation: they are interactive with other experts responsible for other domains in the security team (security manager) or in the organizations or even outside the company when looking for or sharing threat intelligence information (TI)—email feeds in 2004, TI platforms nowadays.

1. *Monitoring:* IDS analysts handle high quantity of alerts, considering most of them as false positives. This high load of alerts causes the monitoring and reacting activities to be performed under time pressure. This is a time consuming but not cognitively challenging task.
2. *Analysis:* When an alert is not considered false positive analysis is required to make the further decision on what reaction to take. This is a highly unpredictable yet non-routine task. Both the frequency and duration of an analysis can take minutes, hours, or even a day. Analysts use heuristics for promoting decisions as fast as possible: they look for known patterns of events, use their previous and mostly implicit experiences, and their knowledge on the signature set (considering some signatures or rules more reliable than others). For the decision, the experience, the context and the knowledge of the own network are essential. With a steep learning curve for this it is hard to share knowledge what is acquired on the job that relies on experiences (e.g. eyeballing long lists of logs). Seniors mostly teach juniors on the job even though both of them have high workload. As the organization size grows, the required network knowledge emerges and job roles are more distinct (system administrators, security administrators, analysts in multiple tiers with SOC or without SOC) what causes heavier reliance on collaboration. Over the time multiple solutions appeared to collect and correlate data in order to reduce the number of events, reduce false positive alerts, enhance collaboration between team members in remote locations. Nowadays SIEMs are the main software functioning in the heart of SOCs providing surface of many individual and collaborative activities.
3. *Response:* IDS analysts make intervention, feedback and reporting when responding to incidents. The intervention takes place in coordination with others both in face-to-face and virtual collaboration. The feedback in case of IDS and in modern SOCs using SIEMs means refining the signatures or rules and generating share threat intelligence information from the incident. The response phase is closed by reporting and the remediation of damages (e.g. restoring from backups).

Reviewing Goodall, Lutters, Komlodi [20] [21] and current SOC literature [3] the similarities show that over time it can be stated that the "security work is collaborative both within the organizations and across the internet". [21: 345] The authors made an important proposition to commit organizational changes besides subsequent technological efforts being made. They

identified the lack of time to analyze alerts and information overload as key issues in case of IDS analysts. Goodall, Lutters, Komlodi [20] advised the separation of monitoring (junior level) and analysis (senior level) job roles and introducing information visualization tools, to furthermore provide support for collaboration. These advices are parallel with the current trends in improving SOC efficiency.

The support of face-to-face and virtual collaboration was obviously missing from this field back in 2004, and it is still requiring major improvements nowadays. Information security teamwork is a CSCW field of collaborative problem solving under high workload, time pressure, and high risk what makes team cognition (e.g. team mental models) a key perspective to understand und provide support. Since then the issues related to staffing and transferring expertise still remained unsolved. It is now crucial to understand what knowledge, skills, abilities and other characteristics contribute to successful information security work and how to support the acquisition of these.

Since 2004 SOC are widespread that is a dedicated team working in collaboration among its members and with other teams, in a structured way. The tasks are both structured within the team and the team space (the SOC room, see Figure 1) is designed towards promoting a common understanding of the security situation. However, the virtual collaboration of remote team members appears as a growing challenge.

Challenges of Teamwork in SOCs

Goodall, Lutters, Komlodi [20] described a workplace where time pressure, monotony of time consuming but not cognitively demanding tasks, and information overload as major challenges in case of analysts; these remained major issues today also.

SOCs nowadays face challenges from both internal and external issues. A global shortage of skills and employees constrains the building of SOC teams. From the point of view of external challenges, intensive and ever more complex cyber-attacks constantly push SOCs toward applying new technology, and toward a change from a reactive to a proactive way of working, one that is based on threat intelligence and hunting activities. [22] From the perspective of internal challenges, once an SOC has been built, the task cannot be considered done. Indeed, the operation and the further development of processes, people, and technology remain crucial all along. From the people's side, collaboration within the SOC team and with other teams are specifically emphasized in recent market analyses. [23] The employee retention is a crucial internal issue compared to all others.

The emerging special segment of SOCs and security teams working together in virtual or mixed ways such as virtual SOCs (model 1), co-managed SOCs (model 3), MSSPs (model 5), or dedicated SOCs (model 4) that are monitoring companies of multiple remote locations are all facing challenges of SOCs in general and mentioned above. In order to identify the key causes of challenges in computer supported collaboration using mixed or entirely virtual channels within and between the teams we are focusing on KSAOs that make people capable to perform in a highly efficient way. The SOC models mentioned above are highly relying on virtual teamwork so the possible human factors of success can be studied. Schultze and Krumm [19] highlighted three main challenges appearing in virtual teams such as we think SOC teams are: (1) technology usage, (2) cultural differences, and (3) geographical dispersion.

Aims

In the previous research phase, we have been focusing on applying teamwork and computer supported collaborative work (CSCW) research to SOCs. [17] As a further step in this paper we are focusing on the prerequisites of a successful teamwork in this environment. We are approaching the question from the challenges of human factors, and virtual teamwork.

Security Operations Centers can be considered as fields of virtual or augmented teamwork. In our study we are aiming to identify the prerequisites of successful SOC teamwork limited to the aspects of virtual teamwork. Information security as all other fields heavily relies on dispersed teams collaborating through computer supported channels both in synchronous and asynchronous ways. The knowledge, skills, abilities and other characteristics (KSAOs) are supposed to play an important role in being effective as a virtual team working in a SOC. Are there KSAOs that promote people in SOC to perform better, stay motivated, work better as a team? We are aiming to identify the challenges and possible KSAOs relating to them using field interviews and literature research.

Methods

We have conducted 15 semi-structured field interviews with industry experts who are operating an SOC or performing tasks related to SOCs. The interviews were focused on the following topics: processes for investigating incidents, roles in the team, collaboration, tools used, levels in SOCs, time frames and escalations, what information is presented and available for the experts, the physical organization of the workplaces, the largest challenges among the daily tasks, etc. Also we included questions in case of managers that cover the employee recruitment, career planning, and learning opportunities in their SOC teams.

The experts interviewed come from the Western-, and Central & Eastern Europe region, North America, and North Africa. They operate SOCs or security organizational units in the IT, finance, governmental, research, and IT security industries. There can be found both in-house SOC operators and managed security service providers (MSSPs) among the interviewees. These interviews were combined with two field visits to currently operating SOC departments: one was an in-house SOC of an IT company, the other was a large managed SOC of an MSSP serving clients in Western Europe. This set of interviews and visits were completed with literature review, the analysis of sector-specific market researches (e.g. Gartner, Forrester), and two interviews with independent market experts. We handle all the sensitive company information anonymously and present them only as aggregated results here.

Results

We have found that SOCs show large differences in maturity levels and SOC models.

On the one hand, there are SOCs owned by enterprises only for compliance reasons, and these are not operated at their full potential. On the other hand, there are highly structured in-house and managed SOCs that focus on proactive security monitoring. The industry trend is to focus on threat intelligence and become more proactive [22] in order to keep up with the rising number of attacks.

We have found that SOC activities are separated from the overall security or operations departments in most cases. Depending on maturity, this means more specified roles, positions, and locations. Similarly, to what have been observed by Goodall, Lutters, Komlodi, [20] [21] the smaller the organization, the more roles a security expert shares in it including system administration, forensics, security administrations, etc. Summarizing the processes that these SOCs (or SOC-like teams) follow, it is important to emphasize that all of them have dedicated escalation levels with defined time frames to handle an event or incident. This is one main source of time pressure across the teams. The main activity besides event and incident handling is the setting and refining of rules. The core tool used in SOCs is a SIEM that uses rule-based alerting. These rules are reactively made based on previous and recent incidents. The rule set builds up a large knowledge base of security incidents that the SOC can detect and handle. Nevertheless, this rule set requires continuous updating as attacks tend to evolve and change over time. This is the most time-consuming and effortful activity in SOC teams. Besides SIEM other specialized tools are also used in SOCs. These tools for e.g. IDS, net flow, malware analysis, endpoint protection, firewalls, threat intelligence sources are also providing information in an incident response situation when all data available have to be analyzed. The multiple tools used cause workload by dividing attention of the users especially when the user experience of these are heterogeneous. Following the trends that Gartner [23] revealed, therefore, TI and proactive ways of working (e.g. use of machine learning) are gaining popularity to reduce the hassles caused by manual rule setting.

The interviews shed light on challenges that specifically related to computer supported cooperation of remotely located people or teams. Experts working in MSSPs mentioned that delay in working hours (because of different locations and time zones) causes interruptions in incident responses and gathering of context information. Cultural related challenges are appearing in language skill differences among distributed team members what makes different preferences in communication channels (email, phone, ticket, etc.). The knowledge of the network monitored and protected is not accurate or up-to-date enough in case of large organizations or managed SOC services providers: the system administrators or clients are neglecting providing this information to the (remote) SOC team. This lack of knowledge of the own network hinders fast understanding of event context thus the ability to respond effectively.

These findings ensure that our sample of SOC experts are representing the industry well and their experiences are a valuable foundation of identifying challenges.

Regarding human factors, it is important to note that monotony is a strong source of stress for analysts: the monitoring task is repetitive and most of the time no significant incident happens, hence vigilance has to be maintained. Most of the events examined are false positives. When something happens the time-pressure is high because the incident handling time windows are limited and sometimes regulated by SLAs. This causes high workload. This is, among others, a cause that contributes to low retention and a lack of employees in the sector. Shift working in 24/7 is the other factor that contributes to heavy workload and stress. Contrarily to other high-risk fields like aviation or utilities, in IT security people are more prone to change jobs (and leave stressful SOCs) to other IT jobs where their skills are applicable. This all together contributes to a lack of skilled security employees in the industry on every level.

The physical work settings, in every case, aim to support the visibility of information: large screens, multiple displays per workstations, and specialized light conditions. The tools analysts use are largely customized based on company requirements, for example, integrated with or even built around the ticketing system.

The roles in SOC teams are highly structured, hence the lack of skilled employees may eventually contribute to more flexibility (e.g. through job rotation) in order to support employee retention. This is an effort observed multiple times in our discussions with experts that SOC management makes in order to cope with human factors challenges. The policies, processes, and even procedures are highly defined to fit company regulation or compliance requirements.

In the SOCs studied, collaboration and cooperation are observable on multiple levels and mediated by several channels. First of all, local team members communicate within the team verbally or using email, chat for synchronous cooperation, and the ticketing system for asynchronous cooperation. The security teams observed in global companies have connections or sub-teams in various locations in the world. There is intensive communication with these remote team members using computer-mediated channels, phone calls, and rarely face-to-face meetings. These later examples are fitting the definition of virtual teams described above. Finally, there is cooperation and communication with employees of the company who are not involved in security functions. They are the "ordinary" people who can be both targets of an attack or represent an insider threat. Information exchange with employees mainly happens using email and phone calls. Reaching company employees is especially complicated in the case of a managed security service when the SOC is operated by an external company in a time zone different from the one where the customer to be protected is. These later issues mentioned by the experts interviewed are related to mixed or virtual team collaboration. All together these features of teamwork either a mixed setting where technology augments the face-to-face interaction or virtual teamwork where the team members are distributed in geolocations, working times, organizational units. This includes both in-house and managed SOC teams on a spectrum of fully virtual team who rarely meet face-to-face to a team that augment their collaboration by using communication technology.

A schematic way of incident handling in an SOC is described by Muniz and his colleagues [3] is summarized in Figure 4. This process is supported by our findings based on our interviews and visits.

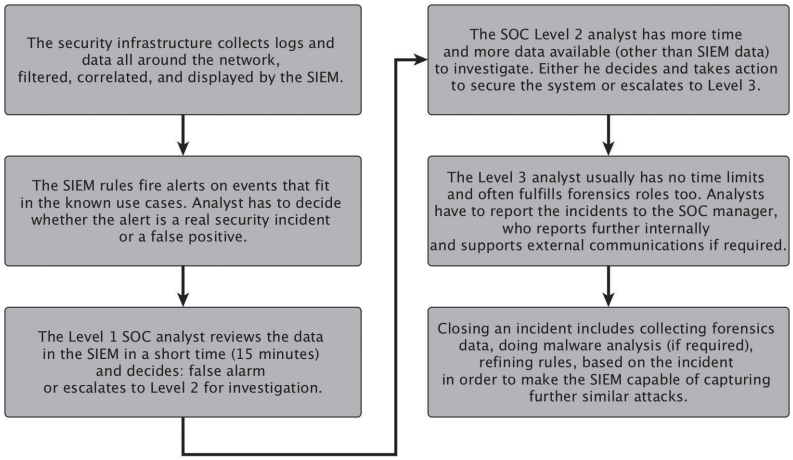

Figure 4. *The schematic steps of incident handling in an SOC is described by Muniz et al.* [Edited by the authors.]

Besides this chain of actions performed when something out of the ordinary happens, the daily routine of the SOC team consists of prescribed monitoring tasks, threat hunting for suspicious events in data, and rule refinements—these are often monotonous tasks.

Discussion

The findings summarized above prove that the information security activities performed in Security Operations Centers rely heavily on team collaboration, cooperation and on how information is shared and used in teams. These teams use multiple computer-mediated channels for working together and for collecting, displaying, storing information, and taking actions. Examples of these channels are the ticketing system, chat applications, phone calls and wikis.

There are multiple levels of remote or virtual collaboration observed in SOC teams sorted using the cells of the CSCW matrix. [16]

1. In the case of face-to-face interactions, discussions and meetings take place in the same time and space in the SOC. The large displays of events or alerts happening in real time are visible from all parts of the SOC room and they provide information in a collocated synchronous way.
2. The same large displays, dashboards, and project management tools (e.g. Jira, Slack) supporting continuous work can be used in an asynchronous way too, while analysts are changing shifts or new experts are involved in the incident response.
3. Remote interactions happen through messaging or chat tools (sometimes integrated in project management applications). The same dashboards and SIEM data are visible in multiple remotely collaborating locations of a SOC. The real-time monitoring of privileged users also fits into this cell of the matrix, that is, when an activity is remotely observed as it happens.

4. Teamwork that is asynchronous in both time and space is related to communication and coordination tools such as the project management or ticketing tools, emails, wikis (e.g. Confluence) and calendars. Threat intelligence and forensics data collection and sharing also fit into this cell.

The issues learned from interviews and field visits are matching the challenges highlighted by the research of virtual teams. Not only technology but individual and organizational factors take important roles in solving challenges that SOCs are facing nowadays. KSAOs are crucial in this set as these are the input elements of a high performing virtual team what SOCs are likely to be.

The SOCs in case of three plus one models can be considered as fields of virtual teamwork. Virtual SOCs (model 1), co-managed SOCs (model 3), MSSPs (model 5), and dedicated SOCs (model 4) when monitoring companies of multiple remote locations are all facing challenges virtual teams. These are challenges of technology usage, cultural differences, geographic dispersion (CITE Schultze). These challenges have impact on communication, coordination, cohesion, trust, performance, innovation or even on functioning. [19] These impacts cover almost every field of teamwork. The results based on the interviews verify these challenges appearing in case of SOC teams. Also the high reliance on technology in case of virtual teams in SOCs make the earlier observations of Goodall, Lutters, Komlodi [20] of IDS analysts from the perspective of CSCW applicable. Even though these have moved to the forefront of discussion in the literature, the high workload and the personnel issues remained a problematic area in the security domain. Changes in technology has to be matched with changes in the organization in order to facilitate a successful cooperative work. [20] Implementing novel tools will not solve the challenges in SOCs: organizational improvements e.g. redesigning job roles or career paths are also required to be successful.

Specifically referring to challenges and related to virtual teams, that SOCs are considered to be similar in certain cases, Schulzte and Krumm [19] provides a detailed review of literature. The authors match the challenges with relevant KSAOs which provides a framework of future research and field applications of virtual teams e.g. to SOCs.

Challenges in Virtual Teams

The main challenges appearing in virtual teams are (1) technology usage, (2) cultural differences, and (3) geographical dispersion. [19] In details the challenges consist of the following:

1. *Technology usage:* the technology used to connect team members often suppress social cues, nonverbal communication which reduces attractiveness, understanding, relationship and trust-building in virtual collaboration. [19] In case of SOCs the technology used to reach out other experts or clients often mentioned to be a source of problems and biases: they are hard to reach or the mutual understanding is missing. Especially in case of asynchronous communication (e-mail, ticketing system, wiki, etc.) the ratio of relational messages in the communication often causes feelings of uncertainty, larger demand for coordination and problem solving. It strengthens this challenge that intensive and ever more complex cyber-attacks constantly push SOCs toward applying new technology.

2. *Cultural differences:* it means differences in values, communicative behavior and language skills. Poor language skills cause anxiety which causes less communication. [19] This may lead to lack of information that is required to be shared across the SOC's dispersed team.
3. *Geographical dispersion:* meaning also configurational, spatial and temporal dispersion. It includes problems of low visibility, reduced awareness of isolated team members leading to increased coordination requirements. Team members dispersed in multiple time zones may suffer low accessibility of information (e.g. who knows the answer is out of his working hours) and reduced coordination which reduces performance. [19] In case of managed SOCs the service provider suffers problems reaching clients out of their working hours and SOC employees working in night shifts to cover the client's time zone are prone to larger workload and stress.

The interviews revealed issues in all three challenges which underline that SOCs share the problems of virtual teams as they are functioning alike in many cases. The knowledge, skills, abilities, and other characteristics (KSAOs) that considered as drivers of virtual team success are grouped into six clusters [19]:

- *Media KSAOs:* knowledge about the medium, knowing how and when to use what, and adapt to channel restrictions
- *Communication KSAOs:* enables people to communicate effectively within dispersed teams, share knowledge, interpret messages appropriately
- *Trust-related KSAOs:* the skill to develop interpersonal trust (e.g. responsiveness, dependability, active and frequent participation)
- *Intercultural KSAOs:* both knowledge and skills that help to interact with people from different (organizational-, functional-, national-) cultures
- *Self-management KSAOs:* the skill to manage oneself effectively (e.g. self-, time-, project- management)
- *Conflict management KSAOs:* the skill to constructively solve conflicts

Schultze and Krumm [19] reviewed the relevant facets of challenges and KSAOs (including motivation, experience, and personality). In case of virtual collaboration in SOCs we consider a selection of this broad review to be summarized here as a practical conclusion providing answers for issues emerged in the interviews.

Knowledge about the Challenge of Technology Usage [19]

The inadequate team communication or collaboration media choice harms teamwork. Contrarily knowledge about media channels is promoting teamwork. Consciously using media with low synchronicity helps transmitting information (conveyance). Using media with high synchronicity promotes mutual understanding in teams (convergence). The complimentary usage of communication technology also supports virtual teamwork. The more modalities are involved in the teamwork (modality augmentation) the less errors and information overhead will happen. These may apply to the selection of tools and communication channels to use in SOCs collaborating in mixed or virtual ways.

Skills about the Challenge of Technology Usage [19]

Certain communication skills support virtual teamwork through usage of technology which are applicable to SOCs. These are expressiveness, coordination (e.g. timing of emails), attentiveness, composure (e.g. how confident one is). These are important for communication within the team or between teams or with clients' communication.

Knowledge about Cultural Differences Related Challenges [19]

Cultural knowledge is a plus in any case of collaboration. Knowing how cultures perceive channels of communication technology differently reduce misunderstandings and even conflicts. It is a valid case of an organizational culture described in one of our interviews where email is the accepted channel of work orders so this is used for a trigger of forensics tasks to do. No other channels apply for this role and the knowledge about this helps to work with that team better. Similarly, email is effective in reducing language problems, miscommunications because it is asynchronous, causes less anxiety in members with lower language skills. The cultural knowledge can be shared in training programs which may have a positive effect on SOC teams' performance.

Skills about Cultural Differences Related Challenges [19]

Cross cultural communication skills acquired by team members promote teamwork in virtual collaboration. Adopting communication with partners (e.g. communicate clearly, reducing slang words) occur 80.3% in verbal and 60.7% in written communication. Verbal communication is a stronger trigger to adapt language level. This application of culture related skills lead to higher trust in the distributed team and higher performance. This facet is fitting the case of global SOCs (of large organizations) and global MSSPs providing service for culturally different clients. These skills should be assessed and developed in order to make a successful SOC team.

Knowledge about Geographical Dispersion Related Challenges [19]

The knowledge that distance hinders synchronous interactions helps to apply compensatory solutions. Regular face-to-face meetings and site visits have a positive effect on virtual teams. The same effect was observed in case of video conferences where non-verbal communication channels are more available. It has a positive effect that the team members know that asynchronous communication is good for conveying information across time zones. In general, it promotes team performance when the members know the effects of certain communication channels because it helps to choose adequately. These can be included in training programs for SOC personnel.

Skills about Geographical Dispersion Related Challenges [19]

High skills in time- and self-management supports virtually collaborating teams to plan, strategize, schedule and reduce communication delays (e.g. keeping shifted working hours

of others in mind). Communication skills applied adequately by providing contextual information promotes shared identity of the team and trust. The same effect is related to frequent and spontaneous communication. Such skills may be the characteristics to look for in SOC employee selection or to develop in training.

Motivation

Motivation plays an important proximal role in virtual team performance. Motivation towards technology usage may appear perceived usefulness of tools or even in computer anxiety which are determining factors in technology usage. [19] Organizations having SOCs or using managed security services have high compliance regulations (e.g. financial sector) where early adoption to new tools and technology is rare. Thus, motivation towards the usage of virtual teamwork related technology may appear constrained. Motivations related to cultural differences in virtual teams appear as a fear of communication in foreign languages or high cultural intelligence as a better case. [19] These motivations can either be perceived or shaped by SOC management. Motivational issues are related to geographical dispersion of the teams for example the feeling of anonymity, low social control, low visibility of own/other team can end up in social loafing which reduces performance. [19] Contrarily trust, coordination, goal setting, self-efficiency promoting motivation of team members dispersed in various locations. Geographic locations per se have an effect on motivation which has to be considered in case of virtually collaborating SOC teams or using managed services.

Experiences

Experiences of team members with virtual team work have a positive effect on coping with all three challenges. [19] Experiences with technology shapes the media channels' perception. Intercultural experiences are precursors of culturally intelligent acting. Dispersed work experiences support self-efficacy which promotes performance. This is applicable to SOCs when searching for employees: experiences with virtual teamwork and its challenges predict better performance.

Personality

Personality characteristics are the less studied area in this field. On a high level, the openness factor of the personality has a positive effect on adaptation to new technology and learning about other cultures. [19] Personality factors may be measured in selection, so looking for high openness in SOC applicants' tests could promote to hiring the right people.

Conclusion

It is important to take into account the fact that not all people are equally capable of working together in teams using computer supported collaboration e.g. virtual collaboration tools. Krumm and colleagues' [24] [25] broad research revealed different sets of knowledge, skills, abilities and other characteristics (KSAOs) that affect virtual teamwork.

SOCs are extensively relying on virtual teamwork especially in case of virtual SOCs (model 1), co-managed SOCs (model 3), MSSPs (model 5), and dedicated SOCs (model 4) when monitoring companies of multiple remote locations. The challenges related to virtual teams were observed in the interviews conducted in this research phase. Focusing on this special and emerging subset of SOC, the virtual team performance related KSAOs proved to be applicable.

These KSAOs can be learned, trained, or looked for in case of selection. These promote SOC team performance and reduce the turnover in SOC personnel. These can be considered as prerequisites of effective virtual teamwork in SOCs. Exactly what KSAOs may be relevant that depends on the working conditions of the teams: the virtual team performs at the highest level when the members have the knowledge, skills, and motivation relevant to the setting.

In a broader perspective: the work of information security teams using computer supported means of collaboration (e.g. virtual or mixed teams) cannot only be supported by new technology but human factors have to be taken into consideration. Changes of technology should be accompanied by organizational changes or support. It requires a perceptive management that perceives the SOCs and all information security activities as socio-technical systems. [20] Goodall et al as an example of that suggested refining roles and positions, designing an effective information visualization tool to enhance IDS analysts work and promote employee retention, and satisfaction despite high workload. Following the authors perspective of CSCW and adding virtual teamwork with the KSAOs predicting high performance we consider that SOC teams have to be studied, supported, and managed in a complex way. This should include technology to provide data, technology to enable collaborative work of dispersed members and knowledge, skills, abilities, and other characteristics to promote a high performance in this setting.

As a practical conclusion identified challenges appearing in SOCs related to virtual teamwork and KSAOs enabling performance to focus on. These KSAOs may help coping with the challenges: finding the right people, develop the people, retain talents, provide leadership guidance in SOCs. This completes the fast-evolving technology in information security industry by adding human factor and interpreting SOC work as a socio-technical system.

This conclusion can be also useful within the military. We should not forget that more and more cadets start serving from Generation Z with deep skills in IT and an option to leave service and start a new career in the private sector. Meanwhile, the threat agents in cyberspace will not be reduced. Officers and politicians responsible for national cyber defense have to keep in mind this generation change and should establish this cultural and environmental change. Cyberspace is the fifth domain of warfare where new strategies and tactics appear on the attacker side day by day, therefore we have to rethink the defense capabilities as well.

References

[1] KASSAI K.: A 2013. évi L. törvény végrehajtása érdekében a magyar honvédségnél szükséges elektronikus információvédelmi szakfeladatok. *Hadmérnök*, 8 (2013), 191–200.

[2] DIETRICH, R., CHILDRESS, T. M.: *Group Interaction in High Risk Environments*. Farnham: Ashgate Publishing Ltd., 2004.

[3] MUNIZ, J., MCINTYRE, G., ALFARDAN, N.: *Security Operations Center: Building, Operating, and Maintaining your SOC*. Indianapolis: Cisco Press, 2015.
[4] FORTE, D.: An Inside Look at Security Operation Centres. *Network Security*, (2003), 11–12.
[5] AHMAD, A., MAYNARD, S. B., SHANKS, G.: A Case Analysis of Information Systems and Security Incident Responses. *International Journal of Information Management*, 35 (2015), 717–723. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.08.001
[6] LEVI, D.: *Group Dynamics for Teams*. Thousand Oaks: SAGE, 2011.
[7] MOHAMMED, S., KLIMOSKI, R., RENTSCH, J. R.: The Measurement of Team Mental Models: We Have No Shared Schema. *Organizational Research Methods*, 3 (2000), 123–165. DOI: https://doi.org/10.1177/109442810032001
[8] KLIMOSKI, R., MOHAMMED, S.: Team Mental Model: Construct or Metaphor? *Journal of Management*, 20 (1994), 403–437. DOI: https://doi.org/10.1177/014920639402000206
[9] BANKS, A. P., MILLWARD, L. J.: Differentiating Knowledge in Teams: The Effect of Shared Declarative and Procedural Knowledge on Team Performance. *Group Dynamics: Theory, Research, and Practice*, 11 (2007), 95–106. DOI: https://doi.org/10.1037/1089-2699.11.2.95
[10] JUHÁSZ M., SOÓS J. K.: Impact of Non-technical Skills on NPP Teams' Performance: Task Load Effects on Communication. *2007 IEEE 8th Human Factors and Power Plants and HPRCT 13th Annual Meeting.* Monterey, 26–31 Aug. 2007.
[11] HUTCHINS, E.: *Cognition in the Wild*. Cambridge: MIT Press, 1995.
[12] GROTE G., ZALA-MEZÖ E.: *GIHRE-Kolleg (Group Interaction in High Risk Environments) of the Daimler-Benz-Foundation—Report on the Psychological Part of the Project "The Effects of Different Forms of Coordination in Coping with Work Load: Cockpit Versus Operating Theatre."* Zürich, 2004.
[13] CARSTENSEN, P. H., SCHMIDT, K.: Computer Supported Cooperative Work: New Challenges to Systems Design. In: In K. Itoh (Ed.): *Handbook of Human Factors*, (1999), 619–636.
[14] WILSON, P. A.: *Computer Supported Cooperative Work: An Introduction*. Bristol: Intellect ltd., 1991.
[15] BAECKER, R. M., GRUDIN, J., BUXTON, W. A. S., GREENBERG, S.: Readings in Human-computer Interaction: Toward the Year 2000 (2nd ed.). *System*, (1995), 595.
[16] *The CSCW Matrix*. https://commons.wikimedia.org/wiki/File:Cscwmatrix.jpg. (Downloaded 20.07.2017)
[17] HÁMORNIK B. P., KRASZNAY Cs.: A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. In: NICHOLSON, D. (ed.): *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17−21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA.* 224–236. Springer International Publishing, Cham, 2017.
[18] LIPNACK, J., STAMPS, J.: *Virtual Teams: Reaching Across Space, Time, and Organizations with Technology*. New York: Wiley, 1997.
[19] SCHULZE, J., KRUMM, S.: The "Virtual Team Player." *Organizational Psychology Review*, 7 (2017), 66–95. DOI: https://doi.org/10.1177/2041386616675522
[20] GOODALL, J., LUTTERS, W., KOMLODI, A.: The Work of Intrusion Detection: Rethinking the Role of Security Analysts. *AMCIS 2014 Proceedings*, (2004), 1421–1427.

[21] GOODALL, J. R., LUTTERS, W. G., KOMLODI, A.: I Know My Network: Collaboration and Expertise in Intrusion Detection. *ACM Conference on Computer Supported Cooperative Work*, (2004), 342–345. DOI: https://doi.org/10.1145/1031607.1031663

[22] BARROS, A., CHUVAKIN, A.: *How to Plan, Design, Operate and Evolve a SOC.* Stamford: Gartner, 2016.

[23] CHUVAKIN, A.: *New Research Starting Soon: Threat Intel, SOC, etc.* http://blogs.gartner.com/anton-chuvakin/2016/05/11/new-research-starting-soon-threat-intel-soc-etc/ (Downloaded 20.07.2017.)

[24] KRUMM, S., KANTHAK, J., HARTMANN, K., HERTEL, G.: What Does It Take to Be a Virtual Team Player? The Knowledge, Skills, Abilities, and Other Characteristics Required in Virtual Teams. *Human Performance*, 29 (2016), 123–142. DOI: https://doi.org/10.1080/08959285.2016.1154061

[25] KRUMM, S., HERTEL, G.: Knowledge, Skills, Abilities and Other Characteristics (KSAOs) for Virtual Teamwork. In. BAKKER, A., DERKS, D. (eds.): *The Psychology of Digital Media and Work.* East Sussex: Psychology Press, 2012.