International Journal of Information Security (2025) 24:217
https://doi.org/10.1007/s10207-025-01106-z

REGULAR CONTRIBUTION

Cyber situation awareness during an emerging cyberthreat: a case study

Annika Andreasson[1] · Henrik Artman[2] · Joel Brynielsson[2,3] · Ulrik Franke[2,4]

Accepted: 22 July 2025
© The Author(s) 2025, corrected publication 2025

Abstract

The digitalization of our societies makes them increasingly vulnerable to emerging cyberthreats. These cyberthreats can manifest themselves in the form of organized, sophisticated, and persistent threat actors, as well as nonadversarial mistakes. Staff involved in responding to cyberthreats and handling incidents in organizations need cyber situation awareness. This paper presents a case study on what challenges members of staff involved in cybersecurity in a large, complex organization experience when developing cyber situation awareness while handling a remote code execution vulnerability in the form of Log4Shell. Two types of qualitative empirical material were used for the case study, data collected through semi-structured interviews with ten informants, and internal documentation. The empirical material was analyzed to create a timeline of events in the organization. The results show how information about the threat spread throughout the organization, the types of artifacts that served as common operational pictures, and the role played by information sharing in maintaining staff cyber situation awareness. Three major challenges to the organization were found: (i) information sharing among staff was not effortless, (ii) there was no organization-wide common operational picture established, and (iii) inaccurate information was shared. This study adds a real-world contribution to the literature on organizational handling of cyberthreats.

Keywords Cyber situation awareness · Common operational picture · Cybersecurity · Public sector · Log4j · Log4Shell

1 Introduction

In a highly connected digital world, organizations face cybersecurity challenges with the potential to compromise their operations and reputation. The increasing sophistication of cyberattacks, in combination with growing attack surfaces, has made the handling of diverse cyberthreats an important aspect of cybersecurity operations.

Software vulnerabilities are among the cyber risks that organizations face on a day-to-day basis. A vulnerability, according to National Institute of Standards and Technology (NIST) [1], is a "[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." The number of vulnerabilities published by the Common Vulnerabilities and Exposures (CVE) Program has rapidly increased. In 2024, 40,257 vulnerabilities have been reported, which is almost twice as many as reported in 2021.[1] The increase in reported vulnerabilities requires organizations to prioritize among them [2], which in turn necessitates the development of methodology to be able to measure and maintain a high level of operational effectiveness [3, 4]. To evaluate the severity of a vulnerability, the Common Vulnerability Scoring System (CVSS) is a standardized framework for calculating a CVSS score, ranging from 1 to 10 with 10 being the most severe, with a formula that considers various metrics that reflect how easy it is to exploit the vulnerability and the potential impact of such an exploit.[2]

A central component in the effort to respond to cyberthreats is the concept of cyber situation awareness (CSA). Having a good CSA gives staff involved in the handling of a cyberthreat an understanding of "what's going on" [5]. While

✉ Annika Andreasson
annika.andreasson@hhs.se

[1] Stockholm School of Economics, Box 6501, SE-113 83 Stockholm, Sweden

[2] KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden

[3] FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden

[4] Swedish Defence University, Box 278 05, SE-115 93 Stockholm, Sweden

[1] https://www.cvedetails.com/.

[2] https://www.first.org/cvss/.

Published online: 26 September 2025

CSA research has matured, there is still a lack of empirical research on CSA [6], and there is also a lack of research looking at the needs of CSA among different roles in an organization [5]. A notable exception is the focused study of roles in a security operations center (SOC) performed by Ofte [7], which was conducted using a cognitive task analysis technique [8] called goal-directed task analysis (GDTA) [9].

This paper addresses the research gap by presenting a case study of how staff in a large and complex public sector organization providing vital societal functions develop CSA while handling an emerging cyberthreat in the shape of CVE-2021-44228,[3] a critical vulnerability in the ubiquitous Apache Log4j Java-based logging library with a CVSS version 3.1 score of 10.0. The study explores how staff report that they developed CSA for handling the vulnerability, from the initial awareness of the vulnerability, the creation of common operational pictures to support CSA, to aspects of organizational information sharing. As far as is known, the vulnerability was not exploited to attack the organization, but this was not clear at the time, and this is a study of staff struggling to establish situation awareness about this cyberthreat. This research aims to contribute to the empirical cybersecurity literature by providing insights on challenges to CSA in organizations, by answering the following research question:

- What challenges do staff involved in cybersecurity work in a large, complex organization experience when developing cyber situation awareness while handling an emerging cyberthreat?

The research question was addressed through the following sub-questions:

- How did information about the emerging cyberthreat spread to staff involved in the handling of the threat throughout the organization?
- What common operational pictures existed to aid staff cyber situation awareness while handling the emerging cyberthreat?
- What were the staff experiences of information sharing for cyber situation awareness during the handling of the emerging cyberthreat?

The rest of the paper is organized as follows. Section 2 provides background and discusses related work. Section 3 explains the method used for this study. Section 4 outlines the results, which are then discussed in Section 5. Section 6 concludes the paper and presents ideas for future research.

2 Background and related work

This section describes the organizational context in which the study is conducted and gives an introduction to the Log4j vulnerability. It also provides an introduction to the concepts cyber situation awareness and common operational picture. Finally, it reviews previously performed qualitative studies on cyber situation awareness.

2.1 Organizational context

The organization studied here is a large and complex one, distributed over several different companies and administrative sections located in Sweden. To safeguard anonymity, identifying specifics have been excluded. The organization is complex in the sense described by Dooley [10]: "[o]rganizational complexity is defined as the amount of differentiation that exists within different elements constituting the organization [and] can also be observed via differentiation in structure, authority and locus of control, and attributes of personnel, products, and technologies."

The main purpose of the organization is to provide vital societal functions covered by Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive). General IT services are provided by the Service department (SD), where there is also an Incident management (IM) function. At the Main office, there is an IT director and a CISO in charge of an Information security unit, which hosts a computer emergency response team (CERT). Some of the subsidiaries have their own independent IT departments. In addition, the main organization and subsidiaries use the same systems and services to a large extent.

2.2 The Log4j vulnerability

The Log4j remote code execution vulnerability CVE-2021-44228,[4] also known as Log4Shell, is a critical security vulnerability. The vulnerability was discovered in the Apache Log4j logging library, which is widely used in Java applications, and disclosed privately to Apache by the security team at Alibaba Cloud on November 24, 2021 [11], with the CVE-2021-44228 being published on December 10, 2021. Briefly explained, the vulnerability allows attackers to execute arbitrary code on systems with vulnerable Log4j versions by sending a request that Log4j logs, making it trivial to exploit. For an attack methodology example, see Doll et al. [12]. The vulnerability was assigned a CVSS score of 10, which is the highest possible score, by NIST analysts.

[3] https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

[4] https://www.cve.org/CVERecord?id=CVE-2021-44228.

As (i) Log4j is used ubiquitously in Java, (ii) the vulnerability is easy to exploit, and (iii) the mitigation of this risk is resource-extensive, this vulnerability had the potential to have a massive global impact, which was recognized by cybersecurity agencies worldwide. The national agencies Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), the United Kingdom's National Cyber Security Centre (NCSC-UK), and the U.S. agencies Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and National Security Agency (NSA) collaborated to issue a joint statement to warn organizations about the potential threat.[5] Also, news about the vulnerability was published in traditional media outlets, where it was referred to as "the most critical vulnerability of the last decade" [13]. Professionals working to address the vulnerability started up crisis management [12], and cybercriminals quickly sought to exploit the vulnerability [11]. The vulnerability affected several organizations all over the world. For more detailed timelines and analyses, see Doll et al. [12] and Hiesgen et al. [11]. It is important to note, however, the difference between a vulnerability being present, and the vulnerability actually being exploited.

2.3 Cyber situation awareness

Situation awareness (SA) has become an important concept within the field of cybersecurity. In the literature, there are a number of theories and definitions of SA suggested [14]. Among the proposed definitions, Mica Endsley's definition of SA as "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" is an intuitive and widely accepted cognitive model [15]. This model comprises three tiers: (i) perception (level 1 SA), (ii) comprehension (level 2 SA), and (iii) projection (level 3 SA) [15]. This means that an actor observes and detects various elements in the environment, which constitutes level 1 SA. The information elements are processed and interpreted to form an understanding of the situation, constituting level 2 SA. Using this understanding, the actor can predict possible future scenarios and outcomes, thereby reaching level 3 SA. This cognitive process enables an actor to assess the environment, grasp the context, and make informed decisions based on current understanding and anticipated future states.

For the cyber domain, improved situation awareness has been identified as a way to strengthen cybersecurity [16]. Franke and Brynielsson [17] take cyber situation awareness (CSA) to be a subset of SA specifically concerning the cyber environment, to be combined with other elements for an overall situation awareness. However, the application of SA models to the cyber domain presents unique challenges. One significant issue is the constraint of "time and space" in Endsley's definition. Franke et al. [5] point out that the cyber environment often transcends conventional temporal and spatial boundaries, with threat actors capable of launching attacks from anywhere in the world while obfuscating their origin. In addition, cyber events can occur at vastly different speeds, from almost instant attacks to longer-term data exfiltration. In previous work, an even more in-depth discussion and comparison of these differences can be found [18].

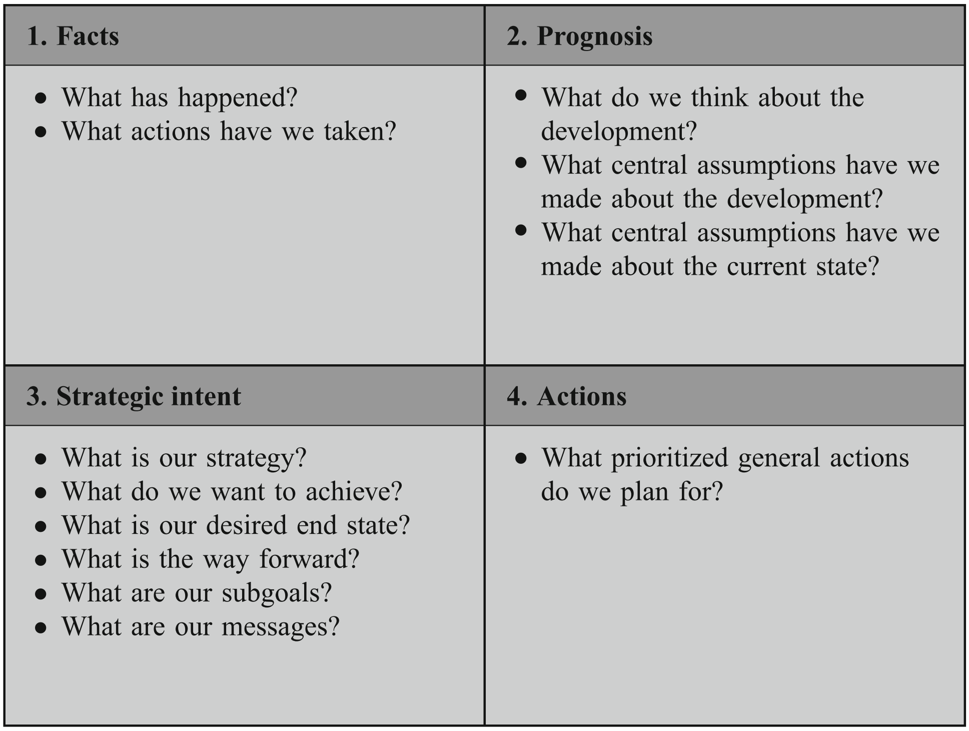
In their systematic literature review of CSA, Franke and Brynielsson [17] looked at all aspects of CSA research. Since then, there have been more specialized literature reviews such as Ofte and Katsikas [19] looking at CSA in SOCs, or Jiang et al. [20] looking at visualizations for CSA. Looking at the Swedish context, a recent study by Andreasson et al. [21] highlighted challenges faced by cybersecurity staff at Swedish government authorities in achieving adequate CSA, due to limited access to relevant information elements and a lack of national-level support.

2.4 Common operational picture

The common operational picture (COP) is a concept closely linked to SA. While SA represents the cognitive state of an actor having awareness, the COP is an artifact designed to provide actors with a representation of relevant information to aid the actor's SA [5]. The origin of COPs can be traced to the military, where they often consist of a map with representations of units showing their tactical activities. COPs are now also frequently used in crisis management as a tool for enhancing information exchange and for supporting SA among responders [22]. The COP has evolved from an "information warehouse," where information is stored, to a "trading zone," where actors negotiate information to make sense of it [23]. In the Swedish context, the Swedish Civil Contingencies Agency's guideline "Gemensamma grunder för samverkan och ledning vid samhällsstörningar" [Common bases for collaboration and management in the event of societal disruptions], henceforth "Common bases," highlights that information sharing and communication between actors are fundamental to crisis management and points to the importance of effective COPs [24].

For the cyber domain, the development of COPs presents both challenges and opportunities. Traditional COP frameworks, such as those suggested in "Common bases," may require adaptation for cyber events. The Swedish financial sector's public-private partnership, FSPOS, has identified four areas to be included in their crisis management

[5] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a.



1. Facts	2. Prognosis
• What has happened? • What actions have we taken?	• What do we think about the development? • What central assumptions have we made about the development? • What central assumptions have we made about the current state?
3. Strategic intent	**4. Actions**
• What is our strategy? • What do we want to achieve? • What is our desired end state? • What is the way forward? • What are our subgoals? • What are our messages?	• What prioritized general actions do we plan for?

Fig. 1 Example of a "quadrants" COP, used in the Swedish financial sector. Adapted from "Cyber-threat perception and risk management in the Swedish financial sector," by Varga et al. [25]

"quadrants" COP: facts, prognosis, strategic intent, and actions [25]. The FSPOS COP takes the shape of four quadrants put together as can be seen in Fig. 1.

In other work, Varga et al. [26] aim to identify what information should be included in a national-level COP to aid CSA for national-level actors. One identified gap is that actors mainly focus on maintaining their own operations and care less about other actors' information needs, indicating a need for additional information-sharing procedures.

One idea for future work in this area is suggested in the literature on visualizations for cybersecurity, namely to explore the development of individually tailored COPs, where each role involved can have its own COP [20, 27]. In other work, the focus is more on the selection of information, and that the selection itself forms the basis for developing flexible, individually tailored COPs where the essential information, possibly originating from different organizational units, for cybersecurity reporting forms the basis for which COP is most suitable [28].

2.5 Qualitative studies on cyber situation awareness

While it may be challenging to get access to the wide range of roles involved in cybersecurity in large, complex, organizations [29, 30], there is a growing empirical literature on CSA, for example, related to incident response (IR). Ahmad et al. [31] conducted a case study in a large financial institution to investigate how organizations can develop CSA for incident response. The case study shows how the organization's IR capabilities have been refined through the utilization of previous cyberattack experience [31]. One step taken is to form a special security leadership team, when needed, to handle critical incidents [31]. This team consists of different cybersecurity leads headed by a chief information security officer (CISO) and acts through communication bridges to management and operations to ensure that all stakeholders are informed and on board during the handling of incidents [31]. The case study also offers a process model that shows how management practice plays a part in acquiring CSA for IR [31].

In a qualitative field study of three computer security incident response teams (CSIRTs) from government, academia, and the private sector, Nyre-Yu et al. [32] identified and ranked eleven themes related to IR. The four top themes concerned (i) the necessity of communication, feedback, and accountability for incident response, (ii) the importance of having organizational alignment on security priorities, (iii) the importance of continuity of awareness and documentation, and (iv) the need for diverse skills in incident response [32]. An interesting finding is that the tiered, and sometimes distributed, organization of SOCs can create barriers for staff sharing expertise and for staff collaborating between tier levels during incident response, which can affect security outcomes [32].

Other recent literature looks at how actors handle specific cyberthreats. For example, Ofte and Katsikas [33] used a case study of the Sunburst attack to investigate how critical infrastructure operators of cyber-physical systems decide between allowing a compromised system to run so that operations can continue, or shutting the systems down in order to withstand an attack and thus halting operations [33]. The authors combine interview data and incident reports related to the Sunburst attack to outline the decision-making processes of the actors [33]. Then they make a comparison between that decision-making process and known SA models. The authors find that Endsley's SA model [15] is not in any major conflict with their model, but that Endsley's model has an individual focus, while their logic model takes the organizational perspective into account [33].

There is also literature highlighting the different perspectives and priorities of staff with respect to cybersecurity. A study presenting field work by Bartnes et al. [34] examines the challenges faced by Norwegian critical infrastructure companies in improving their information security incident management practices. It points to the need for a structured response capability influenced by organizational, human, and technological factors [34]. The results show that training for incident response is often viewed as not being a priority, and that there are different views on the importance of information security among different roles in organizations [34]. Another finding is that a lack of experience with major incidents has led to complacency regarding preparedness for such incidents, and that insufficient training and documentation hinder effective incident management [34]. Bartnes et al. suggest that establishing cross-functional teams for incident response can bridge gaps in understanding between IT and control system staff [34]. They also stress that in order to instill an organizational culture of learning, it is important to conduct and evaluate training for improved SA, as well as to conduct lessons learned after incidents [34].

While the studies reviewed in this section share a focus of examining CSA and incident experience, they are also different from the case study presented here. This case study is interesting as (i) the case presented involves actors from several parts of a large, complex organization rather than just SOC staff, and (ii) it examines the handling of a particular cyberthreat in the form of a vulnerability.

3 Method

A qualitative research approach was taken to explore how staff involved in cybersecurity work in a large and complex organization develop cyber situation awareness while handling an emerging cyberthreat. A single case study was undertaken to look at a phenomenon for in-depth understanding. Two types of qualitative empirical material were used for this case study: data collected through semi-structured interviews and internal documentation (for more on these methods, see Yin [35]). The choice of organization was made based on that it is a large and complex organization that was also willing to share documentation and agreed to be interviewed about how they worked to address the Log4j vulnerability. There had also been frustration in the organization over the fact that different parts of the organization responded to the event in different ways, leading to an organizational interest in shedding more light on the response.

The phenomenon studied is cyber situation awareness for roles involved in handling the Log4j vulnerability in a single complex organization during December 9–20, 2021. These dates span the time from when the organization became aware of the vulnerability to the time of the last organizational CERT message sent out about the vulnerability.

3.1 Informants

The informants interviewed for this study were selected based on their involvement in handling the Log4j remote code execution vulnerability and their need for cyber situation awareness. Ten informants were interviewed during April–May, 2023. Table 1 outlines their roles and time in that role at the time of the event. All informants had the same role at the time of the interviews as at the time of the event,

Table 1 Informants' roles and time in role at the time of the event (*S* Subsidiary, *C* Consultant)

	No.	Role	Years in role
Initial	1	IT security strategist	5
	2	CERT manager	3
	3	CERT technical lead (*C*)	3
	4	CISO	9
Snowball	5	IT director	10
	6	IT manager (acting CIO) (*S*)	6
	7	Information security coordinator (*S*)	5
	8	Process lead incident management	3
	9	Manager digital infrastructure	2 months
	10	Duty officer	6

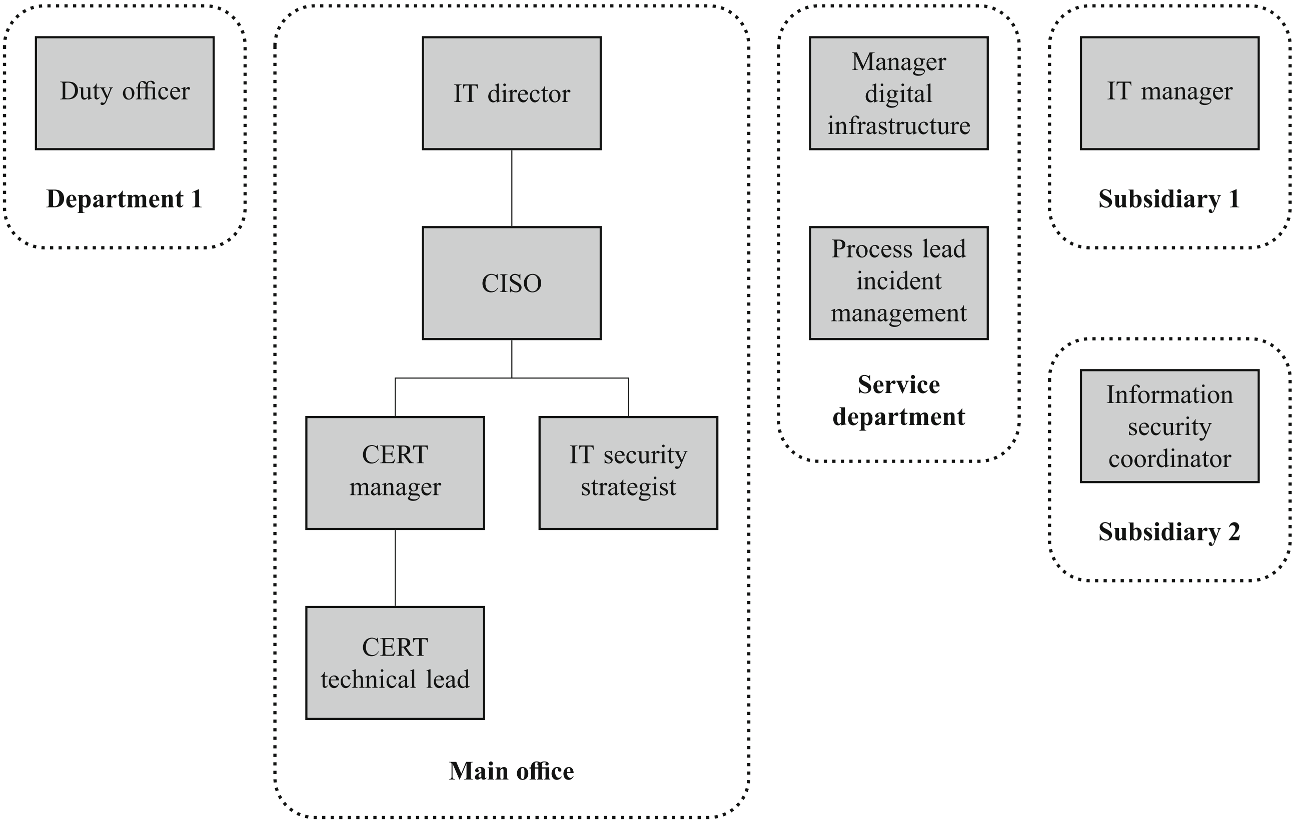


Fig. 2 Informants in their organizational units

with the exception of *CERT technical lead*, who had made a planned role change to CERT analyst. The informants *IT security strategist*, *CERT manager*, *CERT technical lead*, and *CISO*, who are working in the same section of the organization, were scheduled for the first phase, and the research team then requested to interview additional informants based on persons and roles mentioned in the interviews with the initial informants. This way, persons of interest were identified based on the empirical data collected in a snowball fashion [36]. As the organization is complex (see Section 2.1), all informants are not in direct hierarchical relations to each other, but are rather connected through the nature of the event. An overview of the informants' positions in the organization is presented in Fig. 2.

3.2 Interviews

The interviews were scheduled for 90 minutes and were conducted in person with informed consent at the informants' organization, either in the CERT offices or at the offices of the external organizations. Due to the sensitive nature of the interview subject, the interviews were not recorded. Instead, the first author conducted all interviews with one of the coauthors taking notes. After the interviews, the notes were written up and reviewed by the interviewer and the note-taker to ensure agreement on what the informant had stated. Once the interviews had been documented, they were printed and shared with the informants to give them the opportunity to clear up any remaining misrepresentations or provide additional information.

At the start of the interview, the research team introduced themselves and the interviewer gave a brief description of the context and purpose of the interview, and then presented the informant with a consent form to sign, and informed the informant that they could stop the interview whenever they wanted. The informant was also informed that they have the right to withdraw consent to participate at any time in accordance with Swedish law. The informant was then asked if they had any questions and if they agreed to participate in the study. If the informant agreed, they signed the consent form, which was then collected by the interviewer. All the approached informants consented to participate. The interview guide (see Appendix A) was designed with a flexible structure centered around four key areas, allowing informants to freely share their experiences. The four key areas were: (i) about the informant, their duties, and organizational context, (ii) about the event, (iii) after the event, and (iv) system support.

Since the focus of the study was to explore how staff in a large complex organization developed cyber situation awareness while handling an emerging cyberthreat, the interviews were structured around the informant's role and organizational context, how they became aware of the vulnerability and how they developed an understanding of what was going on individually and with their colleagues, if the event had provided an opportunity for learning, and if they lacked system support to handle the vulnerability. The interview started with the informant's own role and then proceeded to the event, where the informant was allowed to speak freely. If the informant covered a question that appeared later in the interview guide, the interviewer checked off the question, and the notetaker recorded the response where appropriate while the interviewer continued asking questions. While the interviews were scheduled for 90 minutes, the actual interviews lasted between 45 minutes and 3 hours. If the interviewer noted that an informant needed more time to respond, the interviewer asked if the informant was available for longer than scheduled, and if the interviewer noted that the informant responded swiftly, the interview was terminated when the questions were asked and the informant had nothing more to add.

3.3 Documents

Documents also formed part of the empirical material. Some of the documents were made available to the researchers to take off-site, and some documents were only available to access on-site. Three types of documents were accessed: (i) the common operational pictures created in the organizational CERT (listed in Table 2), (ii) the CERT messages sent out (listed in Table 3), and (iii) the timelines created in different parts of the organization (listed in Table 4). The CERT COPs were studied on-site and the CERT messages, in addition to the timelines, were shared with the research team.

3.4 Analysis

The empirical material was qualitatively analyzed with a focus on the three research sub-questions: (i) how did information about the emerging cyberthreat spread to the staff involved in the handling? (ii) what common operational pictures aided their cyber situation awareness? and (iii) how did the staff experience information sharing during the event? First, a spreadsheet was created with the interview guide questions and the responses of each informant. Then, the responses from the informants to specific questions were read, reread, and compared to each other as well as the documentation to create a sequential order of events. If responses relevant to one question appeared in another question, notes were taken to ensure that the response was considered in the relevant context. These events were put together into a narrative detailing the experience of how the event unfolded over time as expressed by the actors and through the documentation.

The iterative reading of the material had a focus on common operational pictures and how the staff experienced information sharing during the event. The informants' mentions of common operational pictures and their use were compared to identify what types of common operational pictures were mentioned, their usage, where in the organization they were used, and if they were helpful to the respondent. For informants' experience of information sharing, the material was read to identify different types of information-sharing situations that had had an impact on their cyber situation awareness.

To validate the results, a draft version of the paper was shared with the organization. This provided an opportunity for the organization to provide feedback on the chain of events and how the organization is described from an anonymization perspective.

4 Results

This study set out to explore the challenges for staff involved in cybersecurity work in a large, complex organization to develop cyber situation awareness while handling an emerging cyberthreat. This section presents a history of how the actors experienced the event, what common operational pictures were used to inform their cyber situation awareness, and, finally, how they experienced information sharing when handling the event.

4.1 The Log4j vulnerability as experienced by the actors

This section provides an outline of how the actors involved throughout the organization experienced the Log4j vulnerability handling. This history takes the initial discovery as a starting point and ends with the situation ebbing out.

4.1.1 Calm before the storm

On Thursday December 9, 2021, *CERT technical lead* hears about a possible vulnerability from an external colleague and reflects on how it potentially could affect the organization's operations. Vulnerabilities are a common occurrence in ICT, and patches are often distributed quickly by suppliers upon disclosure, so this is business as usual. The following day, the CERT receives additional information from trusted external sources stating that the vulnerability might be rated "critical," and the CERT analysts feel compelled to issue a CERT message stating that there is a critical vulnerability in the

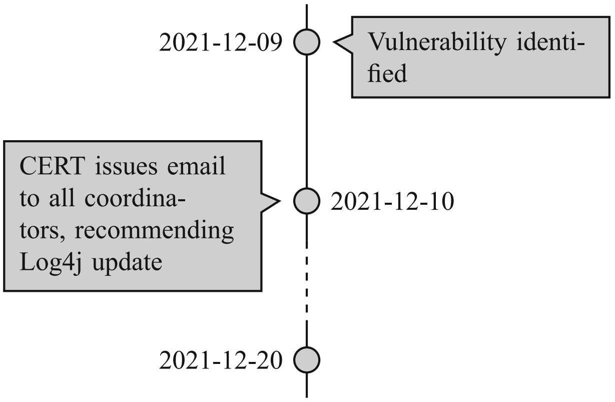

2021-12-09
Vulnerability identified
CERT issues email to all coordinators, recommending Log4j update
2021-12-10
2021-12-20

Fig. 3 Events mentioned in the documentation for December 9–10, 2021

Java library Log4j, but currently without an official severity classification (email E1 in Table 3 in Appendix B). The email message is sent to an email list with all security information contacts at 15:12 in the afternoon of Friday, December 10. At least four of the informants are informed about the vulnerability this Friday.

CERT technical lead has already started to look for information about the vulnerability on /r/netsec[6] and other sources, and has no memory of the national CSIRT, CERT-SE, issuing an alert about the vulnerability when starting to search for additional information. *Information security coordinator* and *Process lead incident management* mention that they were informed by other colleagues about the possible vulnerability, whereas *CISO* reads about the vulnerability in an external information-sharing channel. The main events mentioned in the documentation are outlined in Fig. 3.

Remarks: At this point, the vulnerability is viewed as any other vulnerability the organization encounters. Information regarding vulnerabilities can reach the organization from various sources. As a CERT, the decision to inform the organization about a vulnerability indicates that the vulnerability has a certain severity level. That in itself does not necessarily mean that the organization is immediately threatened.

4.1.2 Red alert—gale and dark skies

On Saturday morning, approximately at the same time, a couple of informants are reached by different external sources. A service provider, where the organization also has a partial ownership stake, henceforth the supplier, phones both *CISO* and *IT director*. According to *IT director*, the supplier phones to call for a meeting, which *CISO* and *IT director* attend. The meeting is for the IT directors of all national organizations with similar mission as the organization, and in this meeting the supplier states that they need to shut down a system or service due to the discovered vulnerability. *IT director* recalls that the meeting feels disorganized and tense, creating more concern than rationality. At the meeting, all the participating organizations together decide on having daily meetings at the national sector level. This decision signals the severity of the situation.

CISO calls *CERT manager* and relates that the supplier says that the vulnerability “has been exploited.” *CISO* calls their external senior advisor (who is also *CERT technical lead*’s consultancy manager) for a consultation about the situation. After meeting and discussing with the senior advisor and *CERT manager*, respectively, *CISO* says they make the decision that the CERT should activate a heightened alert. *CISO* also draws up recommendations for *IT director*, who in turn contacts the most senior civil servant of the organization. The media image of the vulnerability is that the “internet is on fire” according to *CISO*, and that it is “potentially the worst thing happening ever” as recalled by *CERT manager*. Meanwhile, *CERT technical lead* receives a call from their consultancy manager, who recommends that the CERT activates the standard operating procedure for anomalous events. To monitor the situation, *CERT technical lead* immediately starts checking logs and setting up alerts for attacks trying to use the vulnerability. When alarms start going off, they assume the responsibility of anomalous event lead, as they think the organization is vulnerable and the threat credible. At 14:00 on Saturday everyone is informed and staff is in place, according to *CISO*.

In other parts of the organization, *Information security coordinator* is called up for duty for Sunday by their IT manager at the subsidiary. *Duty officer* recalls being called by *CISO* or a member of the CERT, and made aware of a potentially serious situation. *CISO* and *Duty officer* proceed to divide the tasks of informing the communications department and the officer with the mandate to stop operations for safety reasons, respectively. Proactively, *Duty officer* prepares a “quadrants” COP, as described in Section 2.4, to be able to quickly share a COP in case there is a need to activate organization-wide crisis management. *Duty officer* also contacts an off-duty duty officer to safeguard the collective memory of the events by sharing what they currently know with another duty officer, who is then better prepared and briefed about the current situation should the need to escalate arise. The first impression of the current situation is that it will escalate, and *Duty officer* is prepared for organization-wide crisis management. *Duty officer* also relates what’s going on to the officer with the mandate to stop operations for safety reasons, and to the remaining duty officers. An entry is also made in the duty officers’ shared digital system. *Process lead incident management* calls to a collaboration task force meeting for the next morning. *Manager digital infrastruc-*

[6] https://www.reddit.com/r/netsec/.

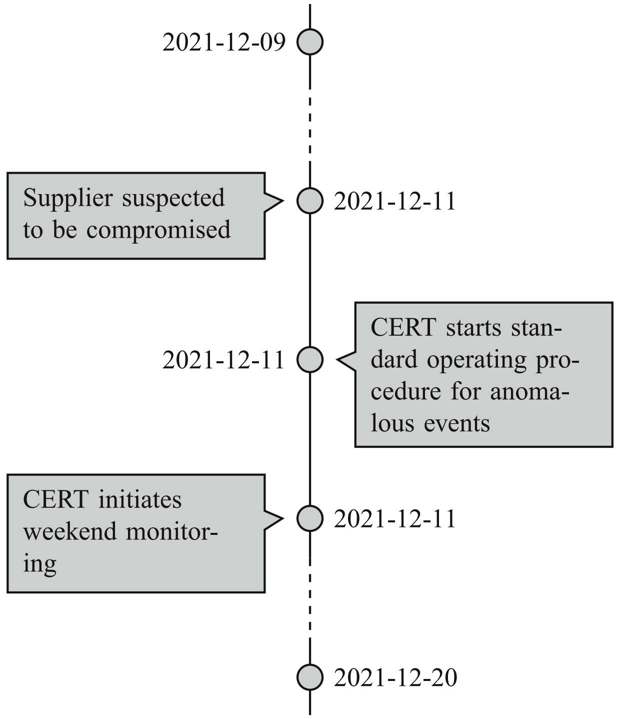

2021-12-09
Supplier suspected to be compromised
2021-12-11
2021-12-11
CERT starts standard operating procedure for anomalous events
CERT initiates weekend monitoring
2021-12-11
2021-12-20

Fig. 4 Events mentioned in the documentation for December 11, 2021

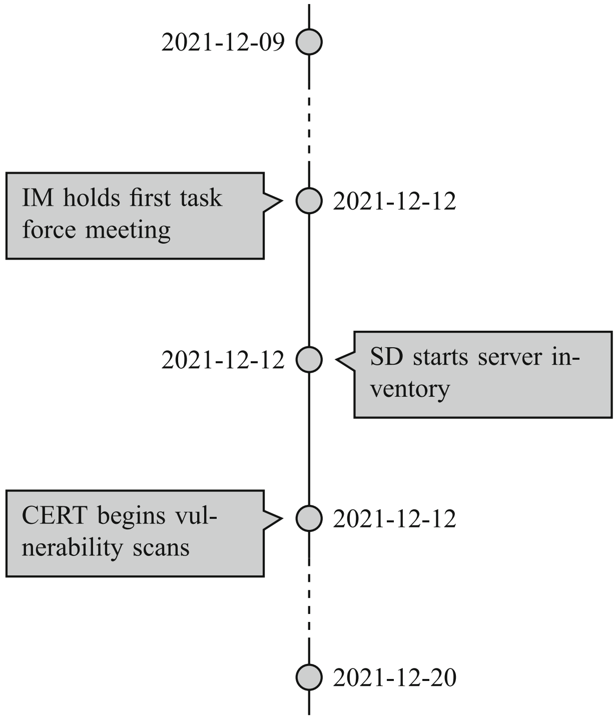

2021-12-09
IM holds first task force meeting
2021-12-12
2021-12-12
SD starts server inventory
CERT begins vulnerability scans
2021-12-12
2021-12-20

Fig. 5 Events mentioned in the documentation for December 12, 2021

ture, who at this time is two months into the job, relates that *CISO* calls at 16:30 to report about the vulnerability. *Manager digital infrastructure* takes this seriously and at 19:20 they hold their first staff meeting where a shift-work schedule is put in place. Later that evening, *Manager digital infrastructure* signs a contract with a private cybersecurity firm that, around midnight, starts to run scans to find instances of the vulnerability in the infrastructure under *Manager digital infrastructure*'s purview. The main events mentioned in the documentation are outlined in Fig. 4.

Remarks: The perception of a supplier, with whom there are close ties, and ambiguity in communication, lead to an increased sense of urgency, which spreads like ripples on the water throughout the organization. This sense of urgency incites action. Given the information available, the actions taken are proportionate to the perceived threat and show a well-prepared organization. At the same time, the organization has no objective evidence of the vulnerability being exploited within their organization. They only have hearsay and a sense of urgency from a supplier with whom there are close ties.

4.1.3 All hands on deck

On Sunday, *Process lead incident management* leads a task force meeting at 10:00. *CERT manager*, *CISO*, *IT manager*, *Information security coordinator*, and *Manager digital infrastructure* all participate in this all hands on deck meeting. *Manager digital infrastructure* recalls that they are still worried, even though they have taken actions to mitigate the threat. At the offices of *Information security coordinator*, they are scanning servers and make the decision to shut down critical services in cases where the suppliers have been nonresponsive to queries about the vulnerability. Both *IT manager* and *Information security coordinator* express frustration with suppliers being slow to respond to requests for updates. At 10:45, *CISO* has a review meeting with the CERT, which now makes use of the "quadrants" and the standard operating procedures for staff work. *CISO* and *IT director* exchange text messages to communicate about the current situation. The main events mentioned in the documentation are outlined in Fig. 5.

Remarks: At this stage, the informants are trying to understand what's going on by looking both for indicators of compromise through an exploitation of the vulnerability, as well as the presence of the vulnerable Log4j element. Centrally, there is no comprehensive configuration management database (CMDB) detailing where components are used in the organization. At this point in time, it is unclear what the consequences are for the organization, how the situation could unfold, or who the potential threat actors posing an active threat are.

4.1.4 What's going on?

Monday morning, the handling of the event takes a more structured approach. With a first meeting at 9:00, in anticipation of the IM standing taskforce meeting at 10:00, the CERT follows their standard operating procedures for anomalous events, meaning that they initiate meetings with staff updates according to the battle rhythm, that is, meetings at regular intervals to share information for decision-making and to establish the current COP at least thrice daily. These meetings continue until Monday December 20, at which point the vulnerability is considered manageable by the regular incident management team. *CERT manager* takes responsibility for coordinating the staff work with *CERT technical lead* and other CERT analysts doing the operative work. *CISO* attends the national-level sector meetings and communicates with the IM function. *CERT manager* focuses on building an understanding of what's going on that can be presented at the IM taskforce meeting at 10:00. They feel it is their job to provide an overarching view of the state of the organization at this meeting.

IT security strategist, who does not participate in the operational work, works toward understanding what the possible consequences are for the organization, should the vulnerability be exploited. They are skeptical of the threat posed by the vulnerability, saying it is one thing that the vulnerability exists and another if it is being exploited, and they had not seen any reports of exploits. They also mention that there was not enough information available to them to form a thorough understanding, and says that the focus in the CERT was on whether the vulnerability had been exploited and not on how it actually worked. The ticket and reporting system did not contain such information and the CERT COPs were not uploaded to the designated area in a timely fashion.

At this time, *CERT manager* says that "everyone was puzzled" and wanted more information, which caused a strained atmosphere. No one seems to understand what's going on. In their view, *Process lead incident management* is probably the one who has the best grasp of what was going on. *CERT manager* thinks it is hard to understand what it is they need to know now. It is also difficult to imagine what others expect them to know. They state that the lack of a comprehensive CMDB makes it harder to trace the vulnerability throughout the organization.

CERT technical lead notes the difference in information flow between Sunday and Monday, when the CERT establishes a COP. Information from trusted sources is reported at the staff meeting and entered into the COP. It is too early to say how the vulnerability might affect the organization other than that it poses a threat. At the CERT they have a better view of the external network than the internal one. The main events mentioned in the documentation are outlined in Fig. 6.

Remarks: Now, there is a Schrödinger's threat situation. There is the understanding that a supplier has been compromised, but the organization has seen no indicators of compromise in their in-house systems. The main focus is that servers with the vulnerability have to be found and updated, and analysis has to be done to see if the vulnerability has been exploited.

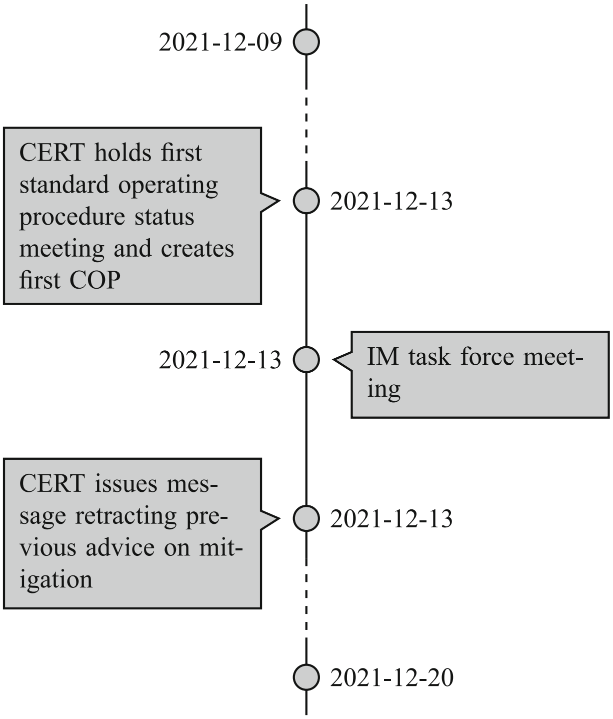

2021-12-09
CERT holds first standard operating procedure status meeting and creates first COP
2021-12-13
2021-12-13
IM task force meeting
CERT issues message retracting previous advice on mitigation
2021-12-13
2021-12-20

Fig. 6 Events mentioned in the documentation for December 13, 2021

4.1.5 Ebbing out

The initial urgency settles and time passes with no indicators of compromise found. *Information security coordinator* thinks they were first to get an overview of the situation as they completed their server scans Tuesday the 14th and from then on could prioritize where to use their resources. The subsidiary where *Information security coordinator* works decides to hire the same private cybersecurity firm as *Manager digital infrastructure*, and initiates endpoint detection and response, EDR, which the private contractor monitors.

In the CERT, *CERT manager* finds out that there was a miscommunication with the supplier who initially reported that they were affected by the vulnerability. The supplier had the vulnerability in their system, but it was never exploited there and *CERT manager* recalls that they never hear about the vulnerability being exploited anywhere. For *CISO*, the heightened alert that existed the first few days recedes with the receipt of the information that in order to exploit the vulnerability, an attacker has to take several advanced steps. This led to a decreased sense of urgency. As the IM list of systems that have been checked gets longer and suppliers mitigate risks, the organization moves towards business as usual.

The calming of the situation leads to *IT director* deprioritizing attending the national meetings and they let *CISO* handle them instead. They see a shift from the vulnerability being "the end of the world" to them knowing what's going on and being able to handle the event as a regular vulnerability. *IT manager* sees the list of potentially vulnerable systems shrinking, and there is a shift to detecting relevant traffic in firewalls rather than to look at individual applications. *Manager digital infrastructure*, who initially reacted as if the event was a de facto incident, quiets down when they see that nothing is happening and that the private cybersecurity firm continues with their work.

According to the timeline in Table 5, on Friday, December 17, all Windows and Unix servers managed by SD have been checked for Log4j and either patched or otherwise mitigated so that the vulnerability cannot be exploited. When the weekend monitoring does not show any anomalies, the CERT discontinues the standard operating procedure of an anomalous event, and makes the assessment that any further actions can be handled through regular processes starting Monday, December 20. These events are also outlined in Fig. 7.

Remarks: As the vulnerable components are identified and patched or otherwise mitigated, and no indicators of compromise are found, and the participants hear no reports of the vulnerability actually being exploited, the situation slows down and is formally sent to the regular incident management. It should be noted, however, that at the time of the interviews, approximately a year and a half after returning the Log4j handling to the regular incident management, *CERT manager* mentions that the issue had not yet been formally closed in the ticket and reporting system.

4.2 Common operational pictures in support of cyber situation awareness

When talking about what, if any, concrete common operational pictures the informants consulted to support their CSA during the event, the informants referred to two types of artifacts: (i) spreadsheet lists, and/or (ii) the "quadrants."

The spreadsheets mentioned contained lists from the IM function at SD, detailing which systems and products could be at risk. These lists were then systematically worked through and checked for the existence of Log4j, if the version installed was vulnerable, and whether the vulnerable version had been remediated. This way, the informants who followed the development through the spreadsheets could see the speed at which the vulnerability was fixed and how many systems were still to be checked. Informants who reported the lists to be part of their COP were *IT manager*, *Information security coordinator*, *Process lead incident management*, and *Manager digital infrastructure*. This is in line with their roles' involvement in the operational handling of the vulnerability.

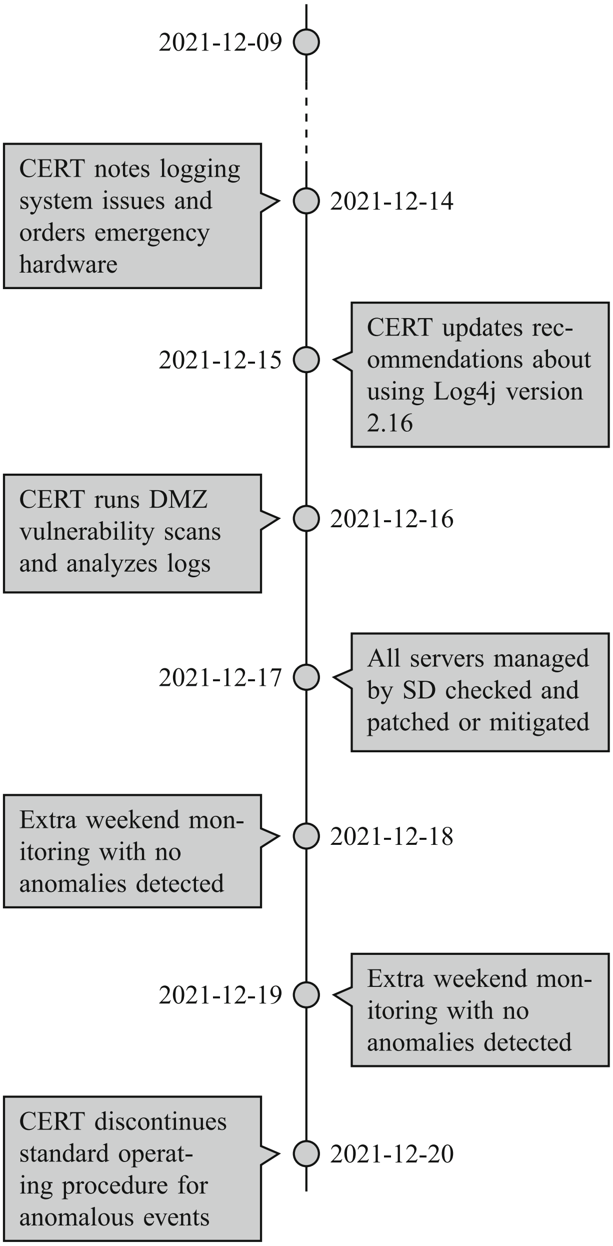

2021-12-09
CERT notes logging system issues and orders emergency hardware
2021-12-14
2021-12-15
CERT updates recommendations about using Log4j version 2.16
CERT runs DMZ vulnerability scans and analyzes logs
2021-12-16
2021-12-17
All servers managed by SD checked and patched or mitigated
Extra weekend monitoring with no anomalies detected
2021-12-18
2021-12-19
Extra weekend monitoring with no anomalies detected
CERT discontinues standard operating procedure for anomalous events
2021-12-20

Fig. 7 Events mentioned in the documentation for December 14–20, 2021

Process lead incident management also mentioned having a "quadrants" COP, but it was not used much.

As part of their standard operating procedure for anomalous events, the CERT established a COP in the form of "quadrants," with the headlines (i) facts, (ii) assumptions, (iii) measures, and (iv) communication. These "quadrants" were updated approximately every two hours according to the battle rhythm. The first CERT COP was established on Monday, December 13, and the last one on Friday, December 17. The exact dates and times of the COPs reviewed are outlined in Table 2. The CERT COPs were intended for the CERT's internal use according to *CERT technical lead*. *IT security strategist*, *CERT manager*, and *CISO* also had access to the COPs and used them as input for their CSA. *CISO*, in turn, used the CERT COP as input to create customized updates for *IT director*.

Duty officer, in their formal role, did not initiate a crisis management organization during this event—this measure was not deemed necessary because operations were not significantly impacted. However, they did start sketching a "quadrants" COP, in accordance with established procedure, as preparation if the need would arise for a crisis management organization. If so, the sketched "quadrants" COP would give an initial understanding of what was going on.

While COPs existed, there were differing views on what they should contain, for whom they are made, and where the responsibility to create an organization-wide COP resides. *IT security strategist* related that no one seemed to think it was their responsibility to create a COP suitable for the top management. In *IT security strategist*'s view, this should be done by the CERT. They had access to the area where the CERT COP should be uploaded and could look at it there. *CERT manager* and *CISO* both considered the CERT COP as too detailed for their needs, but they used it as a basis for the information they shared with others.

The complexity of the organization and the fact that the CERT has no mandate to order the subsidiaries ("satellite organizations" in the quote below) to handle the event in the same way as the rest of the organization present challenges to establishing an overarching COP. *CERT technical lead* mentioned this:

> I have reflected on […] the common operational picture and the fact that the satellite organizations handled the incident in their own way, which makes it difficult for us at the CERT to compile a complete picture.

Remarks: While the "quadrants" were established and updated by the CERT for the CERT analysts and served their needs, other informants working closely with the CERT did not find this COP useful for their own CSA needs. The CERT COP was too detailed and too technical to be immediately helpful to others than the analysts. This problem was handled in different ways. For example, the information from the COP needed additional synthesis by *CISO* before being shared with *IT director* through other means of communication. For *IT security strategist*, who initially did not attend the CERT's battle rhythm staff meetings, there were issues with the established COPs not being uploaded to the designated information-sharing area in a timely fashion, thus delaying access to the information. This lack of COPs customized for different roles' CSA requirements meant that time was being spent on adapting available information or trying to find it.

4.3 Information sharing

From the empirical material gathered, diverse types of information-sharing situations that have an impact on CSA were identified: (i) inaccuracy in information sharing, (ii) delays in information sharing, (iii) trust in information sharing, and (iv) one-way information sharing.

4.3.1 Inaccuracy in information sharing

Inaccurate information sharing contributed to the organization taking the situation very seriously from the start. The initial phone calls from the supplier on Saturday, December 11, where the message was that they had been affected, could be interpreted either as the supplier had experienced *exploitation* of the vulnerability, or that they *had the vulnerable component* in their product. The understanding of the respondents who had talked to the supplier was that the supplier's product had been exploited by a threat actor. This was understood as a fact, wherefore swift action was taken. That the supplier was breached was taken as a fact up until Tuesday, December 14, when the communication quadrant in COP6 (see Table 2) states that there was no breach.

Another case of inaccurate information relates to discrepancies in the initial communication on which versions of Log4j were free of the vulnerability. Information from the CERT about affected versions of Log4j listed version 2.15.0 as not being vulnerable to the attack on December 10, 2021 (email E1 in Table 3). However, shortly thereafter there was another vulnerability discovered in version 2.15.0, namely CVE-2021-45046.[7] In the internal communication from the CERT, email E1 (see Table 3) stated that the CERT recommended to update to version 2.15.0 or to set the value `log4j2.formatMsgNoLookups` to `false`, which was incorrect. This advice was retracted by the CERT on Monday, December 14, 2021, in email E2 (see Table 3). Another related unclear issue was that the information communicated by IM and the CERT was not always aligned. One informant, *Information security coordinator*, mentioned that the communication between the CERT and IM could have been better, as they reported receiving conflicting information about what Log4j versions to use, which caused confusion.

Remarks: These are examples of external and internal communication issues. The unclear communication led to an intense reaction, as the actors in the organization believed it to be a fact that the supplier, with whom there is a collaborative working relationship, had been breached. It is unclear where the failure in communication occurred. If the person communicating for the supplier believed that they had actually been breached, then the failure in communication could be internal at the supplier, which was then propagated to the

[7] https://www.cve.org/CVERecord?id=CVE-2021-45046.

organization. However, if the intention was to communicate having the vulnerable component in their systems, then the failure in communication lies between the supplier and the organization. In either case, the CSA of staff in the organization was based on inaccurate information. The examples of internal issues are of two kinds. The first example shows the importance of communicating accurate information, and the second shows that there are internal conflicts in the communicated information.

4.3.2 Delays in information sharing

Delays in information sharing were experienced by *IT security strategist*. At first, *IT security strategist* was not involved in the operational work with the vulnerability. Instead, they focused on what the vulnerability might mean in the long term for the organization. To understand what was going on in the organization, they relied on information residing in systems, so as not to take up time asking the actors operatively involved.

Initially, *IT security strategist* looked at information provided in the ticket and reporting system. However, when the CERT started working according to the standard operating procedure for anomalous events, the CERT analysts stopped updating the ticket and reporting system and switched to establishing COPs, as per the procedure. The established COPs are to be shared in a designated space. While the COPs were available to those attending the staff meetings where, according to the battle rhythm, the COPs were established, they were not saved to the designated space in a timely fashion.

The communication with some of the organization's suppliers was also delayed. There were difficulties getting hold of the suppliers to confirm that they were taking the vulnerability seriously, and that they were working on updating their products. *IT manager* reported that there was a challenge to the organization as it was unclear who should contact the suppliers. Several subsidiaries in the organization are using the same supplier, but no single role is designated to be responsible for communicating with the supplier to gather the information needed. Such a division of labor only developed as the event unfolded.

Remarks: When the handling of the vulnerability escalated from the regular procedure to the standard operating procedure for anomalous events, the regular information-sharing flow got disrupted. The escalation led to information not being where it was expected to be, and when the right place was found, the information was not available on time. The lack of designated points of contact for supplier communication led to delays in getting information, as the organization had to sort that out prior to contacting the suppliers.

4.3.3 Trust in information sharing

One example of an information-sharing chain with high trust is the chain *CERT manager–CISO–IT director*. Here, *CERT manager* adapted information in the COP established in the CERT to more condensed information for *CISO*, who, in turn, adapted the information from *CERT manager* to a level of granularity suitable for *IT director*. While *CERT manager* had been in the current role for 3 years, they had worked with *CISO* within the organization for 7 years, whereas *CISO* and *IT director* had 9 years of collaboration experience in their respective roles.

Another example of a chain of trust is that between *CISO* and *Duty officer*. *Duty officer* expressed that this event falls outside their competency area, while they are the one with the far-reaching mandate to call for an organization-wide crisis management to be established, if needed. *Duty officer* stated that they have great trust in *CISO* and follow their guidance, and trust the expertise in the organization. *Duty officer* did not seek out additional information externally.

Remarks: The trust in information sharing is here exemplified in two ways. The first is the trust established through long, shared, personal experience of working together combined with an awareness of what level information shared should be at. This is also one of the few directly hierarchical chains of information sharing identified. The second is trust in professional expertise when the actor is aware that the required competence is not available in their own function.

4.3.4 One-way information sharing

While the central functions of IM and the CERT shared information to the subsidiaries about how to mitigate the vulnerability, and the subsidiaries reported back on the progress of the mitigation, there were reports of one-way information sharing at the time of lessons learned. *Information security coordinator* stated that they were providing information to *Process lead incident management* before the lessons learned and that they participated actively in the lessons-learned session, but they did not get access to the final report from the session. According to *Process lead incident management*, who was in charge of the lessons learned, the report was distributed to management groups in the Main office and to SD (see Fig. 2). *IT manager*, in turn, said that there were no lessons learned conducted.

Remarks: While the central parts of the organization have a learning culture, exemplified by conducting lessons learned after the event, the collected knowledge in the lessons-learned report did not reach the more peripheral parts of the organization. Learning from past events can lead to improved CSA when handling future events.

5 Discussion

The aim of this study was to make an empirical contribution to the cybersecurity literature by highlighting challenges to CSA in organizations. This has been done by conducting a case study of a large, complex organization and identifying what the challenges are for staff involved in cybersecurity work to develop CSA while handling an emerging cyberthreat. The emerging cyberthreat in the form of the Log4j vulnerability led the organization to enter crisis management mode, as was the case for many other organizations [12]. The case study identifies several challenges staff can face when handling cyberthreats, and to forming adequate CSA for their roles. These challenges stem from, for example, COPs not supporting CSA for all roles, unclear processes, and a not fully mature learning culture.

One major challenge for the organization was that *information sharing among staff was not without effort*. That information gets siloed in various parts of an organization is not unusual [21], and having an established information flow supports the development of CSA [31]. Here, the different entities in the organization worked according to their own procedures, and there was no overarching procedure—whether formally documented or informally known by all involved—to follow when handling this event. It was not clear if the IM function at the SD or the CERT should take lead in handling the vulnerability. The organization had not established where this responsibility should lie at the time of the event, nor had it been clarified at the time of the interviews, more than a year later. Such process uncertainty can have a negative impact on response to cyberthreats, which can be contrasted with having processes allowing for flexibility as a success factor [31]. Additionally, there is the issue of what entity is responsible for producing an overarching organization-wide COP that could be of use for higher-level management, and presented at the national-level meetings for the sector.

A second major challenge was the *absence of an organization-wide COP*. During the event, no such COP existed, but some informants expressed that there should be one. This meant that information from the CERT COP and the IM COP was combined and presented in a nonstandardized format to the highest-level decision-maker among the informants. The CERT "quadrants" COP, similar to the COP documented by Varga et al. [25], was not presented to them as the level was too detailed and, thus, unsuitable. If the participants in such an information-sharing chain did not trust each other or did not have experience working together for a long time, such manual transformation entails an increased risk. The informants in the Main office surrounding the CERT all had requirements of a less detailed COP than the CERT COP. While there was an expectancy that the CERT should provide a COP suitable to support CSA for the Main office staff, it might not have been the best use of scarce CERT resources. It is possible that there is a role missing that could bridge the gap between the CERT analysts and the staff at the security section of the Main office. For a COP to successfully aid situation awareness, the participants should be familiar with it and its purpose [37].

A third major challenge was *inaccurate information being shared*. The intensity of the response to the vulnerability was partially triggered by the communication from the supplier indicating that their service was affected. The communication from the supplier contributed to the organization going into heightened alert. As the information entered the organization at a high level, it is possible that the contact person at the supplier might not have been technically oriented to answer breach questions. Here, if the organization had an established COP showing no anomalies in their systems, they might have questioned the supplier's statement. Also, if there had been established contacts between analysts at the supplier and the analysts at the CERT, the period of misunderstanding could have been cut shorter.

Events that challenge an organization can provide an organizational learning opportunity. It is important to learn from the most "useful" incidents, where the outcomes of lessons learned can have a high impact on the organizational cybersecurity posture [38]. The event reported here was challenging and shows the importance of integrating experiences from different security functions within an organization to promote learning [39]. The subsidiaries should not be seen as mere information providers, but ought to partake in the final lessons learned.

Addressing these challenges ought to have a positive impact on CSA in the organization. First, information sharing can be improved by conducting a GDTA [9] to identify the information requirements for CSA for different roles. The results of the GDTA show how information should be distributed within the organization so that those in need of it will receive it. Second, the outline of an organization-wide COP can be established using the information requirements from a GDTA and, once established, cyber crisis management exercises can be held where the roles involved can familiarize themselves with the COP during training. Third, establishing routines to ask counter questions to confirm that information received is understood as intended, would be an obvious way to avoid that misunderstandings propagate further within the organization. Lastly, conducting lessons learned after incidents can contribute to staff identifying adverse events quicker and being able to project consequences.

This study is not without limitations. First, the interviews were conducted some time after the handling of the vulnerability, so the informants' recollection of the events might vary. Second, due to the sensitive nature of the interviews, they were not recorded but rather captured through note-taking, which could affect accuracy. To remedy this, all informants have had the opportunity to read the transcribed interviews and give their approval.

This is a single, in-depth case study, which entails certain limitations [35]. Having access to multiple organizations with the same main purpose as the organization reported on here would have permitted a comparison and contrast of how the different organizations' staff developed cyber situation awareness while handling Log4j. Nevertheless, this single, in-depth case study is highly relevant as it provides insights into what challenges staff in an organization experience when developing cyber situation awareness.

All ex post studies of cyber incidents face an unavoidable survivor bias—organizations that were hit so hard as to go bankrupt and cease to exist cannot be studied. This study is no exception. Anyone compiling a literature review of the effects of the Log4j vulnerability should take this bias into account. Whether the organization studied here is representative of the entire surviving population is more difficult to assess. The very fact that they agreed to be studied may indicate that they are at least moderately satisfied with their performance. On the other hand, the study has also uncovered frustration and unresolved issues within the organization. On a balance, it is safest to consider this a case study where the generalizability is analytical, rather than statistical.

6 Conclusions

This case study contributes to the literature on CSA for staff in organizations by highlighting the challenges faced by staff involved in the handling of an emerging cyberthreat. In this case study, ten semi-structured interviews and documents collected show the challenges faced by staff involved in the handling of an emerging cyberthreat.

The study set out to answer the overarching research question mentioned in Section 1: what challenges do staff involved in cybersecurity work in a large, complex organization experience when developing cyber situation awareness while handling an emerging cyberthreat? The conclusions from the three sub-questions, used to answer the overarching research question, are presented here, in addition to recommendations and ideas for future research.

The first sub-question addressed how information about the emerging cyberthreat spread to staff involved in the handling of the threat. As the history of the event unfolded, information about the vulnerability came to the staff in multiple ways from external and internal sources, and also through nonstandard means; for example, it happened that a higher-level decision-maker was contacted by a supplier, which was unusual.

The second sub-question addressed what common operational pictures existed to aid staff cyber situation awareness while handling the emerging cyberthreat. Here there were two main COPs, the "quadrants" in the CERT and the lists from the IM function. In addition, there were preparations made in the form of a COP sketch for duty officers, should the need to call for an organization-wide crisis management arise. There were expectations of an overarching organization-wide COP, but there was none.

The third sub-question addressed what the staff experiences of information sharing for cyber situation awareness were during the handling of the emerging cyberthreat. The results include different experiences in the form of inaccurate information being taken as fact, delays in information sharing exemplified by COPs not being saved in the designated area, suppliers not being available for questions during the weekend, trust between colleagues in a longtime coworking hierarchical stretch of the organization, and experiences of one-way information sharing, where an informant for lessons learned did not receive the final lessons-learned report.

Based on the findings, some recommendations can be made:

- responsibility to create an organization-wide COP should be established,
- the organization-wide COP ought to be designed to facilitate information sharing to national-level COPs for the sector,
- design of useful COPs for different roles should be considered,
- lessons-learned activities and reports should be inclusive to foster a learning culture,
- internal information-sharing requirements should be identified and relevant processes established, and
- designated points of contact for suppliers should be identified for quicker information sharing.

Implementing these recommendations, and conducting exercises to train staff in using new processes and COPs, ought to improve CSA for staff in the organization, but this needs to be evaluated with regard to achieving mission success. Henceforth, to establish that CSA has really been improved, the situation awareness needs to be tested and measured in the cyber domain [18, 40].

The findings presented give rise to some potential directions for future research. As the results showed a need for common operational pictures adapted to different roles, one idea for future research is to use participatory design methods to design such COPs. A first step in that direction was to investigate the actors' need for a tool supporting common operational pictures in aid of cyber situation awareness for diverse roles involved in incident handling in a large and complex organization [41].

In addition, longitudinal studies with researchers embedded in individual organizations should be performed, in order to investigate how staff needing cyber situation awareness develop situation awareness as incidents unfold. Direct observations of how the different roles involved in incident handling share needed information would further an understanding of how cyber situation awareness develops.

Appendix A Interview guide

Translated from Swedish.

1. About the informant

1.1. Tell us about your role in December 2021.

i. What is the formal title?

ii. What tasks do you perform?

iii. Whom do you report to?

iv. What information do you give your manager on a weekly basis?

1.2. How long experience do you have in the role?

1.3. How long have you worked (in the organization)?

2. About the event

2.1. Can you tell us how you became aware of the Log4j vulnerability?

2.2. How were you affected in your role?

2.3. How did you develop an understanding of how the vulnerability could affect (the organization)?

2.4. What tasks did you have while handling the Log4j vulnerability?

2.5. Whom did you collaborate with?

2.6. Did your view of the vulnerability change during the handling?

i. In what way?

2.7. How did you get information about the vulnerability?

i. Internally?

ii. Externally?

2.8. What information would you have needed?

2.9. Were you prepared to handle a vulnerability like Log4Shell?

i. How had you prepared?

2.10. How did you develop an understanding of what was going on?

2.11. According to documentation, there was a task force created on December 12, were you part of it?

i. If no, did you get access to the task force's documentation or information?

2.12. How did your group create a common understanding of what was going on?

i. Who took responsibility for the common understanding of what was going on?

ii. What information was essential for understanding what was going on?

iii. What challenges did you face in creating a common understanding of what was going on?

iv. Did you create a concrete common operational picture and how did it manifest?

A. What determined what information was to be included?

B. What did you want to use the common operational picture for?

C. For whom was the common operational picture created?

D. Did you share the common operational picture with others?

E. Were there others who would have benefited from the common operational picture?

v. Do you think others had other common operational pictures, what did they look like, and why?

vi. Did the common operational picture help you to understand what was going on?

vii. Was there information lacking in the common operational picture that you would have liked to see included?

2.13. How can the presentation of the common operational picture be improved?

3. After the event

3.1. What have you learnt from the event?

3.2. Did any systematic lessons-learned session take place?

i. Did you take part in the session?

ii. Have you partaken in the lessons learned?

3.3. Has your role changed since the event?

i. Mandate?

ii. Tasks?

3.4. Have you changed your processes since the event?

i. What?

ii. Why was this change made?

3.5. Given this event, what would you like to know at future events?

4. System support

4.1. Do you lack system support that would have been useful while handling the event?

4.2. How would you like it to work?

4.3. Are there other roles/functions that would benefit from such a system?

Appendix B Documents collected

Documents were accessed for analysis. The documents in Table 2 were read on-site due to their sensitive nature whereas the documents in Tables 3 and 4 were shared with the researchers. Table 5 details timeline TL1 from Table 4.

Table 2 CERT common operational pictures

Doc	Date	Time
COP1	2021-12-13	09:00
COP2	2021-12-13	11:30
COP3	2021-12-13	13:30
COP4	2021-12-13	16:00
COP5	2021-12-14	11:30
COP6	2021-12-14	11:30[a]
COP7	2021-12-14	11:30[b]
COP8	2021-12-15	11:30
COP9	2021-12-15	14:00
COP10	2021-12-15	14:00[c]
COP11	2021-12-15	14:00[d]
COP12	2021-12-16	09:00
COP13	2021-12-16	11:30
COP14	2021-12-16	16:00
COP15	2021-12-17	09:00
COP16	2021-12-17	09:00[e]
COP17	2021-12-17	11:30
COP18	2021-12-17	14:00

[a] Time not updated
[b] Time not updated
[c] Time not updated
[d] Copy
[e] Copy

Table 3 Emails from CERT

Doc	Date	Time	Subject
E1	2021-12-10	15:12	CERT MESSAGE: Critical vulnerability in Java-library Log4j
E2	2021-12-13	13:44	UPDATE CERT MESSAGE: Critical vulnerability in Java-library Log4j
E3	2021-12-14	14:20	CERT MESSAGE: Update on Critical vulnerability in Java-library Log4j
E4	2021-12-15	12:02	CERT MESSAGE: Update on Critical vulnerability in Java-library Log4j
E5	2021-12-17	13:18	CERT MESSAGE: Information being sent to all contacts for security information (2021-12-17)
E6	2021-12-21	10:22	CERT MESSAGE: Update on Log4j vulnerability “Log4Shell” and preferred versions

Table 4 Timelines created by organization after event

Doc	Description
TL1	Timeline from the CERT lessons-learned report
TL2	Timeline outlining IM check-in meetings and CERT staff meetings

Table 5 Timeline from CERT lessons-learned report

Date	Event
2021-12-09	The vulnerability is identified by developers in the Apache project.
2021-12-10	CERT takes part of information regarding the vulnerability through news articles and deems it to be of such criticality that a security message needs to be issued to all information security coordinators in [the organization], with a recommendation to update Log4j as soon as possible.
2021-12-11	One of [the organization]'s suppliers are suspected to have been compromised through Log4Shell. This causes CERT to work according to the standard operating procedure for an anomalous event.
2021-12-11	CERT initiates weekend monitoring. Alarms are set up in the CERT central logging system that are meant to identify incoming HTTP requests where attempts to exploit Log4j occurs.
2021-12-12	IM calls to the first task force meeting. SD initiates the task of taking inventory of all servers using Log4j.
2021-12-12	CERT initiates regular vulnerability scans on servers exposed to the internet. The scans are thereafter performed until 2021-12-20.
2021-12-13	CERT holds its first status meeting in line with the instructions on how to handle an anomalous event.
2021-12-14	CERT notices that there are issues with the central logging system […], which means that events disappear due to high load. An emergency order of more hardware is placed to secure the environment.
2021-12-15	The Apache project releases a new update for Log4j (version 2.16) as new studies show that the previous version is still vulnerable when Log4j is configured in a specific way. CERT undertakes to update the recommendation in the daily security messages with a recommendation to update Log4j to version 2.16.
2021-12-15	[Organizational unit] provides excerpts from HTTP access logs to the CERT from the servers managed by their IT organization. From these logs, the CERT can identify other versions of Log4Shell calls.
2021-12-16	Redacted.
2021-12-16	CERT runs a vulnerability scan from the DMZ on servers on the network. The purpose is to ensure that the results from the external vulnerability scans are valid without a firewall potentially stopping vulnerabilities from being identified by the CERT scanning tool.
2021-12-16	SD provides access and security event logs from multiple servers placed within the DMZ. The logs are analyzed by CERT with the purpose of finding out if any attack has been successful.
2021-12-17	During the routine daily morning check-in, the SD Incident management function relates that all Windows and Unix servers managed by SD have been checked for Log4j, and patched where possible, or otherwise in other ways mitigated from the possibility of exploiting the vulnerability.
2021-12-(18–19)	CERT sets up extra weekend monitoring to prevent possible attacks during the weekend. Aside from the vulnerability scans, there are no anomalies in the web traffic.
2021-12-20	CERT assesses that the standard operating procedure of an anomalous event can be discontinued and the incident handled through regular operations.

Acknowledgments This work was supported by the Swedish Armed Forces. The authors thank the informants who participated in the study.

Author contributions Conceptualization: A.A., H.A., J.B., and U.F. Methodology: A.A., H.A., J.B., and U.F. Interview data collection: A.A., H.A., J.B., and U.F. Document collection: A.A. Data curation: A.A. Analysis and Interpretation: AA., H.A., J.B., and U.F. Writing - original draft: A.A., H.A., J.B., and U.F. All authors reviewed the manuscript.

Data availability The empirical material analyzed in the current study is not publicly available for reasons of sensitivity and to protect participant anonymity.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Informed consent All participants in this study gave informed consent in accordance with Swedish law.

Ethical approval The study is designed in accordance with the Swedish Ethical Review Act (2003:460), which stipulates that an ethics review must be performed by a national agency (the Ethics Review Authority) if the research fulfills at least one of the following criteria: (i) there is a physical intervention on the research subject (alive or deceased), (ii) the research method is intended to physically or psychologically affect the research person, (iii) there is an obvious risk of physical or psychological harm, (iv) biological matter from the research persons (alive or deceased) is used and traceable to them, or (v) sensitive personal data or personal data concerning the crime record are handled. In our case, it is obvious that the first four criteria do not apply. With respect to the fifth, KTH Royal Institute of Technology has assessed that the study is designed so that sensitive personal data or personal data about violations of the law are not included in the study, and that the study does not intend to process such data.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Joint Task Force Interagency Working Group: Security and privacy controls for information systems and organizations. NIST Special Publication 800-53, Revision 5, National Institute of Standards and Technology, U.S. Department of Commerce (2020). https://doi.org/10.6028/NIST.SP.800-53r5
2. de Smale, S., van Dijk, R., Bouwman, X., van der Ham, J., van Eeten, M.: No one drinks from the firehose: how organizations filter and prioritize vulnerability information. In: Proceedings of the 44th IEEE Symposium on Security and Privacy (SP 2023), pp. 203–219. IEEE, Piscataway, NJ (2023). https://doi.org/10.1109/SP46215.2023.10179447
3. Shah, A., Ganesan, R., Jajodia, S., Cam, H.: A methodology to measure and monitor level of operational effectiveness of a CSOC. Int. J. Inf. Secur. **17**, 121–134 (2018). https://doi.org/10.1007/s10207-017-0365-1
4. Shah, A., Ganesan, R., Jajodia, S., Cam, H.: Maintaining the level of operational effectiveness of a CSOC under adverse conditions. Int. J. Inf. Secur. **21**, 637–651 (2022). https://doi.org/10.1007/s10207-021-00573-4
5. Franke, U., Andreasson, A., Artman, H., Brynielsson, J., Varga, S., Vilhelm, N.: Cyber situational awareness issues and challenges. In: Moustafa, A.A. (ed.) Cybersecurity and Cognitive Science, pp. 235–265. Academic Press, London, United Kingdom (2022). https://doi.org/10.1016/B978-0-323-90570-1.00015-2
6. Gutzwiller, R.S., Dykstra, J., Payne, B.: Gaps and opportunities in situational awareness for cybersecurity. Digital Threats: Research and Practice **1**(3), 1–6 (2020). https://doi.org/10.1145/3384471
7. Ofte, H.J.: The awareness of operators: a goal-directed task analysis in SOCs for critical infrastructure. Int. J. Inf. Secur. **23**, 3253–3282 (2024). https://doi.org/10.1007/s10207-024-00872-6
8. Schraagen, J.M., Chipman, S.F., Shalin, V.L. (eds.): Cognitive Task Analysis. Lawrence Erlbaum (2000). https://doi.org/10.4324/9781410605795
9. Endsley, M.R.: A survey of situation awareness requirements in air-to-air combat fighters. Int. J. Aviation Psychology **3**(2), 157–168 (1993). https://doi.org/10.1207/s15327108ijap0302_5
10. Dooley, K.: Organizational complexity. In: Warner, M. (ed.) International Encyclopedia of Business and Management, 2nd edn., pp. 5013–5022. Thomson Learning, London, United Kingdom (2002)
11. Hiesgen, R., Nawrocki, M., Schmidt, T.C., Wählisch, M.: The Log4j incident: a comprehensive measurement study of a critical vulnerability. IEEE Trans. Netw. Serv. Manage. **21**(6), 5921–5934 (2024). https://doi.org/10.1109/TNSM.2024.3440188
12. Doll, J., McCarthy, C., McDougall, H., Bhunia, S.: Unraveling Log4Shell: analyzing the impact and response to the Log4j vulnerability (2025). https://doi.org/10.48550/arXiv.2501.17760
13. Associated Press: Recently uncovered software flaw 'most critical vulnerability of the last decade.' The Guardian (2021). https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell
14. Salmon, P.M., Stanton, N.A., Walker, G.H., Baber, C., Jenkins, D.P., McMaster, R., Young, M.S.: What really is going on? Review of situation awareness models for individuals and teams. Theor. Issues Ergon. Sci. **9**(4), 297–323 (2008). https://doi.org/10.1080/14639220701561775
15. Endsley, M.R.: Toward a theory of situation awareness in dynamic systems. Hum. Factors **37**(1), 32–64 (1995). https://doi.org/10.1518/001872095779049543
16. Tadda, G.P., Salerno, J.S.: Overview of cyber situation awareness. In: Jajodia, S., Liu, P., Swarup, V., Wang, C. (eds.) Cyber Situational Awareness: Issues and Research, volume 46 of Advances in Information Security, pp. 15–35. Springer, Boston, MA (2010). https://doi.org/10.1007/978-1-4419-0140-8_2
17. Franke, U., Brynielsson, J.: Cyber situational awareness: a systematic review of the literature. Comput. Secur. **46**, 18–31 (2014). https://doi.org/10.1016/j.cose.2014.06.008
18. Brynielsson, J., Franke, U., Varga, S.: Cyber situational awareness testing. In: Akhgar, B., Brewster, B. (eds.) Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities, Advanced Sciences and Technologies for Security Applications, chapter 12, pp. 209–233. Springer, Cham, Switzerland (2016). https://doi.org/10.1007/978-3-319-38930-1_12
19. Ofte, H.J., Katsikas, S.: Understanding situation awareness in SOCs, a systematic literature review. Comput. Secur. **126**, 103069 (2023). https://doi.org/10.1016/j.cose.2022.103069
20. Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., Babar, M.A.: Systematic literature review on cyber situational awareness visualizations. IEEE Access **10**, 57525–57554 (2022). https://doi.org/10.1109/ACCESS.2022.3178195
21. Andreasson, A., Artman, H., Brynielsson, J., Franke, U.: Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. Cognition, Technology & Work **26**(4), 709–731 (2024). https://doi.org/10.1007/s10111-024-00779-1
22. Comfort, L.K.: Crisis management in hindsight: cognition, communication, coordination, and control. Public Adm. Rev. **67**(1), 189–197 (2007). https://doi.org/10.1111/j.1540-6210.2007.00827.x
23. Wolbers, J., Boersma, K.: The common operational picture as collective sensemaking. J. Conting. Crisis Manage. **21**(4), 186–199 (2013). https://doi.org/10.1111/1468-5973.12027
24. MSB: Gemensamma grunder för samverkan och ledning vid samhällsstörningar [Common bases for collaboration and management in the event of societal disruptions]. Publ. MSB777, Swedish Civil Contingencies Agency, Karlstad, Sweden (2018)

25. Varga, S., Brynielsson, J., Franke, U.: Cyber-threat perception and risk management in the Swedish financial sector. Comput. Secur. **105**, 102239 (2021). https://doi.org/10.1016/j.cose.2021.102239
26. Varga, S., Brynielsson, J., Franke, U.: Information requirements for national level cyber situational awareness. In: Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2018), pp. 774–781. IEEE, Piscataway, NJ (2018). https://doi.org/10.1109/ASONAM.2018.8508410
27. McKenna, S., Staheli, D., Meyer, M.: Unlocking user-centered design methods for building cyber security visualizations. In: Proceedings of the 2015 IEEE Symposium on Visualization for Cyber Security (VizSec 2015), pp. 1–8. IEEE, Piscataway, NJ (2015). https://doi.org/10.1109/VIZSEC.2015.7312771
28. Skopik, F., Bonitz, A., Grantz, V., Göhler, G.: From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. Int. J. Inf. Secur. **21**, 1323–1347 (2022). https://doi.org/10.1007/s10207-022-00613-7
29. Rajivan, P., Cooke, N.: Impact of team collaboration on cybersecurity situational awareness. In: Liu, P., Jajodia, S., Wang, C. (eds.) Theory and Models for Cyber Situation Awareness, pp. 203–226. Springer, Cham, Switzerland (2017). https://doi.org/10.1007/978-3-319-61152-5_8
30. Paul, C.L., Whitley, K.: A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In: Proceedings of the 15th International Conference on Human-Computer Interaction, pp. 145–154. Springer, Berlin/Heidelberg, Germany (2013). https://doi.org/10.1007/978-3-642-39345-7_16
31. Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T., Baskerville, R.L.: How can organizations develop situation awareness for incident response: a case study of management practice. Comput. Secur. **101**, 102122 (2021). https://doi.org/10.1016/j.cose.2020.102122
32. Nyre-Yu, M., Gutzwiller, R.S., Caldwell, B.S.: Observing cyber security incident response: qualitative themes from field research. Proc. Hum. Factors Ergon. Soc. Annu. Meet. **63**(1), 437–441 (2019). https://doi.org/10.1177/1071181319631016
33. Ofte, H.J., Katsikas, S.: Paralyzed or compromised: a case study of decisions in cyber-physical systems. In: Proceedings of the 26th International Conference on Human-Computer Interaction, pp. 134–152. Springer, Cham, Switzerland (2024). https://doi.org/10.1007/978-3-031-61382-1_9
34. Bartnes, M., Moe, N.B., Heegaard, P.E.: The future of information security incident management training: a case study of electrical power companies. Comput. Secur. **61**, 32–45 (2016). https://doi.org/10.1016/j.cose.2016.05.004
35. Yin, R.K.: Case Study Research and Applications: Design and Methods, 6th edn. SAGE, Los Angeles, CA (2018)
36. Creswell, J.W.: Qualitative Inquiry and Research Design: Choosing Among Five Approaches, 3rd edn. SAGE, Thousand Oaks, CA (2013)
37. Spak, U.: The common operational picture: a powerful enabler or a cause of severe misunderstanding? In: Proceedings of the 22nd International Command and Control Research and Technology Symposium (22nd ICCRTS). International Command and Control Institute (2017). https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7172
38. Patterson, C.M., Nurse, J.R.C., Franqueira, V.N.L.: I don't think we're there yet: the practices and challenges of organisational learning from cyber security incidents. Comput. Secur. **139**, 103699 (2024). https://doi.org/10.1016/j.cose.2023.103699
39. Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., Baskerville, R.L.: How integration of cyber security management and incident response enables organizational learning. J. Assn. Inf. Sci. Tec. **71**(8), 939–953 (2020). https://doi.org/10.1002/asi.24311
40. Cheng, Y., Deng, J., Li, J., DeLoach, S.A., Singhal, A., Ou, X.: Metrics of security. In: Kott, A., Wang, C., Erbacher, R.F. (eds.) Cyber Defense and Situational Awareness, volume 62 of Advances in Information Security, pp. 263–295. Springer, Cham, Switzerland (2014). https://doi.org/10.1007/978-3-319-11391-3_13
41. Andreasson, A., Lindquist, S.: Envisioning cyber situation awareness through participatory video prototyping. In: Proceedings of the 22nd International Conference on Information Systems for Crisis Response and Management (ISCRAM 2025), Halifax, Canada (2025). https://doi.org/10.59297/xp06tf49

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.