International Journal of Information Security
https://doi.org/10.1007/s10207-024-00872-6

REGULAR CONTRIBUTION

The awareness of operators: a goal-directed task analysis in SOCs for critical infrastructure

Håvard Jakobsen Ofte[1]

Accepted: 4 June 2024

Abstract
Security operation centers (SOCs) are increasingly established to meet the growing threat against cyber security. The operators of SOCs respond to complex incidents under time constraints. Within critical infrastructure, the consequences of human error or low performance in SOCs may be detrimental. In other domains, situation awareness (SA) has proven useful to understand and measure how operators use information and decide the correct actions. Until now, SA research in SOCs has been restricted by a lack of in-depth studies of SA mechanisms. Therefore, this study is the first to conduct a goal-directed task analysis in a SOC for critical infrastructure. The study was conducted through a targeted series of unstructured and semi-structured interviews with SOC operators and their leaders complemented by a review of documents, incident reports, and in situ observation of work within the SOC and real incidents. Among the presented findings is a goal hierarchy alongside a complete overview of the decisions the operators make during escalated incidents. How the operators gain and use SA in these decisions is presented as a complete set of SA requirements. The findings are accompanied by an analysis of contextual differences in how the operators prioritize goals and use information in network incidents and security incidents. This enables a discussion of what SA processes might be automated and which would benefit from different SA models. The study provides a unique insight into the SA of SOC operators and is thus a steppingstone for bridging the knowledge gap of Cyber SA.

Keywords Cyber security · Security operations center (SOC) · Critical infrastructure · Incident response · Situation awareness · Human factors

1 Introduction

Cyber security is of growing concern for society, especially in relation to critical infrastructures. Critical infrastructure is defined by the European Union as assets or systems that are "*essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people*" [1]. Critical infrastructures are rapidly becoming industrial cyber-physical systems with the convergence of information and operational technology [2]. This makes critical infrastructure increasingly vulnerable to cyber incidents highlighting the need for improved cyber security and training across critical sectors [3]. There is meanwhile a growing realization within research that human factors are essential aspects of cyber security. This is highlighted by investigations into the causes of cyber security incidents which estimate that half of all incidents are in some way caused by human error [4]. This shows the large potential for improving security through understanding human performance in this domain. It is not sufficient to develop and implement technical solutions to achieve cyber security. We must consider the decisions and actions of the people responsible for using the tools that are developed. Situation Awareness (SA) is a large field of research specifically aimed at investigating the processes that can lead to human error in contexts of critical importance. The research on how SA affects performance spans many different operational contexts [5]. Some examples include how SA is essential to preserve power system security [6], how it predicts surgery performance [7], and how it can explain and prevent aviation accidents [8]. SA has many definitions, but can most generally be described as "*the process of gathering information about a situation and converting this information into an awareness that can differentiate between the suitability of potential actions*" [9].

✉ Håvard Jakobsen Ofte
havard.ofte@ntnu.no

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

Published online: 19 July 2024

The amount of research on SA within cyber security is growing, but we do not have sufficient in-depth knowledge of SA processes in this domain. Several reviews have pointed to a lack of empirical evidence regarding SA in cyber security [10, 11]. Much of the existing research is aimed towards developing tools that will improve human performance through SA. This research often assumes that such tools improve SA, although this has largely not been empirically tested [9]. The lack of empirical research leaves a considerable gap in our knowledge of how SA impacts cyber security. One recent review concluded that to fill this gap the research community should "*(1) understand what cyber SA is from the human operators' perspectives, then (2) measure it so that (3) the community can learn whether SA makes a difference in meaningful ways to cybersecurity, and whether methods, technology, or other solutions would improve SA and thus, improve those outcomes.*" [11]. If we are to close this gap, we need research that specifically investigates the mental processes of SA for those working within cyber security. Then we can identify what constitutes good SA in this context, and how we can ensure and improve it.

One of the major challenges for SA research on cyber security is access to respondents. To investigate SA mechanisms researchers must gain access to operators and their working environments. There have been relatively few attempts to directly investigate SA within cyber security. Several studies report challenges due to the lack of access to respondents [12–14]. Much of the existing research is conducted in educational settings or exercises as part of public conventions. One proposition is to investigate SA in defined groups of cyber security specialists responsible for specific networks and services [9]. Such groups are often referred to as security operations centers (SOCs). SOCs within critical infrastructure have many of the same characteristics as settings where SA has been researched before. In other fields like aviation, control rooms, and first responders, research has resulted in the operationalization of SA mechanisms [15]. This has in turn enabled empirical testing of SA's impact on human performance [5]. The results of the SA research in other fields hold a promise of increased human performance, but it is only through an in-depth understanding of SA mechanisms that such results will be realized. In-depth understanding can only be achieved with sufficient access to the human operators and their environment.

The first step for investigating SA in SOCs is an analysis of the goals and decisions that are performed and what information is required for the operators to gain sufficient SA during incidents. Methods of task analysis (TA) have been developed to achieve this first step but have not yet been rigorously performed within SOCs. When TAs aimed at SA are conducted in new contexts it is recommended to perform a goal-directed task analysis (GDTA) which also maps and prioritizes the goals and decisions within the specific context [16]. This study aims to conduct a full-scale GDTA establishing the requirements for SA in a SOC for critical infrastructure during incidents. This includes investigating the goals, the decisions, and the information required by the SOC operators. In addition, this study investigates different timelines of decisions and goal completion based on different types of incidents. The study aims to answer the following research questions:

- *RQ1: What are the goals of the SOC and how are they prioritized?*
- *RQ2: What decisions are made by the operators during incidents and what are the related SA requirements?*
- *RQ3: How do the prioritization of goals and order of decisions differ between types of incidents?*

The performed GDTA answers RQ1 and RQ2. An additional investigation of incident timelines answers RQ3.

The contributions of this study are as follows:

- It is the first to complete a full GDTA within the context of SOCs for critical infrastructure.
- It provides empirically based knowledge of the SA requirements for SOC operators during incidents. This gives unique insights into the SA mechanisms of operators responsible for cyber security within critical infrastructure.
- It provides maps of the SOC operators' goals, timelines of how they handle incidents, and a detailed description of how they gather, process, and utilize information to gain SA. This is achieved by performing interviews, reviewing incident reports, and observing SOC operators in their actual working environment. The gained insight is discussed and compared with the current theoretical foundations of Cyber SA.
- The results shed light on how different theories and models of Cyber SA can be related to different SA processes rather than being different explanations of the same phenomena.

The remainder of the paper is structured as follows: Sect. 2 presents the background of the study and related work. Section 3 describes the research methodology, whilst Sect. 4 presents the results. Section 5 discusses the results and Sect. 6 summarizes the conclusions.

2 Background and related work

In the following, the relevant research related to the study at hand is presented. First, the concept of SA is presented in Sect. 2.1. This includes a presentation of the most recognized theoretical model explaining SA as a cognitive process consisting of 3 levels of human information processing. The

section also gives a short presentation of how SA has been conceptualized in groups and at a systemic level. Section 2.2 describes how SA has gained growing interest in cyber security research. It further describes how much of the existing Cyber SA research has been focused on developing tools that alleviate human operators' SA processes with a lack of empirical SA measurements. A short description of recognized methods of measuring SA is also given. In Sect. 2.3 the existing research on SA in teams of cyber security operators is presented. It is explained how such groups are comparable to other contexts where SA research has proven useful before. Lastly, it is explained how a lack of in-depth analyses of SA processes within this context is a major barrier to empirically investigating the impact of SA, and thus a key for bridging the recognized research gap this study is aimed at.

2.1 The concept of SA

SA is a widely researched topic within human factors. The challenge of gaining and maintaining a good awareness of a situation is intrinsic in many domains. The challenge has been exacerbated by information technology enabling humans to monitor and control complex systems. The research on SA was mainly developed within piloting and airspace control. The theory and methods of SA have later been adapted to other domains where human performance is essential, such as control rooms of nuclear power plants, military command, and surgery [17].

The most recognized theory of SA was developed by Endsley and is based on cognitive psychology [17]. The theory focuses on individual information processing and defines SA as «*the perception of the 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*» [18]. This definition is based on the recognition of 3 levels of processing information namely *perception*, *comprehension*, and *projection*. Human operators first perceive elements in their situation which is then comprehended to gain understanding. Then this understanding is used in the projection of the situation's future status to assess the suitability of different actions. This process is influenced by external factors related to tasks and the systems that are operated alongside individual factors related to differences in the mental processing of information. Figure 1 presents Endsley's model of SA showing how information in the environment is processed in 3 levels leading to decisions and actions which in turn feed back into the operator's environment.

Theoretical development within SA research has led to several models that explain SA at different levels of operation. The different theories of SA can be categorized into 3 groups based on what level they conceptualize SA [9]. At the individual level, Endsley's cognitive model is still the most recognized and by many regarded as the de-facto standard. At the group level, *Team SA* focuses on the aggregate of individuals' SA, while *Shared SA* focuses on the overlap between individuals' SA [15]. These group-level SA models are largely based on Endsley's individual model but are extended to explain SA in groups. *Distributed SA* conceptualizes SA at the systemic level as a product of the interactions between both human and technical agents [19]. *Distributed SA* is a systemic theory and does not adhere to the notion that SA only resides in the operators as mental processes. There has been some contention between *Distributed SA* and theories based on Endsley's cognitive model [20].

2.2 SA in cyber security

Improvement of SA has been highlighted as a promising contributing factor to cyber security [21]. Within cyber security, there is growing interest in SA, but the theoretical foundation of the SA research is sometimes unclear. Most of the available research refers to Endsley's theoretical model with the addition of some more technically based theories of SA related to data triage [9]. The term Cyber SA gained adoption from 2009 and is defined as a subset of SA relating to operator tasks aimed at cyber security [22]. A review from 2014 of Cyber SA [10] showed that the research was mainly aimed at developing tools that could improve Cyber SA. Nevertheless, the review pointed to a clear lack of empirical research assessing Cyber SA and its impacts. The knowledge gap regarding an in-depth understanding of Cyber SA processes and their relation to human performance in this domain was confirmed in a later paper [11]. Most of the Cyber SA research trends towards automating processes using technical tools that could alleviate human operators' SA-related tasks. Still, systemic SA theories are rarely used as a basis for this research. This implies a mismatch between the goals of Cyber SA research and the theoretical models used [9].

There are many available methods for measuring SA, but they have not been sufficiently applied in the context of cyber security. The methods are mostly developed within the theoretic framework of Endsley [23]. Measuring SA is a difficult challenge as it needs to assess the quality of the mechanism of processing information. Direct observations through freeze probes like SAGAT [24] are one of the most valid types of measurement for human SA [5]. SAGAT establishes a realistic simulation of tasks that are "frozen" at set intervals where the participants are probed about their awareness of relevant aspects of the situation [24]. Observer-rating is an alternative method where Subject Matter Experts (SMEs) rate the participants' SA based on observation during simulation [5]. Self-rating is used where participants rate their own SA, but this method is criticized based on the prevalence of bias in the measurements. Proxy measurements like eye-tracking

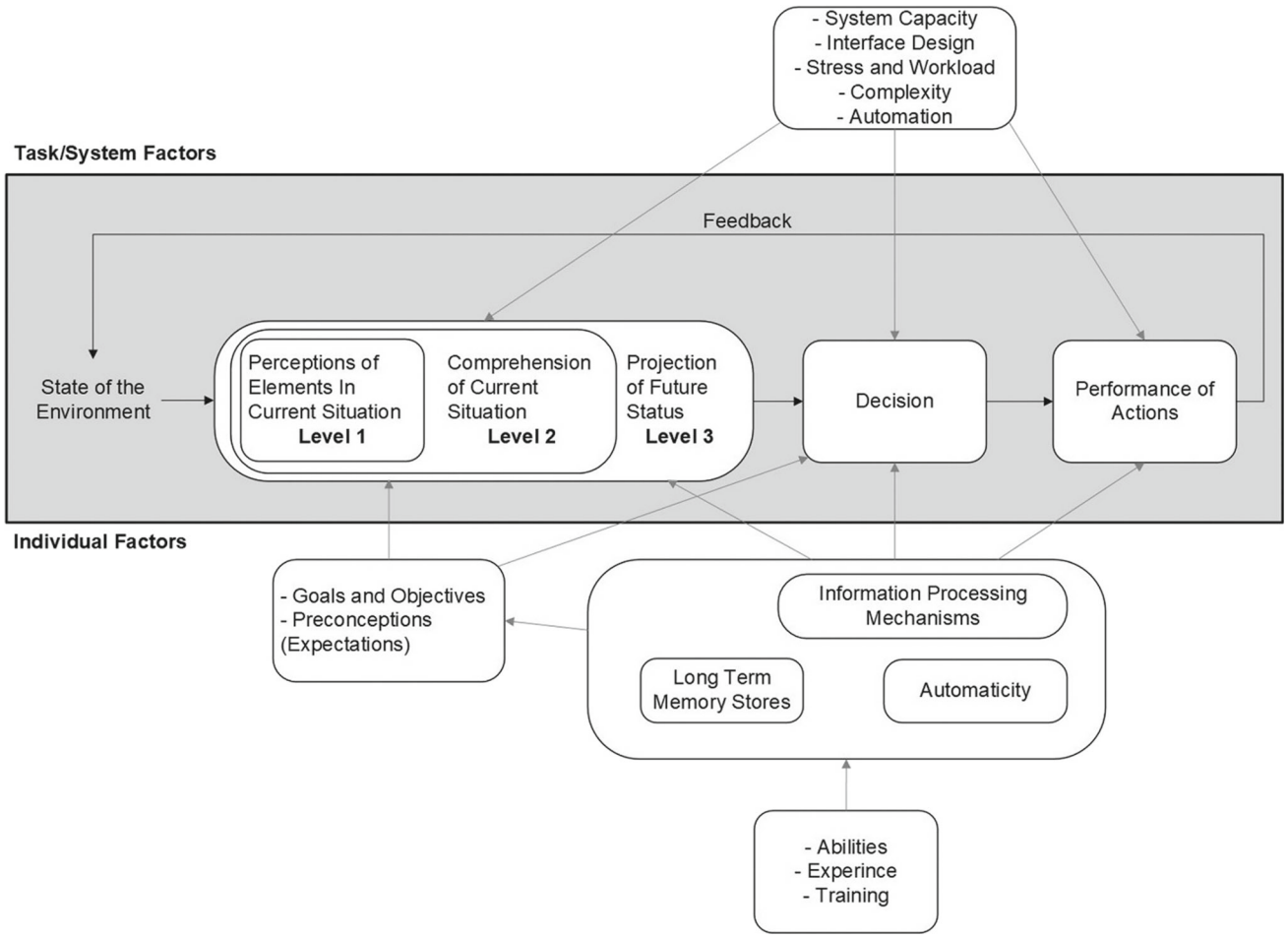

Fig. 1 Endsley's three-level SA model [18]

[23] are sometimes used, but these are dependent on validation through comparison with more direct SA measurements. Lastly, performance measures are often used as a supplement for SA measurement so that relevant performance data can be compared with corresponding measurements of SA [23]. Reviews of Cyber SA research show that there is a distinct lack of empirical testing where SA is measured using recognized methods [10, 11].

2.3 SA in SOCs

Within critical infrastructure, it is the SA of the personnel responsible for protecting digital systems that are most relevant for cyber security [25]. These personnel are often organized as groups of specialists responsible for the security of a defined set of networks, services, and equipment. In this article, such groups are termed *SOCs*. Within the research on SOCs, there is a growing realization that the human aspect of SOCs needs to be better understood. A recent review pointed out that the interactions between the human operators and the technology developed for SOCs need to be researched further to gain the full potential of SOCs [26]. There is likewise a growing realization that the performance of human operators is highly reliant on correct mental models and that training and exercises can benefit the operators in this aspect. The development of cyber ranges demonstrates this development [27]. One could argue that SA is a well-suited concept for investigation in SOCs because this context is highly comparable to other contexts where SA research has proven fruitful before.

In the same way as for Cyber SA more generally, the SA research within SOC settings is dominated by tool development that promises improved SA. In a recent review, we found that these promises are mostly based on assumptions. Very few studies have empirically investigated SA within SOCs. The studies that do assess SA mostly rely on performance measures or proxy measures [9]. There are few but noteworthy exceptions where multiple measurements are used including freeze-probe measurements [28, 29].

The lack of SA measurement in the context of SOCs can be attributed to missing in-depth analyses of SOC tasks. In order to perform specific SA measurements like freeze

probes or observer rating, one must first establish criteria for what constitutes higher or lower quality of SA. This is highly context-dependent and calls for an in-depth analysis of the SA processes within the specific context of SOCs. Methods of Task Analysis (TA) have been developed to gain such understanding of SA mechanisms within a specific context [30]. TAs are qualitative methods that map relevant tasks, decisions, and SA requirements for human operators. To develop rigorous measurement of SA in SOCs, such TAs are therefore an important first step that is largely missing within this context.

Research attempting to conduct TAs in SOC environments has been restricted by access to participants and observations in their working environments. There are several examples of mapping SOC-related tasks [31–42] but only a few studies document complete TAs aimed at SA [12, 13, 43–46]. One study from 2005 analyzed cyber defense tasks of information assurance analysts across several organizations. The few more recent studies that have conducted such TAs had restricted scopes and only analyzed SA in a small set of tasks or roles. One series of studies investigated the tasks and team communication of cyber analysts [13, 44], one study investigated the network defense tasks of cyber analysts [12], and a series of studies analyzed the tasks of log analysts [45, 46]. Many of the studies report that they had to make compromises regarding the scope and choice of methods because of restricted access. Several also stated that they would have conducted GDTAs if they had gained sufficient access to do so [12, 13]. GDTA is a recognized method for establishing an in-depth understanding of SA processes in new contexts [16]. There exists one reference and partial results from an unpublished GDTA for cyber defenders conducted in 2010 by Connors et.al. [47]. Apart from this to the best of the author's knowledge, no complete GDTAs that investigate the SA processes in SOCs have been published.

3 Methodology

The research setting is described in Sect. 3.1. Further, the methodology of this study consists of two parts. The first part of the study is a GDTA conducted according to existing guidelines described in Sect. 3.2. The second is an additional analysis of the variation of how goals are achieved by the SOC during incidents described in Sect. 3.3. The presentation of the methodology is concluded by the analysis of its limitations in Sect. 3.4.

3.1 Research setting

This study was conducted over one year in a SOC operating within Norwegian critical infrastructure. The SOC was responsible for network management and cyber security for large customers within the energy and manufacturing domains. This included tasks of monitoring networks and security systems as well as responding to incidents on a 24-h basis. Over 30 operators were employed at the SOC having varying degrees of experience ranging from 1 to over 15 + years. Their roles ranged in level of responsibility and content e.g., security operator, network operator, network technician, operations coordinator, security executive, technical executive, and SOC director. Nevertheless, they all were counted as SOC operators with overlapping tasks regarding incident response.

The SOC had one main location serving critical infrastructures distributed geographically at a national scale. The main location had one large operations control (OC) room with 8 workstations each with several monitors and a wall of larger monitors in view from all workstations. There was also one smaller OC room similarly configured but with fewer stations for operations coordination. The location also consisted of conference rooms applied with retractable workstations. These were used for incident response and allowed groups to discuss incidents while seamlessly continuing their workstation processes. Apart from this, there were 15 offices with one or two workstations each. Only the SOC employees and additional necessary staff had access to the SOC facilities. Research access to the SOC was ensured by employment as a researcher in the organization with the necessary security clearances to discuss the operators' work in depth and observe their work in situ.

All respondents in the study gave informed consent, and all information revealed in this article was reviewed and risk-assessed regarding unwanted disclosure by the SOC, before publication.

3.2 GDTA method

The first part of the study was a GDTA conducted following recognized guidelines [16]. This method can be described as an extensive qualitative process for establishing an in-depth understanding of SA processes within a new context [47]. GDTA method is comprised of a sequential series of semi-structured interviews with subject matter experts (SMEs). The process is described as an iterative one where the results from one interview are implemented into the preliminary GDTA and used as a base for the next interview. The GDTA can also be complemented with reviews of documents describing routines or documenting previous relevant events [16]. 8 steps are prescribed in the guidelines for conducting GDTAs that were followed throughout this first part of the study [30]. These 8 steps are presented in Fig. 2.

The method of GDTA gains most of its empirical data from interviews with SMEs. Within the guidelines of the GDTA method, there are only general descriptions of how the interviews are to be conducted [16, 30, 48]. In this study,

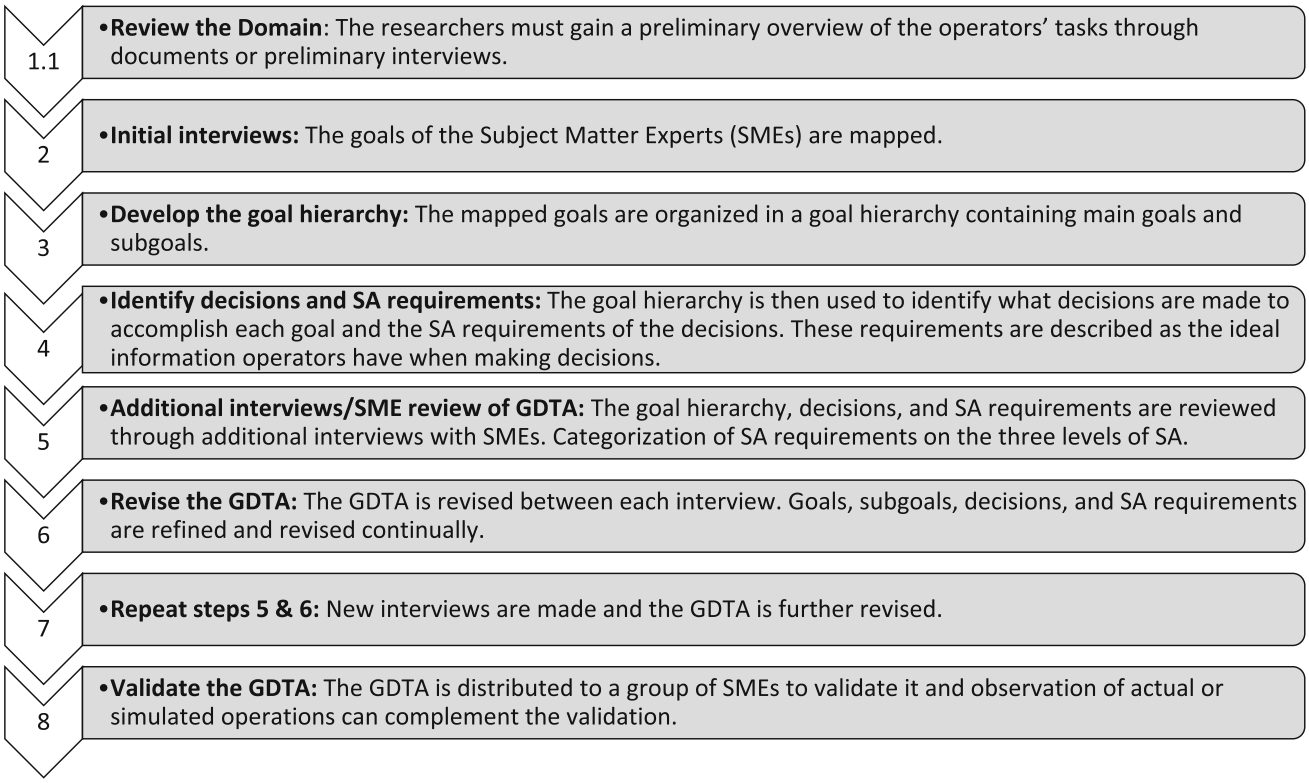

Fig. 2 The steps of the GDTA method [30]

the interviews were conducted with aimed methodological variations as described in Table 1. Empirical data gathered from the interviews were complemented by reviews of documents and reports as well as observation of work within the SOC. Each of the conducted steps of the GDTA is presented in Table 1, including what questions were asked, the number of respondents, and what data was collected.

Step 1 was initiated by a review of all relevant work descriptions and manuals for the SOC operators. This included role specifications and security guidelines as well as routines for incident escalation, incident management, and external communication. Then a series of 3 one-hour long unstructured interviews were conducted with the SOC's director in *Step 2*. These interviews were not audio-recorded but notes regarding the preliminary goal hierarchy were made and discussed during the interviews. Choosing the SOC director as the respondent in this step was done to gain the best overview of the SOC's goals. The SOC director had 15 + years of experience. In *Step 3* observations in the main OC room of the SOC were conducted. These observations were not made during the escalated incident response but during regular monitoring and planned work. This allowed the observation to consist of informal probing regarding how the operators worked and the systems they used. The data gathered in *Steps 1–3* was used to develop a preliminary goal hierarchy. This goal hierarchy was used together with all data gathered in *Steps 1–3* to make a preliminary GDTA in *Step 4*.

An interview guide was made based on recommended GDTA guidelines [16] and this was used during the interviews in *Step 5*. *Step 5* was conducted as six semi-structured interviews with SOC operators. The interviews lasted a total of over 6 h and were audio-recorded to ensure maximal information retention. Choosing respondents in this step was done to cover a wide array of different expertise areas within the SOC. The six respondents had different roles in the SOC, and their experience in their roles ranged from 3 to 10 years. Three of the respondents worked as network operators, while the other 3 worked as security operators. The respondents' responsibilities had some overlap, but they all had different specialist areas e.g., Intrusion Detection and Prevention Systems (IDPSs), Security Information and Event Management Systems (SIEMs), firewalls, network architecture, network diagnosis, and information security management. All the participants had considerable experience with incident response. The interview guide was gradually complemented by updated GDTAs which were used as a starting point for consecutive interviews. After each interview, the GDTA was updated based on the new information given by the respondents, as recommended by existing guidelines [30]. In *Step 6* all the gathered data was reviewed and a revised GDTA was established.

Table 1 Overview of methods used, and data gathered in the GDTA

GDTA step	Method used	Questions asked	Data sources/respondents	Data volume	Retrieved data/results
1. Review the Domain	Document review	How is the incident response of the SOC operators described?	Internal manuals and work descriptions for incident response	Approximately 200 pages of manuals and work descriptions	Notes, thought maps, descriptions
2. Initial interviews	Informal interviews	What are the goals of the SOC during incidents?	SOC-director	3 interviews of 60 min each	List of goals, notes
3. Develop the goal hierarchy	Analysis and observation	How are the goals of the SOC best categorized and put into a hierarchy?	Observation in the main OC room including informal conversations with present operators	12 h of observation on 5 different occasions	Preliminary goal hierarchy, field notes
4. Identify decisions and SA requirements	Analysis	What are the goals, decisions, and SA requirements of the SOC during incidents?	All data gathered in steps 1–3	All data gathered in steps 1–3	Preliminary GDTA
5. Additional interviews/SME review of GDTA	Semi-structured interviews	What tasks, goals, and decisions are involved in responding to incidents? What information is required to make the decision? How do you assess and use the information? How do you assess potential outcomes?	a) Network operator b) Network operator c) Network operator d) Security operator e) Security operator f) Security operator (3–10 years of experience)	a) 75-min interview b) 70-min interview c) 40-min interview d) 60-min interview e) 80-min interview f)50-min interview	Interview recordings, notes
6. Revise the GDTA	Analysis of data	Does the current GDTA adequately represent the gathered data?	All gathered data from steps 1–5	All gathered data from steps 1–5	Revised GDTA
7. Repeat steps 5 and 6	Unstructured interviews (a-b), analysis of data (c)	Does the current GDTA adequately represent the goals, decisions, and SA requirements of the SOC during incidents and the gathered data?	a) Security executive b) Network executive c) All gathered data from steps 1–7	a) 35-min interview b) 40-min interview c) All gathered data from steps 1–7	Interview notes, revised GDTA
8. Validate the GDTA	Observation of real-time incidents (a) and unstructured interviews (b–d)	Does the current GDTA adequately represent the incident response in the SOC?	a) Observation of three real-time escalated incidents b) Security operator c) Security operator and network operator d) Security operator	a) Two network-related incidents and one security-related incident including all meetings and briefings. b) 100-min interview c) 120-min interview with two respondents d) 40-min interview	Field notes, interview notes, final GDTA

Step 7 was conducted as two unstructured interviews with two of the SOC executives who were responsible for network and security operations respectively. The executives both had 15 + years of experience in their roles. Choosing respondents in this step was done to enable a revision of the whole GDTA based on experience in having an overview of operations as well as knowing the details involved. *Step 7* also involved a revision of the GDTA based on feedback from the initial peer review of the reported results. The GDTA was finally validated in *Step 8*. This involved the observation of 3 real-time escalated incidents, two of which were network-related and one security-related. A comparison of the observations made and the revised GDTA was enabled by asking specific questions during the incident evaluation meetings. This confirmed the match between the established GDTA and the actual observed incident responses. Finally, a series of 3 interviews with a total of 4 respondents were conducted to validate the final GDTA. Two of the respondents in *Step 8* had also been respondents in *Step 5*. In total the final GDTA was based on the review of 200 pages of documents, almost 15 h of interviews with 11 different SMEs, and over 25 h of in situ observation and conversations with the SOC operators.

3.3 Timeline method

In addition to the GDTA conducted as presented in Sect. 3.2, timelines describing variations in the prioritization of goals were developed. The timelines provide specific examples of how SA requirements are used to gain SA during incidents. This additional analysis is an original methodological step developed specifically for this study.

Using the developed GDTA as a basis, a review of 34 SOC reports from escalated incidents ranging back at most 3 years prior to the study was conducted. Different prioritizations of the goals in the GDTA during incidents were identified. This review resulted in a goal map that showed different possibilities regarding the order in which goals were performed. Then the different pathways through the goal map were compared with different types of incidents. The different types of identified incidents were exemplified by two realistic and illustrative timelines. This development of the goal map and timelines was also aided by many unstructured conversations with SOC operators throughout the study.

The goal map and the exemplified timelines were verified alongside the GDTA during *Steps 7–8* in the GDTA method described in Sect. 3.2.

3.4 Methodological limitations

Although the study was performed following the prescribed method of GDTA [16, 30] still, it has some methodological limitations. As in many other studies, the empirical base could have been stronger if the number of respondents had been larger. In some studies, this is the case [49, 50], yet the empirical base of this study was complemented by an extensive review of documents and incident reports. Furthermore, the observation of work within the SOC and the additional observation during actual escalated incidents including debriefing, strengthens the findings of the study. When comparing this to the other available studies that have performed TAs in SOC environments, this level of access to participants and their working environment is unique.

The unique access to participants was ensured by the employment of the author as a researcher by the SOC. This might be unconventional and asks for some consideration. One could argue that the author would be biased by the employment of the SOC when doing research. Yet, it is still somewhat difficult to argue that employment would sway the findings of this study in any particular direction. The study aims to describe the SA processes present in the SOC and does not make any judgment on quality nor does it promote a specific approach that benefits the SOC in question. Further, employment was the only way to gain access to the respondents and their environment. This is not only a practical question but also a legal one. Even though it is important to consider the potential bias of the connection between the researcher and respondents, it is equally important to note that the study would not be possible at all without this connection. This is confirmed by the previous attempts at conducting GDTAs in such environments [12, 13].

4 Results

In this section, the results of the study are presented and connected to the defined research questions. First, the goals within the SOC are described and presented in a goal hierarchy; this answers the first research question. Second, decisions and SA requirements are described and presented in tables of decisions with corresponding ideal SA requirements; this answers the second research question. Third, variations of goal prioritization and different timelines through incidents are described and visually presented; this answers the third research question. When presenting the results related to the first two research questions, this is done according to the guidelines of GDTA [16]. Meanwhile the goal map and timelines are additional results developed specifically for explaining SA processes within this context, so these are presented following the format found most suitable. The results including the goal map and timelines are further used in Sect. 6 for discussing SA theory and levels of conceptualization within the context of SOCs.

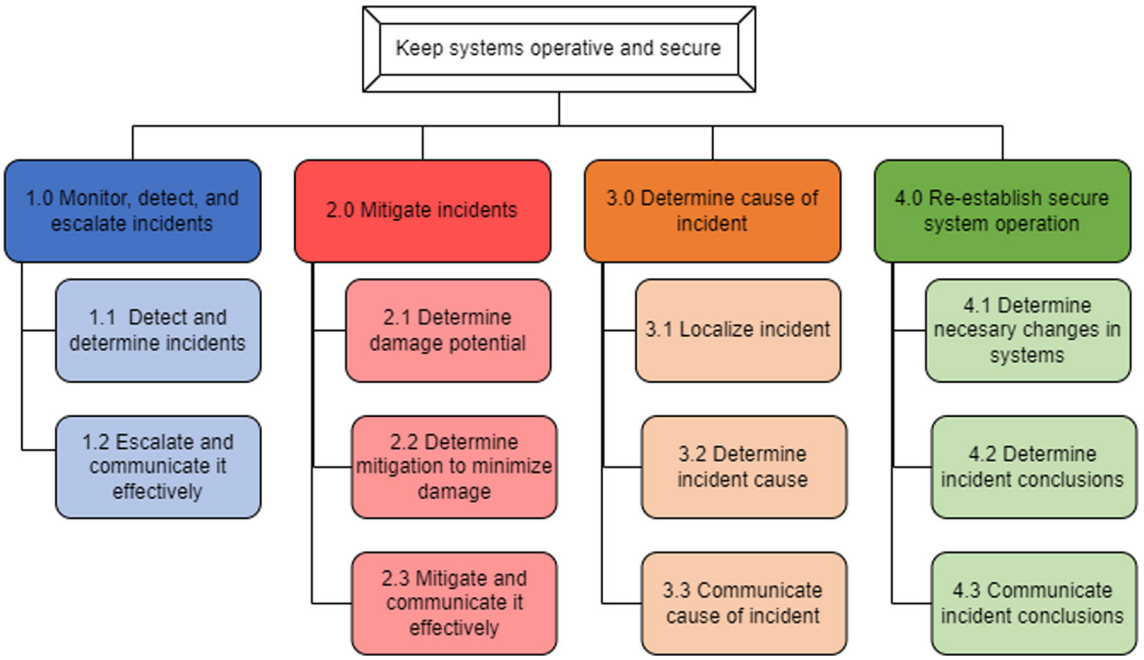

Fig. 3 Goal hierarchy

4.1 Goals within the SOC

When investigating the goals of the SOC, one main goal was identified which is accomplished through a set of interconnected major goals and subgoals. The goal hierarchy is rich with partially conflicting subgoals which are negotiated based on the specifics of the situation. How the goals are prioritized varies based on the nature of the incidents and is also sometimes shifted throughout an incident based on the changing awareness of operators. Still, all the subgoals are completed before the SOC concludes the management of an incident. In Fig. 3 the goals are presented and categorized in the form of a goal hierarchy.

The main goal of the SOC was operationalized and accomplished through the following 4 major goals:

1. *Monitor, detect, and escalate incidents* includes monitoring network status and security alerts. Potential incidents are identified and escalated to mobilize incident response from the SOC.
2. *Mitigate incidents* includes subgoals to assess damage potential and to implement mitigations to minimize damage caused by the incident. The mitigations are temporary and often adjusted according to the progression of the incident. The effective communication of mitigation is an important subgoal to render mitigations effective and minimize negative consequences.
3. *Determine cause of incident* includes the localization of the incident and the assessment of hypotheses regarding its cause. It is also important (subgoals) to verify the correctness of the identified causes and to communicate causes both internally in the SOC and to relevant stakeholders.
4. *Re-establish secure system operation* includes the implementation of necessary lasting changes to systems and communicating these effectively to reduce further vulnerabilities. Another important subgoal is to communicate the conclusions from the incident, to prevent future failures or security incidents.

The goals of the SOC are heavily interconnected, and their prioritization is situation-specific. Usually, it is the completion of goal *1.2 Escalate incident and communicate it effectively* that triggers the other goals in the hierarchy. The mitigation and identification of causes are often intertwined, and the goals are met through iterative processes where the partial completion of one goal serves as an SA requirement for another goal. One example of this is when a preliminary coarse-grained topological localization of a security breach triggers the isolation of a large portion of a network as a mitigation measure. Consecutive fine-grained localizations of the incident serve as updated SA requirements leading to moderated isolations in the network. Other goals are more loosely connected. Subgoal *4.3 Communicate incident conclusions* provides information to the decision-making on other goals in the future. Likewise, the identification of incident causes might trigger temporary changes to the goals of escalating incidents by heightened alertness or focused monitoring. The goal hierarchy presented in Fig. 3 is therefore best described as a general presentation of the SOC's goals. The specific

prioritization of goals varies and is better understood when exemplified by the timelines presented in Sect. 4.3.

4.2 Decisions and SA requirements

The results from the GDTA include a mapping of all decisions related to the goals in the goal hierarchy. For these decisions, ideal SA requirements were identified and categorized based on their level of SA. The study identified a total of 15 decisions related to the subgoals of the operator tasks during incidents. The number of decisions relating to each subgoal ranged from one decision to at most 3 decisions per subgoal. Table 2 presents the identified decisions the operators need to make during the completion of the subgoals presented in Fig. 3.

Each of the decisions had several SA requirements related to them, although the number of ideal SA requirements related to one decision ranged substantially. In total 136 unique SA requirements related to the 15 decisions. Several of them are duplicated and serve as requirements for more than one decision. 83 unique level 1 SA requirements were identified including 13 groups of information that were often used together, that are presented as callouts as recommended in GDTA guidelines [16]. One example is the callout named *Network Management System (NMS) alerts* consisting of *Alert type*, *Alert severity,* and *Node name.* Table 3 presents all the unique level 1 SA requirements, and the grouped callouts numbered 1–13. Table 3 also presents a thematic categorization of the type of information the requirements consisted of.

All the SA requirements were also differentiated into the 3 levels of SA. The requirements on level 1 as presented in Table 3, provide the perceived information that is further used to gain comprehension and projection according to the 3-level model of SA [13]. The categorization of requirements on SA levels is presented in Table 4.

A complete overview of decisions and SA requirements is presented in Table 5. The table presents all the identified SA requirements related to each decision. The SA requirements are also categorized by SA level. Many of the decisions are interconnected through the SA requirements. In addition, one decision may be dependent on another in unpredictable ways. One example is the connection between the 3 decisions: *3.2.2 What is the verified cause of the incident?*, *2.1.1 What is the damage potential of the network incident?,* and *2.2.1 How should incident be mitigated?* In some incidents, one must first verify the cause of the incident (*3.2.2*) to mitigate (*2.2.1*), and only later recognize the true damage potential (*2.1.1*). In other incidents, the damage potential (*2.1.1*) is assessed first to determine the mitigation (*2.2.1*), and the actual cause of the incident (*3.2.2*) is only discovered later. Such connections between decisions and differences between incidents are investigated further in Sect. 4.3.

Table 2 Goals and decisions for operators during incidents

1. Monitor, detect, and escalate incidents	*2. Mitigate incidents*	*3. Determine cause of incident*	*4. Re-establish secure system operation*
1.1 Detect and determine incidents	*2.1 Determine damage potential*	*3.1 Localize incident*	*4.1 Determine necessary changes in systems*
1.1.1 How do current events indicate a network incident?	2.1.1 What is the damage potential of the network incident?	3.1.1 What are the location and extent of the incident?	4.1.1 What system changes should be done?
1.1.2 How do current events indicate a security incident?	2.1.2 What is the damage potential of the security incident?	*3.2 Determine incident cause*	*4.2 Determine incident conclusions*
1.1.3 How can current events be explained as expected or benign?	*2.2 Determine mitigation to minimize damage*	3.2.1 What are potential causes of the incident?	4.2.1 What incident conclusions should be made?
1.2 Escalate and communicate effectively	2.2.1 How should incident be mitigated?	3.2.2 What is the verified cause of the incident?	*4.3 Communicate incident conclusions*
1.2.1 How should escalation be communicated?	*2.3 Mitigate and communicate mitigation effectively*	*3.3 Communicate cause of incident*	4.3.1 How can the incident conclusions be communicated effectively?
	2.3.1 How should mitigation be communicated?	3.3.1 How can the cause be communicated effectively?	

4.3 Goal map and timelines

The identified decisions and SA requirements demonstrate the complex nature of SOC operator tasks. This complexity is partly due to the interconnected nature of goals and consequently, the decisions associated with each goal. In order to present the complexity identified in the GDTA, an additional analysis of incident timelines is presented in this section. Although this is not required in the GDTA method, this author believes that it will provide a more complete understanding of the SA mechanisms present during incidents in SOCs.

Table 3 Level 1 SA requirements categorized by type of information

Information from sensor/analytical technology	*Information from documentation on systems/operations*	*Logged information on systems/operations*	*Information from communication with stakeholders*	*Information on current/future operations*	*Description of routines or requirements*	*External information*
Network Management System (NMS) alerts[1]	Technical documentation of affected parts of network[3]	Historian data indicating recurring benign events	Partner/customer event updates (calls, instant messaging)	Updated Planned Activity In Network (PAIN) list[6]	Incident escalation routine description	Weather forecast
• Alert type	• Node type	Event log	Internal event updates (calls, instant messaging)	• Planned activity description	Service level agreements with partner/customer	Common Vulnerabilities and Exposures (CVE) reports[9]
• Alert severity	• Connection type (fiber/wired/wireless/radio)	Partner/customer communication logs (calls, instant messaging)	Incoming support requests from partners/customers	• Time of planned activity	Incident response routine description	• Vulnerability description
• Node name	• Power source type and redundancy	Partner/customer communication logs (calls, instant messaging)	Partner/customer incident updates (calls, instant messaging)	• Expected network impact of planned activity	Results from security revisions	• Severity level of vulnerability
NMS status of affected parts of network[2]	• Technical specifications of equipment and software (Manufacturer, model, patch version, patch date, release notes, etc.)	Internal communication logs (calls, instant messaging)	Internal incident updates (calls, instant messaging)	• Responsibility for planned activity	State of the art descriptions[13]	• Vendor and system information
• Node status	Contextual documentation of affected systems[4]	Connection log[10]	Communication with public relations responsible	Relevant tickets for requested work in network	• Governmental system requirements	Media reports of security events
• Link status	• Geographical position (site location, asset location on site)	• Source IP	On-site cause verification results (physical observations, user/operator statements)	Updated staff roster with responsibilities	• Industry standard requirements	Media reports of network or online service outages
• Network congestion status	• Topological architecture (network redundancy and rerouting possibilities)	• Destination IP	Feedback from customer/partner on incident performance	Mitigation requirements (staff, equipment, system access, etc.)	• Recommended best practice	External verification of cause hypotheses (incident statements from governmental or industry actors)
• Hardware status (temperature, system resource utilization)	• Installation and maintenance logs	• Geoloc		System change requirements (staff, equipment, time, etc.)	Governmental requirements for CVE	

Table 3 (continued)

Intrusion Detection and Prevention System (IDPS) alerts[7]	Connected services documentation[5]	• Destination Port				
• IDPS signature match	• Description of connected services	Notes from determination of mitigation (see subgoal 2.2)				
• IP address	• Criticality of connected services	Notes from determination of cause (see subgoal 3.2)				
• Session type (TCP/UDP)	• Service redundancy	Time of first incident indication				
• Port	Updated partner/customer contact database	Time of incident escalation				
• Data packet inspection results	System design information[11]	Escalation level initially and throughout incident				
• Logged prevention system actions	• Access information	Summary of occurred events				
Security Information and Event Management (SIEM) alerts[8]	• Protocols	Summary of mitigations				
• SIEM signature match	• Services	Summary of incident cause				
• System type (OS type and version)	• Security design principles (zero trust, least privilege)					
• User ID	User privilege escalation information[12]					
• System process information	• Security group membership					
• Severity level of SIEM alert	• Active directory					
• Identified anomalies based on log inspection	• Config of services					
Current power failures in electrical grid map	Firewall policy status					
Technical cause verification results (system tests, reboots, equipment replacements)	Spare equipment inventory					
	Results from internal evaluation of incident performance					
	Incident conclusion results					

Table 4 SA requirements categorized by SA level

Perception (SA level 1)	Comprehension (SA level 2)	Projection (SA level 3)
NMS alerts[1]	Assessed impact of network events on operational status	Predicted impact of network events
NMS status of affected parts of network[2]	Assessed impact of external factors on operational status	Predicted impact of security events
Technical documentation of affected parts of network[3]	Assessed impact of security events on operational status	Predicted benign cause of current events
Contextual documentation of affected systems[4]	Assessed impact of external security indications on operational status	Projected required escalation communication
Connected services documentation[5]		Projected damage potential of network incident
Partner/customer event updates (calls, instant messaging)	Assessed impact of benign or expected events on present incident indications	Projected damage potential of security incident
Internal event updates (calls, instant messaging)		Projected impact of network mitigation
Weather forecast	Assessed required incident communication content	Projected impact of security mitigation
Incoming support requests from partners/customers	Assessed required incident communication recipients	Projected required mitigation communication
Updated PAIN list[6]	Determined technical impact of network incident	Projected extent of incident
Relevant tickets for requested work in network	Determined contextual impact of network incident	Predicted cause of incident
IDPS alerts[7]	Determined impact of external factors	Projected required cause communication
SIEM alerts[8]	Determined technical impact of security incident	Projected impact of system changes
CVE reports[9]	Determined contextual impact of security incident	Projected improvements in future incident response
Media reports of security events	Determined network mitigation alternatives	Projected required incident conclusion communication
Media reports of network or online service outages	Assessed impact of network mitigation alternatives	
Current power failures in electrical grid map	Determined security mitigation alternatives	
Historian data indicating recurring benign events	Assessed impact of security mitigation alternatives	
Event log	Assessed required mitigation communication content	
Partner/customer communication logs (calls, instant messaging)	Assessed required mitigation communication recipients	
Internal communication logs (calls, instant messaging)	Determined geographical location(s) of incident	
Notes from determination of incident (see subgoal 1.1)	Determined topological location(s) of incident	
Incident escalation routine description	Assessed potential for incident spreading	
Updated staff roster with responsibilities	Assessed network cause hypotheses	
Service level agreements with partner/customer	Assessed security cause hypotheses	
Updated partner/customer contact database	Assessed verification method of incident cause	
Partner/customer incident updates (calls, instant messaging)	Determined verification of cause	

Table 4 (continued)

Perception (SA level 1)	Comprehension (SA level 2)	Projection (SA level 3)
Internal incident updates (calls, instant messaging)	Assessed required cause communication content	
Historian data from similar incidents	Assessed required cause communication recipients	
Connection log[10]	Determined system changes	
System design information[11]	Determined incident conclusions	
User privilege escalation information[12]	Determined gap between current incident response and incident conclusions	
Firewall policy status		
Mitigation requirements (staff, equipment, system access, etc.)	Assessed required incident conclusion communication content	
Spare equipment inventory		
Notes from determination of mitigation (see subgoal 2.2)		
Incident response routine description		
On-site cause verification results (physical observations, user/operator statements)		
Technical cause verification results (system tests, reboots, equipment replacements)		
Communication with public relations responsible		
External verification of cause hypotheses (incident statements from governmental or industry actors)		
Notes from determination of cause (see subgoal 3.2)		
Results from security revisions		
State of the art descriptions[13]		
System change requirements (staff, equipment, time, etc.)		
Time of first incident indication		
Time of incident escalation		
Escalation level initially and throughout incident		
Summary of occurred events		
Summary of mitigations		
Summary of incident cause		
Results from internal evaluation of incident performance		
Feedback from customer/partner on incident performance		
Incident conclusion results		
Governmental requirements for CVE		

See Table 3*for SA requirement callouts 1–13*

Table 5 Goals, decisions, and SA requirements

1. Monitor, detect, and escalate incidents	*2. Mitigate incidents*	*3. Determine cause of incident*	*4. Re-establish secure system operation*	*Information Requirement Callouts*
1.1 Detect and determine incidents	*2.1 Determine damage potential*	*3.1 Localize incident*	*4.1 Determine necessary changes in systems*	*1 Network Management System (NMS) alerts*
				· Alert type
1.1.1 How do current events indicate a network incident?	2.1.1 What is the damage potential of the network incident?	3.1.1 What are the location and extent of the incident?	4.1.1 What system changes should be done?	· Alert severity
Δ Projection | – Comprehension | · Perception	Δ Projection | – Comprehension | · Perception	Δ Projection | – Comprehension | · Perception	Δ Projection | – Comprehension | · Perception	· Node name
Δ Predicted impact of network events	Δ Projected damage potential of network incident	Δ Projected extent of incident	Δ Projected impact of system changes	
– Assessed impact of network events on operational status	– Determined technical impact of network incident	– Determined geographical location(s) of incident	– Determined system changes	*2 NMS status of affected parts of network*
· NMS alerts[1]	· NMS alerts[1]	· NMS alerts[1]	· Technical documentation of affected parts of network[3]	· Node status
· NMS status of affected parts of network[2]	· NMS status of affected parts of network[2]	· NMS status of affected parts of network[2]	· Contextual documentation of affected systems[4]	· Link status
· Technical documentation of affected parts of network[3]	· Technical documentation of affected parts of network[3]	· IDPS alerts[7]	· Connected services documentation[5]	· Network congestion status
· Contextual documentation of affected systems[4]	· Partner/customer incident updates (calls, instant messaging)	· SIEM alerts[8]	· System design information[11]	· Hardware status (temperature, system resource utilization)
· Connected services documentation[5]	· Internal incident updates (calls, instant messaging)	· Contextual documentation of affected systems[4]	· CVE reports[9]	
· Partner/customer event updates (calls, instant messaging)	– Determined contextual impact of network incident	· Partner/customer incident updates (calls, instant messaging)	· Results from security revisions	*3 Technical documentation of affected parts of network*
· Internal event updates (calls, instant messaging)	· Contextual documentation of affected systems[4]	· Internal incident updates (calls, instant messaging)	· State of the art descriptions[13]	· Node type
–Assessed impact of external factors on operational status	· Connected services documentation[5]	– Determined topological location(s) of incident	· System change requirements (staff, equipment, time, etc.)	· Connection type (fiber/wired/wireless/radio)
· Weather forecast	· Partner/customer incident updates (calls, instant messaging)	· NMS alerts[1]	· Service level agreements with partner/customer	· Power source type and redundancy
· Incoming support requests from partners/customers	· Internal incident updates (calls, instant messaging)	· NMS status of affected parts of network[2]		· Technical specifications of equipment and software (Manufacturer, model, patch version, patch date, release notes, etc.)

Table 5 (continued)

1. Monitor, detect, and escalate incidents	*2. Mitigate incidents*	*3. Determine cause of incident*	*4. Re-establish secure system operation*	*Information Requirement Callouts*
· Updated PAIN list[6]	· Historian data from similar incidents	· Technical documentation of affected parts of network[3]	*4.2 Determine incident conclusions*	
· Relevant tickets for requested work in network	– Determined impact of external factors	· IDPS alerts[7]		*4 Contextual documentation of affected systems*
	· Weather forecast	· SIEM alerts[8]	4.2.1 What incident conclusions should be done?	· Geographical position (site location, asset location on site)
1.1.2 How do current events indicate a security incident?	· Incoming support requests from partners/customers	· System design information[11]	Δ Projection | – Comprehension | · Perception	· Topological architecture (network redundancy and rerouting possibilities)
Δ Projection | – Comprehension | · Perception	· Updated PAIN list[6]	· Contextual documentation of affected systems[4]	Δ Projected improvements in future incident response	· Installation and maintenance logs
Δ Predicted impact of security events	· Relevant tickets for requested work in network	– Assessed potential for incident spreading	– Determined incident conclusions	
– Assessed impact of security events on operational status		· NMS status of affected parts of network[2]	· Time of first incident indication	*5 Connected services documentation*
· IDPS alerts[7]	2.1.2 What is the damage potential of the security incident?	· Technical documentation of affected parts of network[3]	· Time of incident escalation	· Description of connected services
· SIEM alerts[8]	Δ Projection | – Comprehension | · Perception	· Contextual documentation of affected systems[4]	· Escalation level initially and throughout incident	· Criticality of connected services
· Contextual documentation of affected systems[4]	Δ Projected damage potential of security incident	· Connected services documentation[5]	· Summary of occurred events	· Service redundancy
· Connected services documentation[5]	– Determined technical impact of security incident	· System design information[11]	· Summary of mitigations	
· Partner/customer event updates (calls, instant messaging)	· IDPS alerts[7]	· User privilege escalation information[12]	· Summary of incident cause	*6 Updated Planned Activity In Network (PAIN) list*
· Internal event updates (calls, instant messaging)	· SIEM alerts[8]	· CVE reports[9]	· Results from internal evaluation of incident performance	· Planned activity description
– Assessed impact of external security indications on operational status	· Connection log[10]	· Partner/customer incident updates (calls, instant messaging)	· Feedback from customer/partner on incident performance	· Time of planned activity
· CVE reports9	– Determined contextual impact of security incident	· Internal incident updates (calls, instant messaging)	– Determined gap between current incident response and incident conclusions	· Expected network impact of planned activity
· Media reports of security events	· System design information[11]	· Historian data from similar incidents	· Incident escalation routine description	· Responsibility for planned activity

Table 5 (continued)

1. Monitor, detect, and escalate incidents	*2. Mitigate incidents*	*3. Determine cause of incident*	*4. Re-establish secure system operation*	*Information Requirement Callouts*
· Incoming support requests from partners/customers	· User privilege escalation information[12]	·Weather forecast	· Incident response routine description	
	· Contextual documentation of affected systems[4]	· Incoming support requests from partners/customers	· Incident conclusion results	*7 Intrusion Detection and Prevention System (IDPS) alerts*
1.1.3 How can current events be explained as expected or benign?	· Connected services documentation[5]			· IDPS signature match
Δ Projection | – Comprehension | · Perception	· Firewall policy status	*3.2 Determine incident cause*	*4.3 Communicate incident conclusions*	· IP address
Δ Predicted benign cause of current events	· CVE reports[9]			· Session type (tcp/udp)
– Assessed impact of benign or expected events on present incident indications		3.2.1 What are potential causes for the incident?	4.3.1 How can the incident conclusions be communicated effectively?	· Port
· Updated PAIN list[6]	*2.2 Determine mitigation to minimize damage*	Δ Projection | – Comprehension | · Perception	Δ Projection | – Comprehension | · Perception	· Data packet inspection results
· Partner/customer event updates (calls, instant messaging)		Δ Predicted cause of incident	Δ Projected required incident conclusion communication	· Logged prevention system actions
· Internal event updates (calls, instant messaging)	2.2.1 How should incident be mitigated?	– Assessed network cause hypotheses	– Assessed required incident conclusion communication content	
· Media reports of network or online service outages	Δ Projection | – Comprehension | · Perception	· NMS alerts[1]	· Incident conclusion results	*8 Security Information and Event Management (SIEM) alerts*
· Current power failures in electrical grid map	Δ Projected impact of network mitigation	· Event log	– Assessed required incident conclusion communication recipients	· SIEM signature match
· Historian data indicating recurring benign events	– Determined network mitigation alternatives	· NMS status of affected parts of network[2]	· Service level agreements with partner/customer	· System type (OS type and version)
	· NMS status of affected parts of network[2]	· Technical documentation of affected parts of network[3]	· Communication with public relations responsible	· User ID
1.2 Escalate and communicate effectively	· Technical documentation of affected parts of network[3]	· Contextual documentation of affected systems[4]	· Governmental requirements for CVE	· System process information
	· Contextual documentation of affected systems[4]	· Partner/customer incident updates (calls, instant messaging)		· Severity level of SIEM alert
1.2.1 How should escalation be communicated?	· Mitigation requirements (staff, equipment, system access etc.)	· Internal incident updates (calls, instant messaging)		· Identified anomalies based on log inspection

Table 5 (continued)

1. Monitor, detect, and escalate incidents	*2. Mitigate incidents*	*3. Determine cause of incident*	*4. Re-establish secure system operation*	*Information Requirement Callouts*
Δ Projection | – Comprehension | · Perception	· Updated staff roster with responsibilities	· Historian data from similar incidents		
Δ Projected required escalation communication	· Spare equipment inventory	– Assessed security cause hypotheses		*9 Common Vulnerabilities and Exposures (CVE) reports*
– Assessed required incident communication content	· Service level agreements with partner/customer	· IDPS alerts[7]		· Vulnerability description
· Event log	– Assessed impact of network mitigation alternatives	· SIEM alerts[8]		· Severity level of vulnerability
· Partner/customer communication logs (calls, instant messaging)	· NMS status of affected parts of network[2]	· Contextual documentation of affected systems[4]		· Vendor and system information
· Internal communication logs (calls, instant messaging)	· Technical documentation of affected parts of network[3]	· Connected services documentation[5]		
· Notes from determination of incident (see subgoal 1.1)	· Contextual documentation of affected systems[4]	· System design information[11]		*10 Connection log*
· Incident escalation routine description	· Connected services documentation[5]	· User privilege escalation information[12]		· Source IP
– Assessed required incident communication recipients	· Partner/customer incident updates (calls, instant messaging)	· CVE reports[9]		· Destination IP
· Incident escalation routine description	· Internal incident updates (calls, instant messaging)	· Connection log[10]		· Geoloc
· Updated staff roster with responsibilities	· Historian data from similar incidents			· Destination Port
· Service level agreements with partner/customer	Δ Projected impact of security mitigation	3.2.2 What is the verified cause of the incident?		
· Updated partner/customer contact database	– Determined security mitigation alternatives	Δ Projection | – Comprehension | · Perception		*11 System design information*
	· System design information[11]	–Assessed verification method of incident cause		· Access information
	· User privilege escalation information[12]	· Technical documentation of affected parts of network[3]		· Protocols
	· Firewall policy status	· Contextual documentation of affected systems[4]		· Services
	· CVE reports[9]	· Historian data from similar incidents		· Security design principles (zero trust, least privilege)

Table 5 (continued)

1. Monitor, detect, and escalate incidents	*2. Mitigate incidents*	*3. Determine cause of incident*	*4. Re-establish secure system operation*	*Information Requirement Callouts*
	· Mitigation requirements (staff, equipment, system access, etc.)	· Connected services documentation[5]		
	· Updated staff roster with responsibilities	· System design information[11]		*12 User privilege escalation information*
	· Spare equipment inventory	· User privilege escalation information[12]		· Security group membership
	· Service level agreements with partner/customer	· CVE reports[9]		· Active directory
	– Assessed impact of security mitigation alternatives	· Partner/customer incident updates (calls, instant messaging)		· Config of services
	· Contextual documentation of affected systems[4]	· Internal incident updates (calls, instant messaging)		
	· Connected services documentation[5]	· Service level agreements with partner/customer		*13 State of the art descriptions*
	· System design information[11]	– Determined verification of cause		· Governmental system requirements
	· User privilege escalation information[12]	· On-site cause verification results (physical observations, user/operator statements)		· Industry standard requirements
	· CVE reports[9]	· Technical cause verification results (system tests, reboots, equipment replacements)		· Recommended best practice
	· Partner/customer incident updates (calls, instant messaging)	· External verification of cause hypotheses (incident statements from governmental or industry actors)		
	· Internal incident updates (calls, instant messaging)			
		3.3 Communicate cause of incident		
	2.3 Mitigate and communicate mitigation effectively			
		3.3.1 How can the cause be communicated effectively?		
	2.3.1 How should mitigation be communicated?	Δ Projection | – Comprehension | · Perception		
	Δ Projection | – Comprehension | · Perception	Δ Projected required cause communication		

Table 5 (continued)

1. Monitor, detect, and escalate incidents	*2. Mitigate incidents*	*3. Determine cause of incident*	*4. Re-establish secure system operation*	*Information Requirement Callouts*
	Δ Projected required mitigation communication	– Assessed required cause communication content		
	– Assessed required mitigation communication content	· Partner/customer communication logs (calls, instant messaging)		
	· Partner/customer communication logs (calls, instant messaging)	· Internal communication logs (calls, instant messaging)		
	· Internal communication logs (calls, instant messaging)	· Notes from determination of cause (see subgoal 3.2)		
	· Notes from determination of mitigation (see subgoal 2.2)	– Assessed required cause communication recipients		
	· Incident response routine description	· Updated staff roster with responsibilities		
	– Assessed required mitigation communication recipients	· Service level agreements with partner/customer		
	· Updated staff roster with responsibilities	· Updated partner/customer contact database		
	· Service level agreements with partner/customer	· Communication with public relations responsible		
	· Updated partner/customer contact database			
	· Communication with public relations responsible			
	· Incident response routine description			

It was pointed out in many of the interviews that the prioritization of goals was context-dependent. Upon further questioning regarding the specifics of this variation, the study sampled different possible paths through the completion of the 4 identified major goals and their subgoals. The sampled paths were then compared with the reviewed incident reports. This confirmed the presence of some assumed paths and complemented the developed map with some additional pathways. Finally, a complete map of possible pathways through the goals was validated. This resulted in the goal map presented in Fig. 4. The coloring of the goals in Fig. 4 matches that of Fig. 3, to facilitate comparison.

As the goal map in Fig. 4 shows, there are several possible paths available for completing the subgoals during an incident. The incident response is in most cases initiated by completing the goal of *1. Identify and escalate incidents.* Going forward from this, there are several different possibilities for how to prioritize consecutive goals. *2. Mitigate incidents* and *3. Determine cause of incident* is often an effort done in tandem where loops of iterative goal completion are necessary. Some clear patterns in the choice of pathways between different types of incidents were identified in this study. Although a complete explanation of contextual considerations behind the choice of pathway is beyond the scope

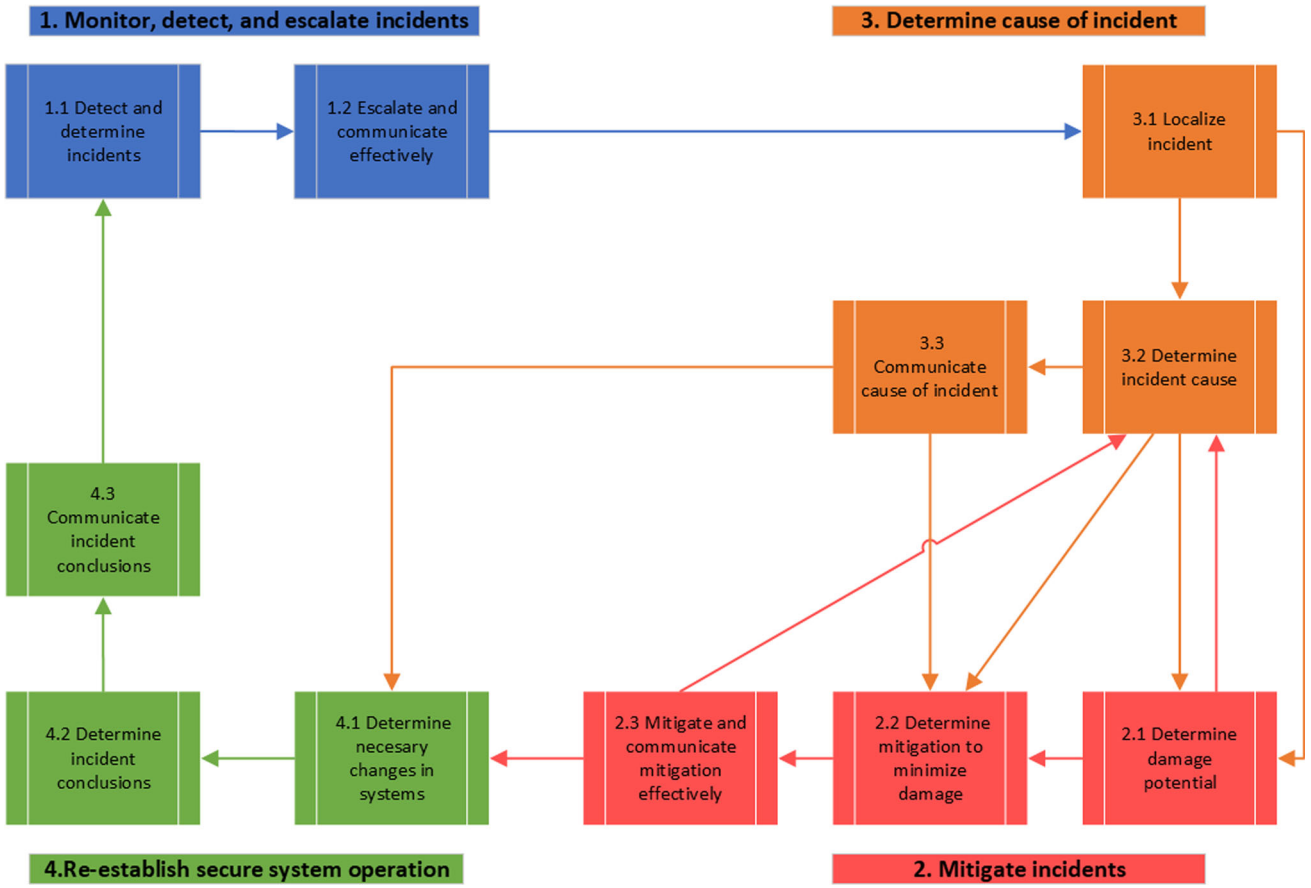

Fig. 4 Goal map

of this study, some of the identified patterns are described and presented.

The most prevalent pattern regarding the choice of goal paths was related to differences between network and security incidents. Network incidents are here defined as incidents causing parts of the network to be unavailable because of physical, technical, or logical failures. Security incidents are on the other hand defined as incidents causing confidentiality or security attributes within the network to be threatened or compromised. When reviewing the incident reports, it was identified that in network incidents the identification of cause was prioritized before mitigation. The interviews revealed that this was because it often was impossible to perform mitigation in network incidents before the cause was identified. This was not the case in security incidents where mitigation often was prioritized early in the incident and modified in tandem with the development of SA regarding the cause.

This main difference in goal paths is further explained by presenting two different timelines. One timeline presents a realistic network incident (Fig. 5), and one presents a realistic security incident (Fig. 6). The timelines show why and how the completion of goals is prioritized differently and consequently why decisions are made in different orders between the timelines. Validation of the realism of timelines was established during *Steps 7–8* in the GDTA method described in Sect. 3.2. The timelines were found to be representative of the two types of incidents by the respondents.

Relations between goals, decisions, and SA requirements were explained in more detail by the timelines. They show how not all identified SA requirements for a given decision are relevant in all incidents. In Table 5 decisions and SA requirements are presented following existing guidelines for the GDTA method. Table 5 thus presents the totality of SA requirements relevant across all types of incidents. In contrast, the timelines in Fig. 5 and Fig. 6 only present the relevant SA requirements in the given situations. Therefore, the timelines give a complementary understanding of how SA requirements may vary from incident to incident. Specific SA requirements related to each decision are presented throughout the exemplified incidents.

To facilitate comparison between figures and tables, the decisions in the timelines are colored according to the overview of goals in Fig. 3. Furthermore, the path taken through the goal map of Fig. 4 is indicated at the top of each timeline contributing to such comparison.

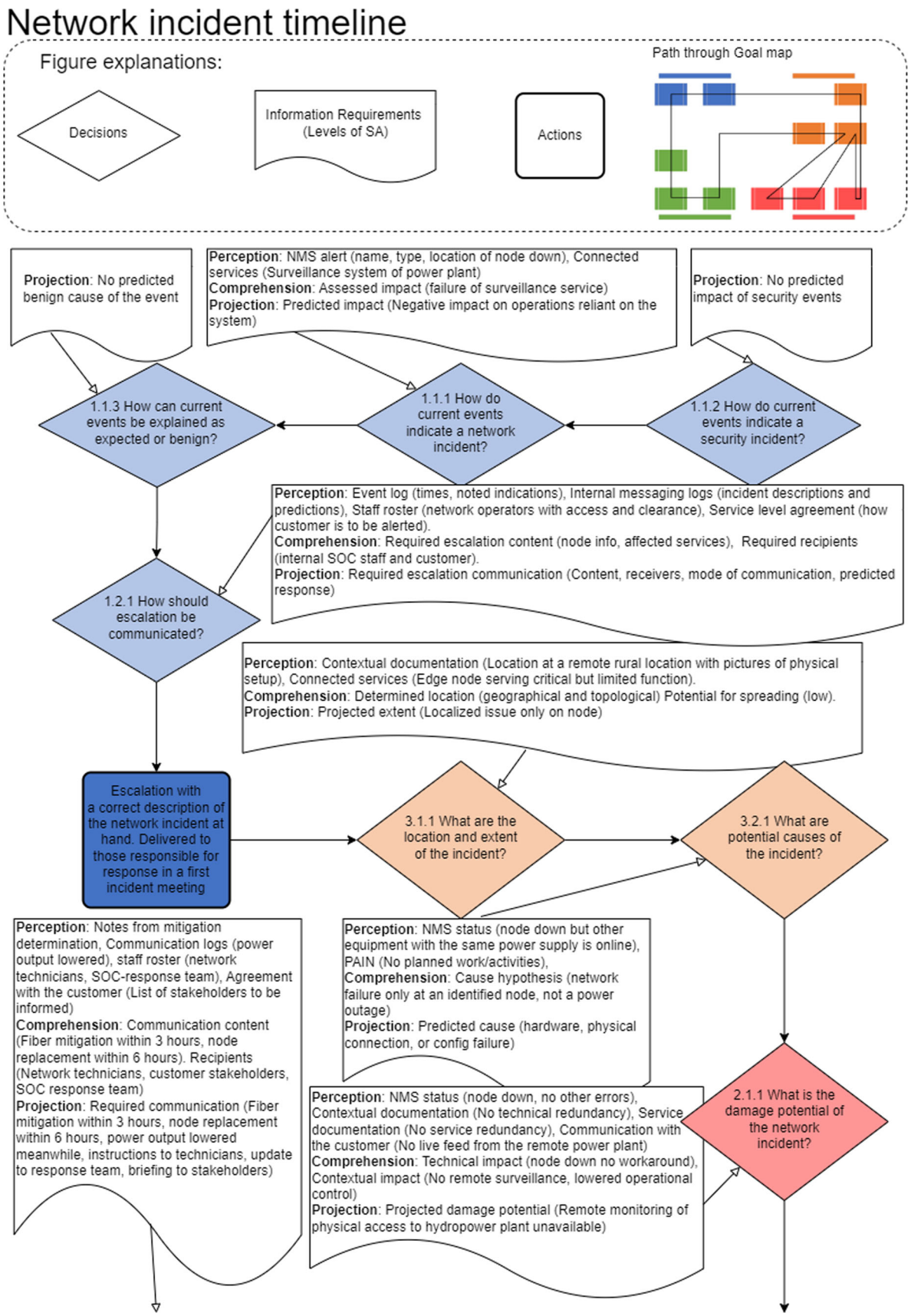

Fig. 5 Network incident timeline

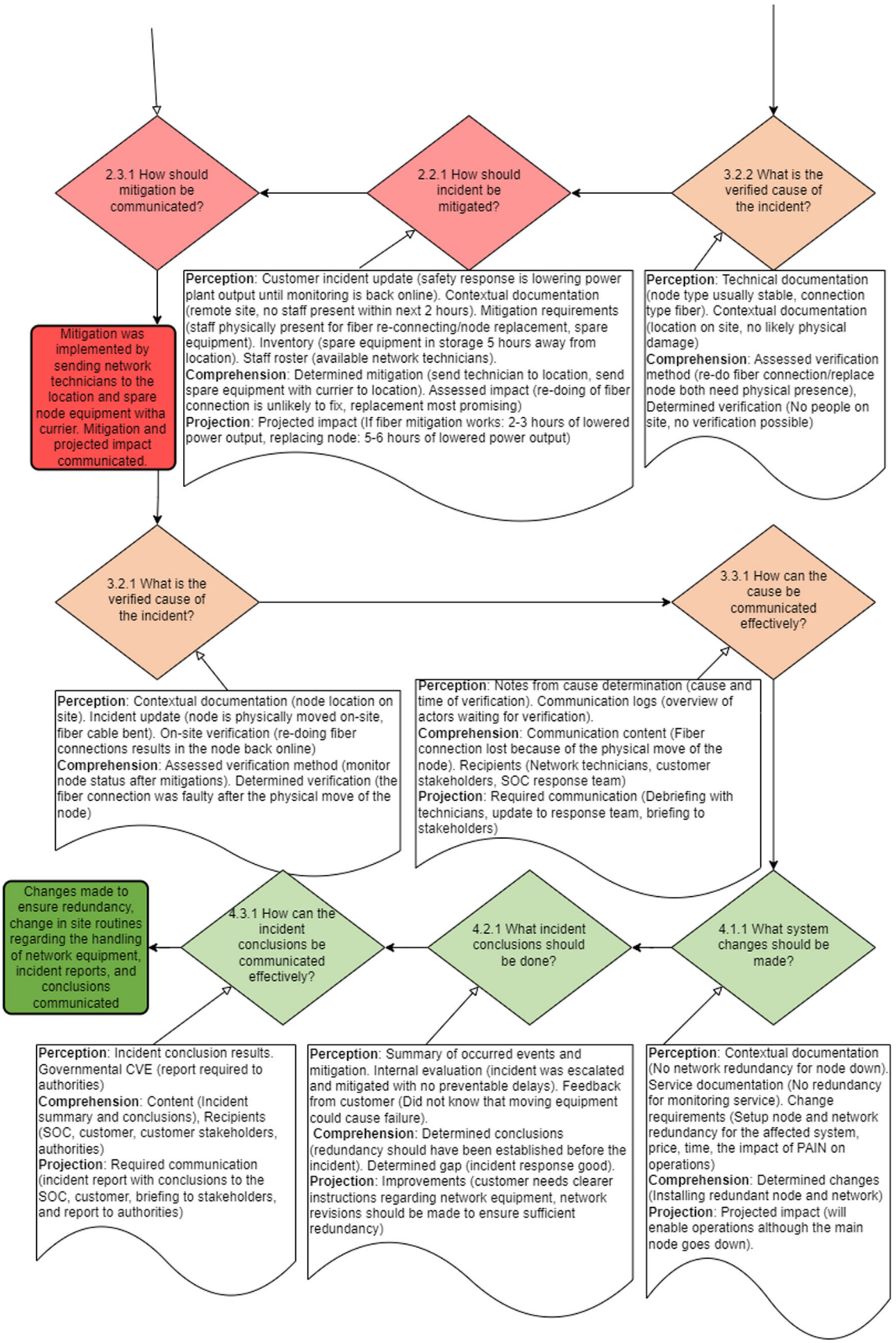

Fig. 5 continued

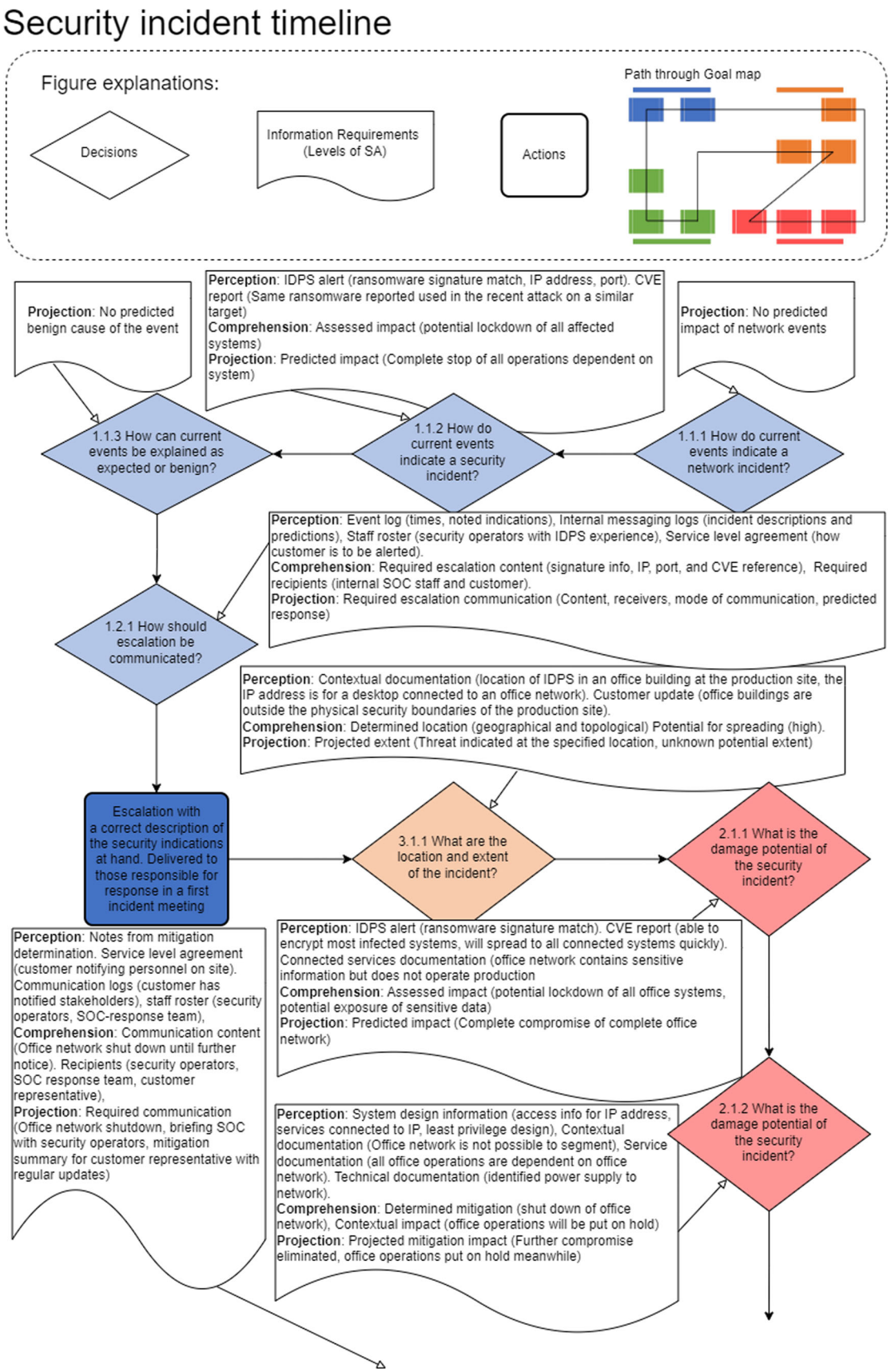

Fig. 6 Security incident timeline

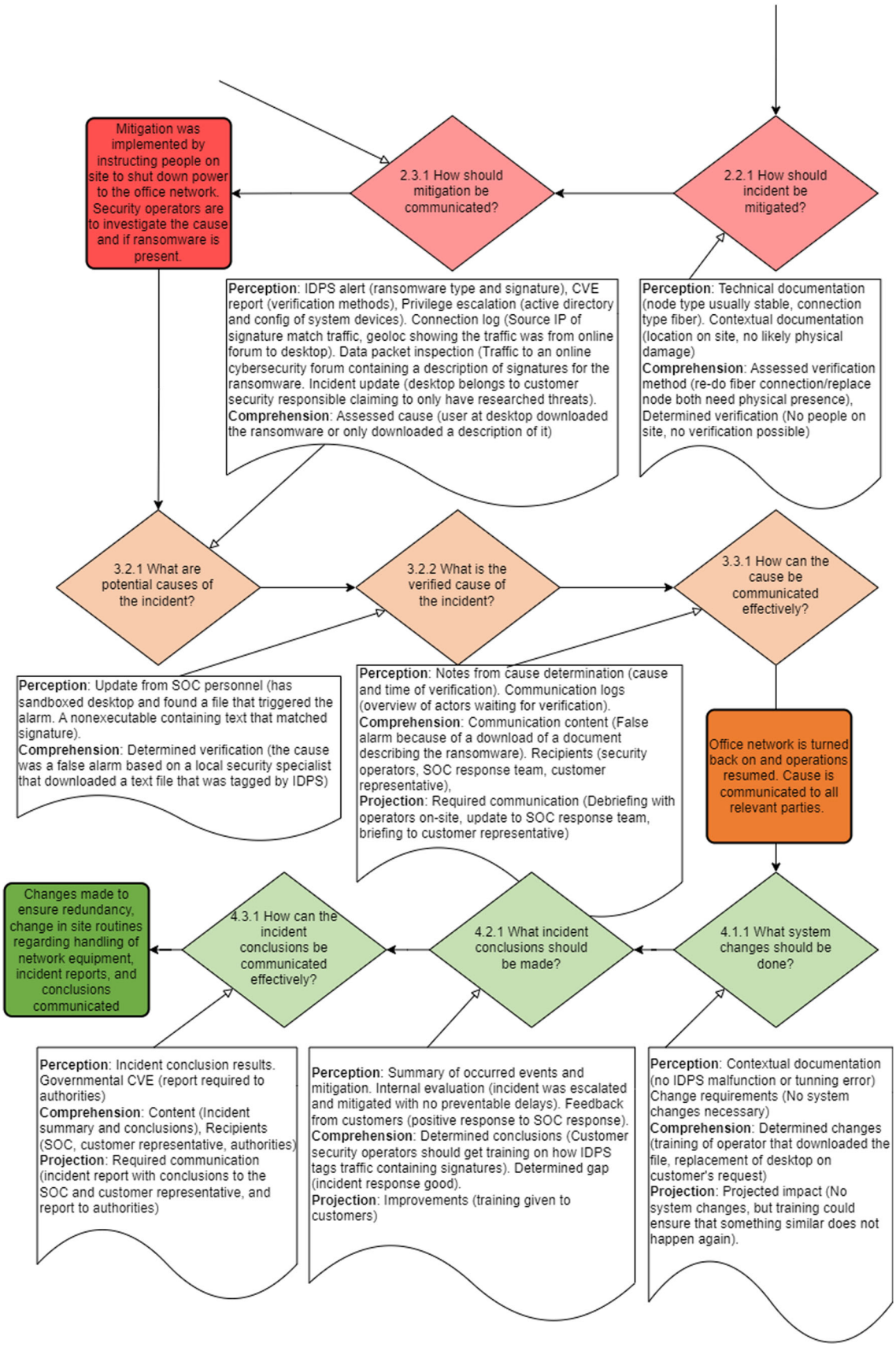

Fig. 6 continued

When analyzing these two timelines we see examples of reasons why goals are prioritized differently between incidents. We see that in a typical network incident, the partial assessment of the cause (marked in orange) is prioritized early in the incident response. In a typical security incident, the mitigation (marked in red) is prioritized earlier and before this assessment of the cause. There is a simple explanation for this prioritization: In many network incidents, mitigation is only possible after the cause is identified. In many security incidents, it is the other way around i.e., mitigation must be done early to maintain security attributes, but also because the investigation of cause only can be performed in a safe setting. The results are discussed further in Sect. 5.

5 Discussion

As explained in the introduction, a complete GDTA within SOCs for critical infrastructure has not been conducted before. It is therefore important to consider if this study shows that GDTAs are possible and relevant to conduct in this context. How one can understand the SA from the human operators' perspective is still an open question within the field of Cyber SA [11]. The results of this study show that the goal hierarchy of SOC incident response is possible to identify and that it is comparable to goal hierarchies identified in other fields [48–50]. This points toward asserting that SOC environments, such as the one studied here, are comparable to environments where SA research has proven useful before. Furthermore, this points towards the conclusion that such SOC environments are compatible with the established methods of assessing SA for human operators.

When we consider the goal hierarchy identified in this study as presented in Fig. 3, it becomes clear that the operational scope of the SOC investigated here might be larger than the typical internal SOC within an organization or SOC services for hire [51]. Other SOCs are often exclusively focused on the cyber security aspects [52]. The SOC investigated in this study was responsible for responding to both network incidents and security incidents. During the interviews, the respondents clearly stated that the combination of responsibility for both aspects was inherently necessary because the SOC served critical infrastructure. They argued that if these two aspects are not considered in tandem, one cannot respond adequately to incidents within critical infrastructure.

The main goal of the SOC was to "Keep systems operative and secure". This two-part goal of keeping the systems both operative and secure highlights the complicated negotiation of SOC operator goals. These two considerations were not always aligned. Keeping systems secure will sometimes demand reducing their operative status and vice versa. For SOCs in critical infrastructure, the availability of networks and services can in given circumstances be of the highest priority. One example is the operation of networks that control physical processes in critical infrastructures like power generation or manufacturing. The loss of availability can potentially be more severe than a security breach leading to the disclosure of sensitive information. The SOC operators must therefore constantly negotiate between keeping the networks operative and secure. Often one aspect is given priority first and then the other is prioritized at a later point in time. The tension between these aspects demonstrates the complexity and time-sensitive nature of SOC operators' tasks within critical infrastructure.

Another interesting aspect of the results was how flexibly the SA requirements were used. As explained in the results many SA requirements served several decisions, but in different ways. One example is the SA requirements of the callout *4 Contextual documentation of affected systems.* At an early stage of an incident, these SA requirements serve to gain an understanding of how severe the situation is. This information is crucial for being able to project the situation into the future in subgoal 2.1 specified by *Projected damage potential of network incident* and *Projected damage potential of security incident* as level 3 requirements. Meanwhile, when the secure operation of systems is re-established through changes in the system in subgoal 4.1, this documentation mostly serves SA perception regarding the status quo of the system. At this stage, it is the requirements in the callout *13 State-of-the-art descriptions* that are mostly necessary to project into the future.

The flexibility in the use of SA requirements points toward another feature of the SOC operator that is not common in other settings. Throughout the study, it became clear that SOC operators often tweak and self-develop the interface of their available information. Many of the operators were accomplished programmers and several of the tools they used to gain information were developed in-house or adapted based on need. One such example was how they used the Network Management System (NMS). During an observed incident caused by network overload, the operators quickly scripted a customized query that identified network patterns similar to the one at hand. Based on this information they projected the probable peak of the network load. Based on this projection they scripted a stepwise and timed denial of specified network services which would cause minimal disruption of availability. The available NMS tool was not developed with this in mind, but the operators extended the potential use of the tool to meet their SA requirements.

Many of the respondents argued that experience was the most important factor in handling the task complexity. They did confirm that the SA requirements at level 1 and 2 were necessary. But often when discussing level 3 SA they argued that experienced intuition was the most important requirement. One example was the great challenge of triaging the available information to recognize information of relevance.

The author's first assumption was that the benefit of experience was the ability to filter through a large amount of information in a short amount of time. Based on the respondents' answers this was not the case. They argued that experience helped in knowing where to look for the right information based on situational context and ignoring large parts of the total available information. This challenges the aspect of ideal SA requirements. In one way the ideal SA requirement across incidents is to have all possible information available, but in the specific case, one only wants the relevant information available. There is an interesting parallel finding in research on human intelligence and cognitive performance. The neuro efficiency theory shows that higher intelligence or cognitive performance is not associated with more activity in the brain, but rather less. This finding is valid across tasks where training improves performance [53].

When considering the results from the GDTA it is useful to compare the findings to previous research analyzing tasks in SOC settings. Previous TAs have investigated SA for operators handling network incidents [12] and security incidents [13, 43, 45, 46]. Their findings align with the findings of this study in many aspects. Two common findings are the importance of experience and collaboration between team members. The respondents in this study all worked in flexible teams assembled based on the need for expertise in each specific incident. According to the respondents, this maximized the positive effect of experience across different incidents. In other studies, these flexible roles seem less common in operation centers that exclusively focus on cyber security than those responsible for network incidents. If we take the goal map and timelines into account, we can start to reflect on why this is the case. In network incidents, the cause of the incident is of immediate and critical importance. The response involves a fast generation of cause hypotheses and consequently pruning of possible causes by targeted information gathering. This somewhat creative process can in many security incidents be done later without strict time constraints through digital forensics [54]. Such delay of cause verification will arguably also allow for more specialized operator roles. A strong argument against this specialist approach is pointed out by this study. One cannot always sacrifice availability for confidentiality or integrity in critical infrastructure.

The two timelines presented in Figs. 5 and 6 highlight the differences between network incidents and security incidents. The interviews revealed that in many incidents there were complex combinations of network and security aspects. One illustrative example was incidents related to firewalls for critical networks which had some aspects of IDPS as integrated functions. When the SOC experienced such components being unavailable, the situation had characteristics of both a network incident and a security incident. The balancing of availability against security aspects was often highly complex and challenging. A network-focused mitigation would be to circumvent the faulty firewall, but this would compromise the security enabled by the firewall. In such incidents, the operators had to consider the possibility of this device being taken down by an adversary with the goal of a response that would open an unprotected link into the network in question. The rise of Advanced Persistent Threats [55] including such targeted network attacks is yet another argument for combining the responsibilities of both network and security aspects for SOCs in critical infrastructure. Recent research has argued that such integration of network and security operations centers is beneficial [52].

In an earlier review of SA research in SOCs, it is shown that there is some theoretical mismatch between the goals of the research and its theoretical underpinnings. Much of the existing research is aimed at automating SA processes in SOCs while the referenced theoretical framework of Endsley disagrees with this approach [9]. The additional analysis of SA processes performed in this study, resulting in the goal map and timelines, may be used as a basis for investigating the compatibility of the different theoretical frameworks for SA within this context. Furthermore, the goal map and the timelines help the understanding of what processes might match different theories and operationalizations of SA in SOCs. A complete analysis of the compatibility of different models of SA with different parts and paths through the goal map is outside the scope of this article. Still, a preliminary reflection regarding such an analysis is made here.

1. *Monitor, detect, and escalate incidents* is marked in blue in Figs. 4, 5 and 6. One can identify that many of these SA processes may be good candidates for automation. It is often the information systems themselves that present the operator with potential incidents, and the consideration of escalation is to a large degree rule-based. When considering theoretical models of SA, the dependence on alerts from systems during this first stage of the incident response could indicate that the systemic perspective of Distributed SA would be a good match [19]. This perspective is also well aligned with the aim of developing more autonomous systems. The identification of potential security incidents is often done by systems like IDPSs which are inherently prone to a large degree of false positives. A rule-based automation of escalation therefore requires the integration of the information in the callouts of *4 Contextual documentation of affected systems* and *5 Connected services documentation.* One could imagine an effective system based on Artificial Intelligence (AI) that would serve such a function. With the current technology [56] one would need a large set of relevant training data. Such a dataset must connect alerts from existing systems like IDPSs with contextual

documentation and include verified escalation interpretations. The lack of availability of such datasets, especially within critical infrastructure, might prove a significant barrier against establishing such AI systems. There is one notable exception to the match with a systemic approach to SA regarding the decision *1.2.1 How should escalation be communicated?* This decision would arguably be better approached with the Shared SA perspective at the group level [9] because it tries to achieve a common understanding of the specifics of the incident for the involved parties.

2. *Mitigate incidents* is marked in red in Figs. 4, 5 and 6. There seems to be a need for several SA models to explain the processes. *2.1.1 What is the damage potential of the network incident?* and *2.1.2 What is the damage potential of the security incident?* can partially be understood through Distributed SA [19]. The level 2 requirements of *Determined technical impact of network incident* and *Determined technical impact of security incident* would arguably be possible to automate because they mostly rely on the synthesis of information already present in the technical systems. *Determined contextual impact of network incident, Determined impact of external factors,* and *Determined contextual impact of security incident* require much more human involvement. Here the shared SA model is not beneficial because different operators and stakeholders understand different aspects of the contextual damage potential. One can therefore argue that an aggregate approach of individual SA through Team SA would be most fitting [15]. The same argument can be made for the two decisions under *2.2 Determine mitigation to minimize damage.* This subgoal also involves negotiation between stakeholders regarding the positive and negative consequences of the mitigations themselves. Such negotiations demand the consideration of conflicting viewpoints which indicate Team SA as the right approach. *2.3.1 How should mitigation be communicated?* would benefit from the Shared SA perspective [15] following the same logic as explained regarding decision *1.2.1.*
3. *Determine cause of incident* is marked in orange in Figs. 4, 5 and 6. This process also includes a variety of SA mechanisms best explained by different SA models. *3.1 Localize incident* could be automated to a large degree and thus benefit from the Distributed SA model [19]. *3.2.1 What are potential causes of the incident?* is a creative collaborative effort best understood through the Team SA model [15]. Within decision *3.2.2 What is the verified cause of the incident?,* the level 2 SA requirement of *Assessed verification method of incident cause* entails the goal of a common understanding of how to verify the cause which points towards the Shared SA model [15]. *Determined verification of cause* on the other hand is in the interviews explained as processes performed individually through prioritized delegation. Here the classic individual SA model of Endsley [18] would be most fitting. *3.3.1 How can the cause be communicated effectively?* suggests the Shared SA model [15].
4. *Re-establish secure system operation* marked in green in Figs. 4, 5 and 6, would probably prove difficult to automate. Within this part of the goal map, the Shared SA model seems most appropriate maybe except *4.1.1 What system changes should be done?* which could benefit from the more diverse SA approach of Team SA [15].

The reflections regarding the differentiated use of models for understanding SA processes in SOCs should be investigated further. Such an investigation should include measurements of SA within the context of SOCs. This has until now proven difficult [11], but as this study provides the necessary in-depth understanding of SA processes in SOCs, such research will now be possible to conduct. In further research, one could perform SA measurements of different parts of the goal map while emphasizing the different approaches of the SA models. If this research shows that different processes of the goal map benefit measurably by the different SA models this can lead to improved performance through both automation and human operator performance. This would also form the basis for a synthesis of SA approaches in SOC environments and contribute to bridging the knowledge gap of Cyber SA [11]. If such further research is successful, it can ultimately contribute to the synthesis of opposing SA theories in general [20].

6 Conclusions

This study is the first to conduct a GDTA in SOCs for critical infrastructure. This was done to gain an in-depth understanding of the SA processes in the SOC throughout incidents. Following the prescribed methods, the study completed a GDTA by conducting a targeted set of unstructured and semi-structured interviews as well as an extensive review of documents. In addition, the GDTA was aided by in situ observation of the work within the SOC. This was further complemented by an analysis of different types of incidents and how they resulted in different prioritizations of goals and decisions during the incidents. Different pathways through the goal hierarchy were identified based on the review of 34 reports of previously escalated incidents and were validated alongside the GDTA.

The results of the GDTA showed that the goal hierarchy consisted of 4 major goals and 11 subgoals. The 11 subgoals consisted of 15 different decisions that had a total of 136 unique ideal SA requirements related to them. A categorization of the 89 level 1 SA requirements was also conducted

based on what types of information they contained like *logged information on systems/operations, information from sensor/analytical technology*, and *description of routines or requirements.* All SA requirements were categorized regarding which level of SA they served. A complete overview of the ideal SA requirements for each of the decisions in the goal hierarchy was presented. This gives a complete overview of the SA requirements relevant to incident response in a SOC for critical infrastructure.

It became clear throughout the study that the SA processes during the handling of incidents are complex and highly dependent on context. Therefore, the GDTA was complemented by a goal map showing different identified paths through the goal hierarchy and two exemplified types of incidents. Two main types of incidents were identified, namely network incidents and security incidents. These had different patterns of moving through the goal hierarchy and had somewhat different SA requirements associated with them. The additional analysis gives an even more in-depth understanding of SA mechanisms within SOCs for critical infrastructure.

The main contribution of this study is the conducted and presented GDTA. This is a unique contribution to closing the knowledge gap regarding Cyber SA [5] and enabling the direct measurement of SA in SOC environments. Moreover, the goal map and timelines provide a foundation for further research into how different SA processes might best be understood by different SA models. This study provides a discussion of how some of the SA processes may be automated, and which SA processes might best be understood and facilitated by different existing SA theories and models. This shows the potential of explaining SOC incident response through a synthesis of different SA models. Different models can explain SA mechanisms in different parts of the goal map of SOCs for critical infrastructure. Such synthesis of SA models could focus research regarding what processes to automate, and what processes to optimize for human performance. This study can thus be a steppingstone in a coordinated effort to improve both human performance and automated processes within SOCs.

Acknowledgements I would like to thank my supervisor, Prof. Sokratis Katsikas for valuable guidance, encouragement, and advice throughout this research.

Author Contributions The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital). This work was supported by the Research Council of Norway (Norges Forskningsråd) under Project number 333900 "Situation awareness in virtual security operations centers" and Project number 310105 "Norwegian Centre for Cyber Security in Critical Sectors (NORCICS)".

Data Availability The data that support the findings of this study are not openly available due to reasons of sensitivity and Norwegian legislation regarding critical infrastructure. Data will be made available from the corresponding author upon reasonable and lawful request.

Declarations

Conflict of interest The author was employed in a research position at the participating SOC at the time of this study. See Sect. 3.4 Methodological limitations for more details. The author declares that he had no other known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent All respondents to interviews in this study gave informed consent. This article does not contain any other studies with human participants or animals performed by the author.

References

1. EuropeanUnion: Council Directive 2008/114/EC of 8 December 2008–on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Off. J. Eur. Union **345**, 75–82 (2008)
2. Kayan, H., et al.: Cybersecurity of industrial cyber-physical systems: a review. ACM Computing Surveys (CSUR) **54**(11s), 1–35 (2022). https://doi.org/10.1145/3510410
3. Chowdhury, N., Gkioulos, V.: Cyber security training for critical infrastructure protection: a literature review. Comput. Sci. Rev. **40**, 100361 (2021). https://doi.org/10.1016/j.cosrev.2021.100361
4. Evans, M., et al.: Human behaviour as an aspect of cybersecurity assurance. Secur. Commun. Netw. **9**(17), 4667–4679 (2016). https://doi.org/10.1002/sec.1657
5. Endsley, M.R.: A systematic review and meta-analysis of direct objective measures of situation awareness: a comparison of SAGAT and SPAM. Hum. Factors **63**(1), 124–150 (2021). https://doi.org/10.1177/0018720819875376
6. Panteli, M., et al.: Assessing the impact of insufficient situation awareness on power system operation. IEEE Trans. Power Syst. **28**(3), 2967–2977 (2013). https://doi.org/10.1109/TPWRS.2013.2240705
7. Gardner, A.K., Kosemund, M., Martinez, J.: Examining the feasibility and predictive validity of the SAGAT tool to assess situation awareness among medical trainees. Simul. Healthc. **12**(1), 17–21 (2017). https://doi.org/10.1097/SIH.0000000000000181
8. Stanton, N.A., Chambers, P.R., Piggott, J.: Situational awareness and safety. Saf. Sci. **39**(3), 189–204 (2001). https://doi.org/10.1016/S0925-7535(01)00010-8
9. Ofte, H.J., Katsikas, S.: Understanding situation awareness in SOCs, a systematic literature review. Comput. Secur. (2022). https://doi.org/10.1016/j.cose.2022.103069

10. 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
11. Gutzwiller, R., Dykstra, J., Payne, B.: Gaps and opportunities in situational awareness for cybersecurity. Digit. Threat. Res. Pract. (2020). https://doi.org/10.1145/3384471
12. Gutzwiller, R.S., Hunt, S.M., Lange, D.S.: A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. In: 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016. https://doi.org/10.1109/COGSIMA.2016.7497780.
13. Rajivan, P., Cooke, N.: Impact of team collaboration on cybersecurity situational awareness, In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. p. 203–226.
14. Munsinger, B., Beebe, N., Richardson, T.: Virtual reality for improving cyber situational awareness in security operations centers. Comput. Secur. **132**, 103368 (2023). https://doi.org/10.1016/j.cose.2023.103368
15. Stanton, N.A., et al.: State-of-science: situation awareness in individuals, teams and systems. Ergonomics **60**(4), 449–466 (2017). https://doi.org/10.1080/00140139.2017.1278796
16. Endsley, M.R.: Designing for situation awareness: an approach to user-centered design. CRC Press, London (2016)
17. Endsley, M.R., Garland, D.J.: Theoretical underpinnings of situation awareness: a critical review. Situat. Aware. Anal. Meas. **1**(1), 3–21 (2000)
18. 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
19. Salmon, P.M., et al.: Distributed situation awareness: theory, measurement and application to teamwork. CRC Press, London (2017)
20. Endsley, M.R.: Situation awareness misconceptions and misunderstandings. J. Cognit. Eng. Decis. Mak. **9**(1), 4–32 (2015). https://doi.org/10.1177/1555343415572631
21. Jajodia, S., et al., *Cyber situational awareness*. 2009: Springer.
22. Tadda, G.P., Salerno, J.S.: Overview of cyber situation awareness. In: Cyber Situational Awareness, pp. 15–35. Springer, Berlin (2010)
23. Salmon, P.M., et al.: Measuring situation awareness in complex systems: comparison of measures study. Int. J. Ind. Ergon. **39**(3), 490–500 (2009). https://doi.org/10.1016/j.ergon.2008.10.010
24. Endsley, M.R.: Situation awareness global assessment technique (SAGAT). In: Proceedings of the IEEE 1988 National Aerospace and Electronics Conference. 1988. IEEE https://doi.org/10.1109/NAECON.1988.195097.
25. Skopik, F., et al.: From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. Int. J. Inf. Secur. **21**(6), 1323–1347 (2022). https://doi.org/10.1007/s10207-022-00613-7
26. Vielberth, M., et al.: Security operations center: a systematic study and open challenges. IEEE Access **8**, 227756–227779 (2020). https://doi.org/10.1109/ACCESS.2020.3045514
27. Katsantonis, M., et al.: Cyber range design framework for cyber security education and training. Int. J. Inf. Secur. (2023). https://doi.org/10.1007/s10207-023-00680-4
28. Giacobe, N.A.: A picture is worth a thousand alerts. In: Proceedings of the Human Factors and Ergonomics Society. 2013. https://doi.org/10.1177/1541931213571039.
29. Giacobe, N.A., et al.: Capturing human cognition in cyber-security simulations with NETS. In: IEEE ISI 2013—2013 IEEE International Conference on Intelligence and Security Informatics: Big Data, Emergent Threats, and Decision-Making in Security Informatics. 2013. https://doi.org/10.1109/ISI.2013.6578844.
30. Hoffman, R.R.: Protocols for cognitive task analysis. Florida Institute for Human and Machine Cognition Inc Pensacola FL. (2005)
31. Zhong, C., et al.: ARSCA: A computer tool for tracing the cognitive processes of cyber-attack analysis. In: 2015 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision, CogSIMA. 2015. https://doi.org/10.1109/COGSIMA.2015.7108193.
32. Mullins, R., Nargi, B., Fouse, A.: Understanding and enabling tactical situational awareness in a security operations center. In: Advances in Intelligent Systems and Computing. 2020. p. 75–82.
33. Le Blanc, K., et al.: Characterizing cyber tools for monitoring power grid systems: what information is available and who needs it? In: 2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC. 2017. https://doi.org/10.1109/SMC.2017.8123164.
34. Pahi, T., Leitner, M., Skopik, F.: Analysis and assessment of situational awareness models for national cyber security centers. In: ICISSP 2017—Proceedings of the 3rd International Conference on Information Systems Security and Privacy. 2017. https://doi.org/10.5220/0006149703340345.
35. Skopik, F.: The limitations of national cyber security sensor networks debunked: why the human factor matters, In: Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS). 2019. p. 405–412.
36. Kanstrén, T., Evesti, A.: A study on the state of practice in security situational awareness. In: 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). 2016. https://doi.org/10.1109/QRS-C.2016.14.
37. Eldardiry, O.M., Caldwell, B.S.: Improving information and task coordination in cyber security operation centers. In: IIE Annual Conference and Expo. 2015.
38. Smith, R., et al.: The agile incident response for industrial control systems (AIR4ICS) framework. Comput. Secur. **109**, 102398 (2021). https://doi.org/10.1016/j.cose.2021.102398
39. Ahrend, J.M., Jirotka, M., Jones, K.: On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. In: 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA. 2016. https://doi.org/10.1109/CyberSA.2016.7503279.
40. 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. https://doi.org/10.1109/ASONAM.2018.8508410.
41. Ahmad, A., et al.: How can organizations develop situation awareness for incident response: a case study of management practice. Comput. Secur. (2021). https://doi.org/10.1016/j.cose.2020.102122
42. Paterson, D.M.: Work Domain Analysis for network management revisited: Infrastructure, teams and situation awareness. In: 2014 IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA. 2014. https://doi.org/10.1109/CogSIMA.2014.6816548.
43. D'Amico, A., et al.: Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2005. SAGE Publications Sage CA: Los Angeles, CA https://doi.org/10.1177/154193120504900304.
44. Champion, M.A., et al.: Team-based cyber defense analysis. In: 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA. 2012. https://doi.org/10.1109/CogSIMA.2012.6188386.
45. Lif, P., Granåsen, M., Sommestad, T.: Development and validation of technique to measure cyber situation awareness. In: 2017 International Conference on Cyber Situational Awareness, Data

Analytics and Assessment (Cyber SA). 2017. IEEE https://doi.org/10.1109/CyberSA.2017.8073388.
46. Lif, P., Sommestad, T., Granasen, D.: Development and evaluation of information elements for simplified cyber-incident reports. In: 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). 2018. IEEE https://doi.org/10.1109/CyberSA.2018.8551402.
47. Endsley, M.R., E.S. Connors: Foundation and challenges. Cyber defense and situational awareness, 2014: p. 7–27 https://doi.org/10.1007/978-3-319-11391-3_2.
48. Sharma, A., Nazir, S., Ernstsen, J.: Situation awareness information requirements for maritime navigation: a goal directed task analysis. Saf. Sci. **120**, 745–752 (2019). https://doi.org/10.1016/j.ssci.2019.08.016
49. Connors, E.S., M.R. Endsley, and L. Jones.: *Situation awareness in the power transmission and distribution industry*. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 2007. SAGE Publications Sage CA: Los Angeles, CA https://doi.org/10.1177/154193120705100415.
50. Rummukainen, L., et al.:*Situation awareness requirements for a critical infrastructure monitoring operator*. In: *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*. 2015. IEEE https://doi.org/10.1109/THS.2015.7225326.
51. Shah, A., Ganesan, R., Jajodia, S.: A methodology for ensuring fair allocation of CSOC effort for alert investigation. Int. J. Inf. Secur. **18**(2), 199–218 (2019). https://doi.org/10.1007/s10207-018-0407-3
52. Shahjee, D., Ware, N.: Integrated network and security operation center: a systematic analysis. IEEE Access **10**, 27881–27898 (2022). https://doi.org/10.1109/ACCESS.2022.3157738
53. Neubauer, A.C., Fink, A.: Intelligence and neural efficiency. Neurosci. Biobehav. Rev. **33**(7), 1004–1023 (2009). https://doi.org/10.1016/j.neubiorev.2009.04.001
54. Castelo Gómez, J.M., et al.: A context-centered methodology for IoT forensic investigations. Int. J. Inf. Secur. **20**, 647–673 (2021). https://doi.org/10.1007/s10207-020-00523-6
55. González-Manzano, L., et al.: A technical characterization of APTs by leveraging public resources. Int. J. Inf. Secur. (2023). https://doi.org/10.1007/s10207-023-00706-x
56. Gupta, M., et al.: From chatgpt to threatgpt: Impact of generative AI in cybersecurity and privacy. IEEE Access (2023). https://doi.org/10.1109/ACCESS.2023.3300381