Development and validation of technique to measure cyber situation awareness

Patrik Lif, Magdalena Granåsen, Teodor Sommestad
Swedish Defence Research Agency
Department of C4ISR
Olaus Magnus väg 42, Linköping, Sweden
{patrik.lif, magdalena.granasen, teodor.sommestad}@foi.se

***Abstract*—Within the cyber security domain, specifically within the field of computer network defence, professional log analysts are employed to monitor organizations' networks in order to detect malicious activity and suggest necessary measures. A log analyst needs to *perceive* malicious activity, *comprehend* the impact and type of threat, and *predict* future consequences. In other words, they need good cyber situation awareness. Research about cyber situation awareness measurement is limited, especially when it comes to practical examples. The current paper describes the development and validation of a freeze-probe technique aiming to measure log analysts' situation awareness. Goal directed task analysis and hierarchical task analysis were used to develop a first version of a measurement technique. The measurement technique had the form of two questionnaires designed for the two different roles in log analysis. The validation was conducted in a realistic setting during an exercise involving five professionals, where the questionnaires were well received by the log analysts. Only smaller adjustments were suggested. The results suggest that the technique can be used to evaluate cyber situation awareness for log analysts, as well as function as a tool in log analysts' daily work to keep track of incidents.**

Keywords— cyber situation awareness; log analysis; cyber network defence; situation awareness; SAGAT

I. INTRODUCTION

The professional domain of cyber security is diverse and encompasses several different work roles. The American National Cybersecurity workforce framework lists 928 tasks, 359 skills and 614 different knowledge aspects associated with the cyber security profession [1]. This paper focuses on the specialist field called Computer Network Defense Analysis (CND analysis). According to the American National Cybersecurity workforce framework, CND analysis encompasses 25 tasks, where several deal with identifying malicious activity based on system logs. CND analysis is an active research field in which over a thousand new articles are presented annually in scientific forums. The vast majority of these publications focus on technical solutions and only a small portion involve the people that are supposed to use the technical solutions. In the current paper, the specialists working with CND analysis are called log analysts. A log analyst's main tasks are to monitor, analyze and decide on appropriate measures for the detection of threats and attacks [2]–[4].

Detection and management of threats demand a good understanding for the system that is monitored, including knowledge of system vulnerabilities, the capacity of available tools (sensors) for detecting anomalies and how to interpret the detected anomalies [4]–[6]. In other words, log analysts need a good situation awareness (SA). Poor situation awareness may lead to that antagonists are allowed to exploit an organization's information system vulnerabilities unimpeded, with severe consequences such as process disturbances, information being leaked or information being manipulated.

Endsley [7] defines situation awareness 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."*. Thus, situation awareness consists of three levels; perception, comprehension and projection. For a log analyst, that can for instance include to *perceive* malicious activity, *comprehend* the impact and type of threat, and *predict* future consequences [8].

Situation awareness measurement methods have been used and evaluated in various domains [9]–[11]. However, it remains to investigate which methods that are suitable for measuring situation awareness within cyber security in general, and log analysis tasks in particular. The purpose of the current study was to develop and evaluate a technique to measure cyber situation awareness (CSA) for log analysts. The paper presents results from an empirical validation of the technique made in a realistic setting involving professional log analysts. The results suggests that the technique can be used to evaluate CSA for log analysts, as well as function as a tool in log analysts' daily work to keep track of incidents.

In this paper, *related work* describes research about situation awareness measurement methods and how these methods can be used to measure cyber situation awareness. Then, with starting point from other research and conducted cognitive- and goal directed task analysis, we present a *freeze-probe technique* that was developed to measure situation awareness for log analysts. This is followed by an initial *validation* of the developed questionnaires in a realistic setting with experts, resulting in a revised technique to measure log analysts' situation awareness. Finally, conclusions and future work are described.

II. Related work

There are numerous situation awareness measurement methods. These are applicable to different tasks and domains. The sections below give an overview of situation awareness measures that been applied in various domains and detail how these have been applied to cyber situation awareness.

A. Situation awareness measurement

Salmon et al. [12] divide situation awareness measurement into seven categories: 1) SA requirement analysis, 2) freeze probe techniques, 3) real-time probe techniques, 4) self-rating techniques, 5) observer-rating techniques, 6) performance measures, and 7) process indices (e.g. eye tracker).

1) SA requirement analysis

An SA requirement analysis [9] is the first step in any assessment of situation awareness. It is conducted in order to determine the elements that comprise operators' situation awareness in a specific task and is a necessary activity when developing a questionnaire (e.g. SAGAT) [13]. SA requirement analysis usually includes interviews with subject matter experts (SME's), goal directed task analysis and questionnaires [14].

2) Freeze probe techniques

Freeze probe techniques ask participants queries regarding the current situation in a simulation or exercise, usually with operator displays disabled during the "freeze". The primary advantage associated with these techniques is their direct nature; the primary disadvantage is the intrusion on the task that the operators perform caused by the disruption. The most popular freeze probe technique is Situation Awareness Global Assessment Technique (SAGAT) [9], [15], [16]. SAGAT has been applied in a number of areas, including military aviation [7], air traffic control [10], military operations [17], driving [18] and the process industry [19].

3) Real-time probe techniques

Real-time probe techniques use queries without freezing the work situation. Queries are developed by subject matter experts and both query response content and response time are used as situation awareness measures. The real-time probes are argued to be non-intrusive, but the queries may direct participants' attention towards what is asked for in the queries and thereby bias the data. One example of real-time probe technique is the situation present assessment method (SPAM) [20] that was developed for air traffic controllers.

4) Self-rating techniques

Self-rating techniques assess the participants' subjective situation awareness through a rating scale, and are typically administered post-trial. They are easy to administer, but have received critique, e.g. concerning poor recall post-trial, lack of sensitivity, and that participants may misunderstand the situation and believe they have good situation awareness when in fact they have poor situational awareness. The situation awareness rating technique (SART) [16], [21] is one of the most well-known self-rating techniques. It is administered post-trial and consists of ten dimensions which are ranked on a seven-point rating scale. There is also a condensed version, 3D-SART, which includes only three dimensions.

5) Observer rating techniques

Observer rating techniques are most commonly used in the field, and usually involve subject-matter experts as observers. The main advantage is that these techniques are non-intrusive and that they can be used in a non-simulated setting. However, subject-matter experts' ability to accurately rate participants' situation awareness is disputed. The situation awareness behavioral rating scale (SABARS) is one example of an observer rating technique that has been used for infantry personnel [17]. This technique includes 28 observable behaviors, rated on a five point rating scale.

6) Performance measures

Performance measures can be used as an indirect measure for situation awareness. These measures vary with task and situation, but can typically be hits, misses, false alarms, correct rejection, and response time. Performance measures are often easy to administer and non-intrusive, but the relation between performance and situation awareness is not always clear.

7) Process indices

One example of a process index used for measuring situation awareness is eye-tracking [12], which is an objective measure that records information regarding where operators look. However, the recorded data only contain information about what they look at, not what they perceive. Furthermore, eye tracking works fairly well in the laboratory but is often problematic in real settings because of interference from different light sources. Furthermore it is often problematic to install technical equipment such as an eye-tracker in airplanes and vehicles.

B. Cyber situation awareness

There is extensive research about situation awareness in the cyber security domain. However, cyber situation awareness (CSA) is loosely defined and the literature describing how CSA should be measured as well as which elements comprise CSA is limited [22]. A notable difference is that much of the research on cybersecurity and situational awareness is technology-oriented. Gutzwiller, Hunt, & Lange [23] therefore argue that the term CSA is associated with data fusion [24], [25] and propose to use the term cyber-cognitive situation awareness (CCSA) for CSA focusing on human activities. Although this is an interesting viewpoint, the traditional view is that the cognitive aspect is already implicit in situation awareness, and therefore the concept CSA is used as a denomination for log analysts' situation awareness in this paper.

Research about what should be visualized to log analysts [26], and previous task analyzes in the field [27] give some insight in what information that is important to obtain good CSA. Dressler et al. [27] argue that a system must utilize six classes of information to establish operationally relevant situation awareness. The six classes are: threat environment, anomalous activity, vulnerabilities, key terrain, operational readiness, and ongoing operations. These six classes give a good overall understanding of CSA but need to be further defined and analyzed. Shiravi et al. [26] conducted a review of network security visualization. They provide six potential data sources:

network traces, network events, application logs, security events, as well as context related to network activity, users and assets. However, these data sources encompass only a limited portion of CSA since they focus solely on anomalous activities, and not the other five aspects in Dressler's classification.

Although the number of scientific publications regarding human factors and situation awareness in the cyber domain [28]–[35] have increased, few have presented research in which an actual CSA measurement technique has been used [36] and evaluated in a realistic situation with users from the targeted domain. One of few examples is presented by Giacobe [37], [38] who used a cyber-SAGAT questionnaire to evaluate one visual and one text-based interface. Giacobe [37] used SAGAT to evaluate the participants' understanding of what specific IP-addresses represent (e.g. workstation, internal server, external web server or external host), what is a reasonable value for a vulnerability scan, and if specific alerts should be reported. Huang [8] used performance measures and SAGAT to provide post-training feedback to trainees, but also to receive feedback from trainees during system evaluations. Evangelopoulou and Johnson [39] applied SART and SAGAT in a cyber security study. They found the measures difficult to use, and stated that there is room for improvements. Malviya, Fink, and Landon [36] used the observer based probe technique SPAM in a study of cyber security collaborative work. They found a weak correlation between their situation awareness measure and performance. Apart from these studies, we have not found any publications where standardized situation awareness methods are used for assessing CSA. These studies clearly show that there is still much work required in order to develop a CSA-method to measure participants' situation awareness in a valid and reliable manner. The questions in the abovementioned studies are reasonable and can therefore be used as a starting point to develop and evaluate a valid freeze-probe technique to measure CSA.

III. Development of Technique to Meausure Cyber Situation Awareness for Log Analysts

The freeze probe technique was preferred for measuring log analytics' situation awareness since the measure will mainly be used in a cyber range environment, allowing freezing of simulations, and since SAGAT is the most established of the freeze probe techniques we used that as a starting point. Development of SAGAT requires careful work with subject matter experts to ensure that the queries are relevant for the operators [9]. The questions should be phrased as similar as possible to how the log analysts think about the information, and not require extra transformation of the content. Development of SAGAT should according to praxis [9] contain detailed information from operators and experts to identify which aspects are most important. This can be done through the use of task analysis.

A. Literature review

A literature review was conducted in order to obtain an understanding for the field of log analysis [28], [39]–[41] and possible reuse or experience of existing CSA measurement techniques [36], [37], [42]. Based on previous research on cyber security, situation awareness and the insufficiency regarding methods to measure CSA we started to develop a technique to measure log analytics' cyber situation awareness.

B. Goal directed task analysis

The next step was a goal-directed task analysis [13]. This was conducted as two individual 1.5-hour interviews with professional cyber security log analysts. Since it was identified that a log analyst essentially works in two different roles, each interview was divided into two parts, discussing first the role as *scout*, and then the role as *analyst*.

C. Hierarchical task analysis

The hierarchical task analysis was conducted by an expert within cyber security while observing an exercise with professional log analytics' working in a realistic setting. This resulted in an overall structure of activities conducted by the team leader, scouts and analysts, as illustrated in Fig. 2. The figure describes the participants' work in general terms, which means that the detailed information have been excluded.

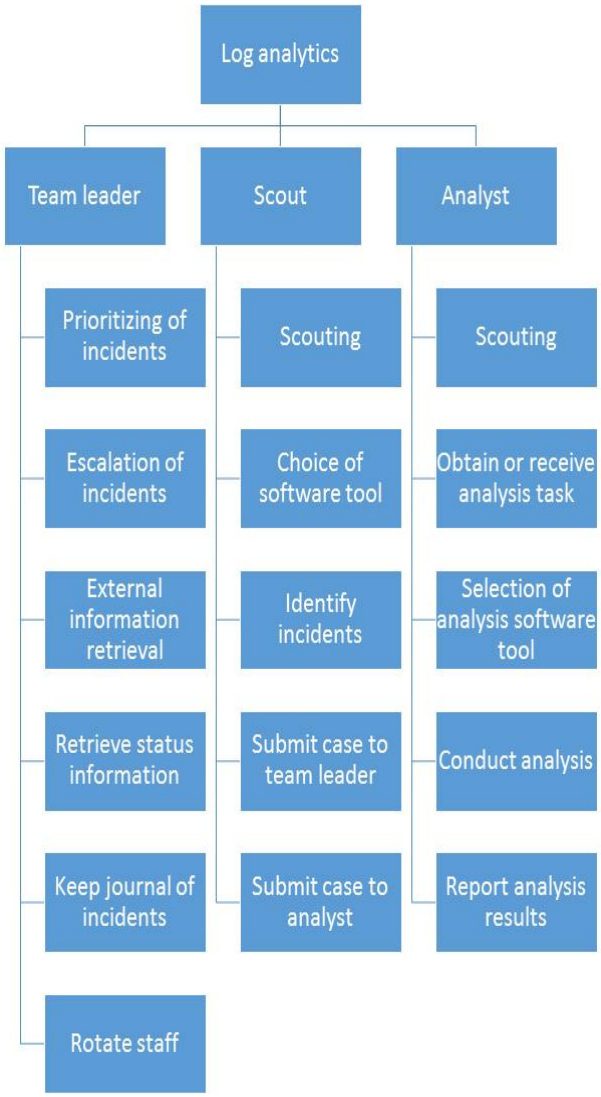


Fig. 2. Hierarchical task analysis for team leader, scout and analyst.

D. Questionnaire development

The information retrieved during the goal-directed task analysis and the hierarchical task analysis was used for the development of two questionnaires; one for scouts and one for analysts. The questionnaires were designed to measure CSA in relation to the different levels of SA: perceive, comprehend and predict future consequences. The questions for the two roles partly overlapped. CSA-measures in other research, [8], [36]–[39] include questions about specific IP addresses, e.g. if the traffic between two specific IP-addresses are as expected, and expected result of a vulnerability scan. These questions are reasonable but the conducted interviews as well as the feedback received from the validation of our questionnaires showed that this is not enough. It is also important to categorize the attacks according to a predetermined taxonomy, to assess where in the attack chain attacks are, and to have a good situation awareness of the network and where the sensors are located. In addition, we included queries about the purpose of the attack, how severe the attack is, what vulnerabilities that were exploited, and how fast countermeasures must be taken. These kinds of queries are not included in earlier SAGAT-questionnaires within cyber security. Furthermore, earlier suggestions to measure CSA do not adapt the questionnaires to different role descriptions. Ratings scales are commonly used within human factors [43], usually with five- or seven-point scales [44]. We selected a seven-point scale because it was assessed that a five-point-scale would not provide sufficient sensitivity. The rating scale was used to measure participants' perception of e.g. how critical the system under attack was or how urgent it was to take action. Low ratings indicated that the system under attack was considered not at all critical (not urgent to take action) and high values indicated that the system was very critical (very urgent to take action).

The questionnaire we developed for scouts contained eleven items. The scouts were first asked to indicate sensors in a network map. Then they were asked to assess the relationship between actual incidents and false positives, how many incidents that had occurred since the last freeze, and how many of these that had been reported to the analysts. For a particular incident (chosen by themselves in this exercise), the scouts were asked to estimate the start and end time, categorize the type of incident, assess the seriousness and urgency for action, assess the reason behind the attack, what the antagonist wanted to achieve, and whether the attack was manually or automatically generated.

The questionnaire for analysts contained ten items, all relating to a specific incident. First, they were asked to draw a graph of what happened in the network during the attack, including start and end time, sources and targets. Thereafter they were asked to assess their confidence of their analysis, assess the type of incident, which vulnerability was exploited, what the antagonist wanted to achieve, the seriousness of the incident, whether the attack was directed to a specific target, whether it was manually or automatically generated, what actions should be taken and the urgency for these actions.

IV. Validation

The two developed questionnaires for scouts and analysts were validated during an exercise conducted in a realistic simulated environment. Participants were five professional log analysts.

A. Environment

The exercise was performed in a virtual environment called CRATE [45], located at the Swedish Defence Research Agency. The environment contained a number of web servers, mail servers, file servers, network equipment and more than 200 office computers with the Windows 7 operating system and typical office applications. Typical office user activities, such as e-mail traffic, visiting websites and opening files, were simulated with scripts. The simulated user activities occurred with the same frequency as users of real office computers at a company with about 150 employees. There were also machines located outside of the network perimeter of the monitored systems. These external machines simulated the internet during exercise.

The attacks were carried out with the in-house developed tool Scanning, Vulnerabilities, Exploits and Detection (SVED) [46] and consisted of network scans from inside and outside the network, password guesses on network services, infected USB sticks, denial of service attacks, and email with malicious attachments. The attacks were carried out so that log analysts' mental workload would be high throughout the day.

Participants had been provided with a description of the environment before the exercise. Each of the five participants was equipped with two laptops with 15-inch screens. The participants monitored the network traffic with sensors at twelve positions in the network. For analysis they had access to the log analysis tools Wireshark [47], ELK [48] and Snort [49]. System events such as Windows Event Log [50] were collected in a central system and transferred to the analysis tool ArcSight [51].

B. Participants and tasks

Five professional log analysts participated in the exercise, all males. One participant was selected as team leader, who in his turn assigned the remaining four participants job roles, two as scouts and two as analysts. The team leader had the mandate to change the roles over time, depending on the number of attacks, the severity of the threats, and which tasks that required extra attention. When the team leader discovered or was briefed by the others of anomalies or threats that were considered priority, additional resources could be put on analyzing data (Fig. 1).

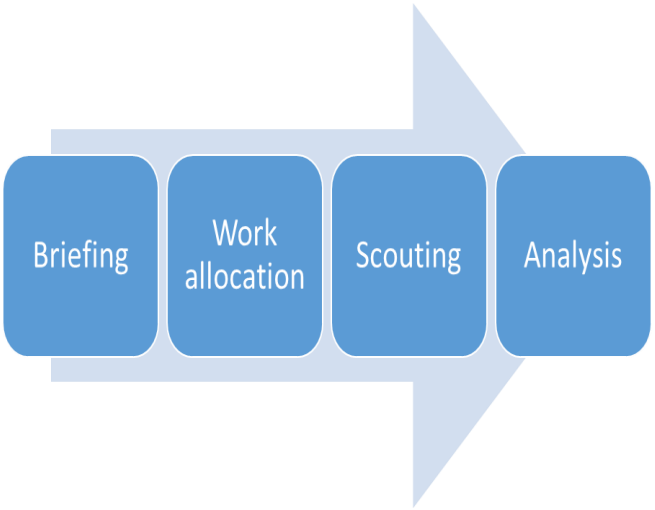


Fig. 1. Validation procedure: briefing from manager, work allocation from team leader, and log analytic work with scouting and analysis.

C. Data collection

The questionnaires were administered during four 'freezes'. During each freeze, the four participants working as scouts and analysts individually answered the queries responding to their current role. After the exercise, an after action review was conducted, discussing and evaluating the content of the two questionnaires. The participants were further asked to write down improvement suggestions of the two questionnaires after the exercise. Additionally, they had the possibility to provide individual comments to the experimenter at the end of the completed validation and during after action review. Since the focus of this paper is to validate the CSA technique, only the methodological results from the validation is included in this paper.

D. Validation results

All participants were positive to the questionnaires and perceived that the queries covered the essential aspects of what is needed to obtain good situation awareness in log analysis. That is, the questionnaires' had good face validity. The participants suggested minor changes to further improve the questionnaires. One proposal was to estimate each incident according to the "cyber kill chain" [52], [53], i.e., the stage the attack was in. Furthermore, it was suggested that the taxonomy used to classify incidents should be changed to better suit the participants' environment.

The professional log analysts considered that selected parts of the questionnaires after adjustment according to proposed suggestions may be useful as an instrument to help keeping track of identified events during their daily work. That is, the questionnaire is could be used as a type of template for logging events. Details about how this can be digitalized and implemented in log analysts' daily work remain to be investigated.

E. Further development of CSA measurement tool

Based on the validation results including analysis of verbal and written comments from the experts, the questionnaires for scouts (Fig. 3) and analysts (Fig. 4) were revised. The most important changes were the inclusion of a kill chain (Fig. 3 question 11 and fig. 4 question 5), and a changed taxonomy for defining type of attack (question 9 for scouts and 3 for analysts). It is likely that the taxonomy needs to be adapted to the work situation and the type of system being monitored. The revised questionnaires use a taxonomy from Hansman & Hunt [54] with four dimensions for describing attacks. This choice has not yet been validated.

Questionnaire for scouts

1. Draw where the sensors are (use separate network map).
2. What proportion of the incidents are false positive?
3. What proportion of the incidents does the sensors detect?
4. How many incidents have you reported to analysts (since last game stop)?
5. How many incidents have occurred since the last game stop?
6. What general threat level are we at (draw in the graph below)?

Incident 1

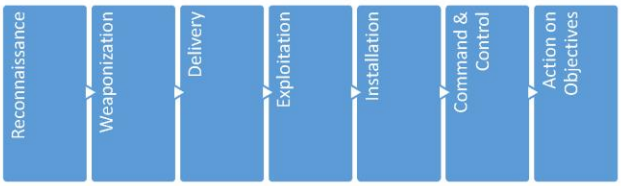
7. When did the incident take place (start time & end time)?
8. How confident are you that there is a real attack?

Not at all confident ① ② ③ ④ ⑤ ⑥ ⑦ Very confident

9. What kind of attack was it (use separate taxonomy)?
10. How confident are you about kind of attack (referring to question 9)?

Not at all confident ① ② ③ ④ ⑤ ⑥ ⑦ Very confident

11. Where in the kill chain is the current attack (use the figure bellow)?



12. What was the reason behind the attack?
13. Which system or systems are under attack?
14. How critical is the system?

Not at all critical ① ② ③ ④ ⑤ ⑥ ⑦ Very critical

15. How severe was the attack?

Not at all severe ① ② ③ ④ ⑤ ⑥ ⑦ Very severe

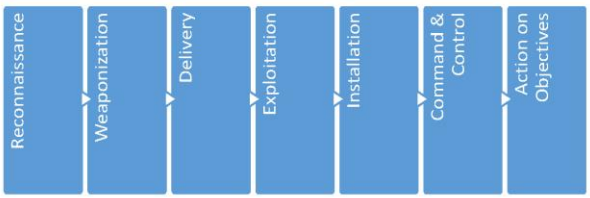
16. How urgent is it that the analyst start further investigations?

Not at all urgent ① ② ③ ④ ⑤ ⑥ ⑦ Very urgent

Fig. 3. Questionnaire to measure cyber situation awareness for scouts.

Questionnaire for analysts

1. Draw a network description of attack 1 and include the following information (use separate template): sources and targets (e.g. IP-addresses, ports, MAC-addresses, hostnames and mail addresses). Also note start- and end-time of the attack.
2. How confident are you about the description above (0-100%)?
3. What kind of incident was it (use separate taxonomy)?
4. What vulnerabilities were exploited?
5. Where in the kill chain is Attack 1?



6. What was the reason behind the attack?
7. Which system or systems are under attack?
8. How critical is the system?

Not at all critical ① ② ③ ④ ⑤ ⑥ ⑦ Very critical

9. How severe was the attack?

Not at all severe ① ② ③ ④ ⑤ ⑥ ⑦ Very severe

10. Was the attack automatic?
11. Was the attack directed?
12. What actions should be taken?
13. How urgent is it to take action?

Not at all urgent ① ② ③ ④ ⑤ ⑥ ⑦ Very urgent

Fig. 4. Questionnaire to measure cyber situation awareness for analysts.

V. Discussion

Modern organizations rely on information systems, and most information systems are exposed to threats. Operators monitoring a technical infrastructure need a good situation awareness to prevent antagonists from detecting and exploiting vulnerabilities in the information system, something which may result in severe consequences. There is extensive research about situation awareness, and extensive research on computer network defense analysis, but research combining the two fields in order to develop reliable and valid measure of cyber situation awareness is more limited. Previous research has emphasized the value of CSA and that it is necessary to develop methods to measure CSA [55], but research that present and evaluate a proposal on how this should be done is rare.

Cyber security is a broad area with many different tasks that are performed in different settings. It is therefore impossible to define cyber situational awareness that is applicable in all situations, and similarly, it is not advisable to develop one general CSA measurement method. We believe that the main reason to why our technique was well received by the participants was the work made in developing a technique in which they could recognize their vocabulary and tasks. Transferring the technique to another branch of cyber security would require a situation awareness requirements analysis to ensure that the queries are applicable and understandable in that setting. The elements that constitute situational awareness in a specific work situation need to be identified. From these elements, methods to measure situational awareness can be developed.

In the current paper we conducted a goal-directed task analysis and a hierarchical task analysis to obtain better understanding of log analysts' work and to identify elements constituting their situation awareness. This resulted in two questionnaires, one for scouts and one for analysts. These were developed and validated in close cooperation with professional log analysts. The results from this validation were positive and only minor improvements were suggested by the log analysts. This suggests that the goal-directed and hierarchical tasks analyses are methods well suited for detecting elements constituting CSA, and more specifically log analysis. The revised questionnaires (Fig. 3 and 4) presented in the current paper is one of the few proposals that is based on an established situation awareness technique (SAGAT) to measure CSA. CSA-measures published before, generally include specific questions such as whether a specific IP address is a problem that must be reported, if the traffic between two specific IP addresses are as expected, and what the expected result of a vulnerability scan is. These questions are reasonable and meaningful, but in the interviews we conducted, and the feedback we receive from the validation of our questionnaires, this is not enough. In particular because these questions do not address a broader understanding for the magnitude and consequences of the attack. For instance, it is also important to categorize the attacks according to a predetermined taxonomy, to assess where in the attack chain attacks are, understanding the network map, the purpose behind the attack, how severe the attack is, what vulnerability that were exploited, and how fast countermeasures must be taken. These kinds of queries are not included in earlier SAGAT-questionnaires within cyber security. Furthermore, earlier suggestions to measure CSA do not adapt the questionnaires to different roles in the way we did for scouts and analysts.

The questionnaires presented in this paper should not be regarded as final, but the positive validation results suggests that they contain many elements considered to be CSA by professionals. However, the revised questionnaires need to be re-introduced for subject matter experts. Even though the questionnaires were well received, other situation awareness measures and performance measures should be considered. The correlation between different measures (e.g. situation awareness, performance and mental workload) is not clear [37]. Therefore, the next natural step after the positive feedback on face validity is to test and receive quantitative feedback from experts regarding convergent and discriminant validity. Furthermore, it is important to investigate correlations between different CSA measurement methods and performance measures. This requires further testing with subject matter experts.

VI. Conclusion

The main conclusion from the research presented in this paper is that the established situation awareness measurement method freeze probe is well suited for measuring situation awareness within cyber security during exercises. We contribute to this research area through the development of two freeze probe questionnaires that can be used to measure log analytics' cyber situation awareness. During the validation professional log analytics confirmed that selected parts of the developed questionnaires can further be used as a template to keep track of identified events during their daily work.

VII. References

[1] B. Newhouse, S. Keith, B. Scribner, and G. Witte, "Draft NIST SP 800-181, NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Eduction (NICE)."

[2] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology."

[3] ENISA, "Good practice guide for incident handling," 2010.

[4] T. Sommestad and A. Hunstad, "Intrusion detection and the role of the system administrator," *Inf. Manag. Comput. Secur.*, vol. 21, no. 1, pp. 30–40, Mar. 2013.

[5] J. R. Goodall, W. G. Lutters, and A. Komlodi, "Developing expertise for network intrusion detection," *Inf. Technol. People*, vol. 22, no. 2, pp. 92–108, Jun. 2009.

[6] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: the diagnostic work of IT security incident response," *Inf. Manag. Comput. Secur.*, vol. 18, no. 1, pp. 26–42, Mar. 2010.

[7] M. R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 37, no. 1, pp. 32–64, Mar. 1995.

[8] Z. Huang, "Human-centric training and assessment for cyber situation awareness," 2015.

[9] M. R. Endsley, D. J. Garland, R. L. Wampler, and M. D. Matthews, "Modeling and Measuring Situation Awareness in the Infantry Operational Environment." 2000.

[10] M. R. Endsley and M. W. Smolensky, *Situation awareness in air traffic control: The picture.* Academic Press, 1998.

[11] M. D. Matthews, L. D. Strater, and M. R. Endsley, "Situation Awareness Requirements for Infantry Platoon Leaders.," *Mil. Psychol.*, vol. 16, no. 3, pp. 149–161, 2004.

[12] P. M. Salmon *et al.*, "Measuring Situation Awareness in complex systems: Comparison of measures study," *Int. J. Ind. Ergon.*, vol. 39, no. 3, pp. 490–500, 2009.

[13] M. R. Endsley and D. Garland, *Direct meusurement of situation awareness: validity and use of SAGAT*. Mahwah, NJ: Lawrence Erlbaum Associates, 2000.

[14] M. R. Endsley, "A Survey of Situation Awareness Requirements in Air-to-Air Combat Fighters," *Int. J. Aviat. Psychol.*, vol. 3, no. 2, pp. 157–168, Apr. 1993.

[15] M. R. Endsley, "Situation awareness global assessment technique (SAGAT)," in *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, pp. 789–795.

[16] M. R. Endsley, S. J. Selcon, T. D. Hardiman, and D. G. Croft, "A Comparative Analysis of Sagat and Sart for Evaluations of Situation Awareness," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 42, no. 1, pp. 82–86, Oct. 1998.

[17] M. D. Matthews and S. A. Beal, "Assessing Situation Awareness in Field Training Exercises." 2002.

[18] G. H. Walker, N. A. Stanton, T. A. Kazi, P. M. Salmon, and D. P. Jenkins, "Does advanced driver training improve situational awareness?," *Appl. Ergon.*, vol. 40, no. 4, pp. 678–687, 2009.

[19] D. N. HOGG, K. FOLLES⊘, F. STRAND-VOLDEN, and B. TORRALBA, "Development of a situation awareness measure to evaluate advanced alarm systems in nuclear power plant control rooms," *Ergonomics*, vol. 38, no. 11, pp. 2394–2413, Nov. 1995.

[20] F. T. Durso and A. Dattel, "No Title," in *A cognitive approach to situation awareness: Theory, measures and application*, New York, NY: Aldershot, 2004, pp. 137–154.

[21] R. M. Taylor, "Situation awareness technique (SART): The development of a tool for aircrew system design," in *Situation awareness in aerospace operations*, Neuilly-Sur-Seine, France, 1990.

[22] J. Brynielsson, U. Franke, and S. Varga, "Cyber Situational Awareness Testing," Springer International Publishing, 2016, pp. 209–233.

[23] R. S. Gutzwiller, S. M. Hunt, and D. S. Lange, "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, pp. 14–20.

[24] T. Bass and Tim, "Intrusion detection systems and multisensor data fusion," *Commun. ACM*, vol. 43, no. 4, pp. 99–105, Apr. 2000.

[25] R. S. Gutzwiller, S. Fugate, B. D. Sawyer, and P. A. Hancock, "The Human Factors of Cyber Network Defense," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 59, no. 1, pp. 322–326, Sep. 2015.

[26] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A Survey of Visualization Systems for Network Security," *IEEE Trans. Vis. Comput. Graph.*, vol. 18, no. 8, pp. 1313–1329, Aug. 2012.

[27] J. Dressler, C. L. Bowen, W. Moody, and J. Koepke, "Operational data classes for establishing situational awareness in cyberspace," in *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, 2014, pp. 175–186.

[28] S. Mahoney, E. Roth, K. Steinke, J. Pfautz, C. Wu, and M. Farry, "A Cognitive Task Analysis for Cyber Situational Awareness," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 54, no. 4, pp. 279–283, Sep. 2010.

[29] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Human Behav.*, vol. 48, pp. 51–61, 2015.

[30] B. M. Bowen, S. J. Stolfo, and R. Devarajan, "Measuring the Human Factor of Cyber Security," 2012.

[31] M. W. Boyce, K. M. Duma, L. J. Hettinger, T. B. Malone, D. P.

Wilson, and J. Lockett-Reynolds, “Human Performance in Cybersecurity: A Research Agenda,” *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 55, no. 1, pp. 1115–1119, Sep. 2011.

[32] V. Dutt, Y.-S. Ahn, and C. Gonzalez, “Cyber Situation Awareness,” *Hum. Factors*, vol. 55, no. 3, pp. 605–618, Jun. 2013.

[33] V. F. Mancuso, J. C. Christensen, J. Cowley, V. Finomore, C. Gonzalez, and B. Knott, “Human Factors in Cyber Warfare II,” *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 58, no. 1, pp. 415–418, Sep. 2014.

[34] V. F. Mancuso, A. J. Strang, G. J. Funke, and V. S. Finomore, “Human Factors of Cyber Attacks,” *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 58, no. 1, pp. 437–441, Sep. 2014.

[35] Y. J. Tenney and R. W. Pew, “Situation Awareness Catches On: What? So What? Now What?,” *Rev. Hum. Factors Ergon.*, vol. 2, no. 1, pp. 1–34, Apr. 2006.

[36] A. Malviya, G. A. Fink, L. Sego, and B. Endicott-Popovsky, “Situational Awareness as a Measure of Performance in Cyber Security Collaborative Work,” in *2011 Eighth International Conference on Information Technology: New Generations*, 2011, pp. 937–942.

[37] N. A. Giacobe, “Measuring the Effectiveness of Visual Analytics and Data Fusion Techniques on Situation Awareness in Cyber-security.” 2012.

[38] N. A. Giacobe, “A Picture is Worth a Thousand Alerts,” *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 57, no. 1, pp. 172–176, Sep. 2013.

[39] M. Evangelopoulou and C. W. Johnson, “Attack Visualisation for Cyber-Security Situation Awareness,” in *9th IET International Conference on System Safety and Cyber Security (2014)*, 2014, p. 1.2.2-1.2.2.

[40] P. Barford *et al.*, “Cyber SA: Situational Awareness for Cyber Defense,” Springer US, 2010, pp. 3–13.

[41] B. D. Sawyer *et al.*, “Cyber Vigilance,” *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 58, no. 1, pp. 1771–1775, Sep. 2014.

[42] N. A. Stanton, P. R. Salmon, G. B. Walker, and D. Jenkins, *Human Factors Methods: A Practical Guide for Engineering and Design*. Surrey, England: Ashgate Publishing Limited, 2013.

[43] Samual G. Charlton, “Questionnaire Techniques for Test and Evaluation,” in *Handbook of human factors testing and evaluation*, 2nd. ed., T. G. O. Samuel G. Charlton, Ed. Mahwah, N.J.: Lawrence Erlbaum Associates, Publishers, 2002, pp. 81–99.

[44] Andrew M. Colman, Claire E. Norris, and Carolyn C. Preston, “Comparing Rating Scales of Different Lengths: Equivalence of Scores From 5-Point and 7-Point Scales.”

[45] T. Sommestad, “STO-MP-IST-133 Experimentation on operational cyber security in CRATE.”

[46] H. Holm and T. Sommestad, “SVED: Scanning, Vulnerabilities, Exploits and Detection,” in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, pp. 976–981.

[47] “Wireshark · Go Deep.” [Online]. Available: https://www.wireshark.org/. [Accessed: 14-Feb-2017].

[48] “ELK Product Overview,” 2017. [Online]. Available: https://www.elastic.co/products. [Accessed: 15-Feb-2017].

[49] “Snort - Network Intrusion Detection & Prevention System.” [Online]. Available: https://www.snort.org/. [Accessed: 14-Feb-2017].

[50] “Windows Event Logs.” [Online]. Available: https://technet.microsoft.com/en-us/library/cc722404(v=ws.11).aspx. [Accessed: 14-Feb-2017].

[51] “SIEM, Enterprise Security Information Event Management Solutions | Hewlett Packard Enterprise Sverige.” [Online]. Available: http://www8.hp.com/se/sv/software-solutions/siem-security-information-event-management/index.html. [Accessed: 14-Feb-2017].

[52] “Cyber Kill Chain® · Lockheed Martin.” [Online]. Available: http://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html. [Accessed: 15-Feb-2017].

[53] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, “A multi-layered and kill-chain based security analysis framework for cyber-physical systems,” *Int. J. Crit. Infrastruct. Prot.*, vol. 11, pp. 39–50, 2015.

[54] S. Hansman and R. Hunt, “A taxonomy of network and computer attacks,” *Comput. Secur.*, vol. 24, no. 1, pp. 31–43, 2005.

[55] J. Brynielsson, U. Franke, M. Adnan Tariq, and S. Varga, “Using cyber defense exercises to obtain additional data for attacker profiling,” in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 37–42.