A Test Tool to Evaluate the Skill Sets of Tier-1 Security Analysts in a SOC Environment: A Case Study from Recruitment to Operations

Adriana Radu
Eindhoven University of Technology
a.radu@student.tue.nl

Leon Kersten
Eindhoven University of Technology
l.kersten.1@tue.nl

Rik Wosyka
Eindhoven University of Technology
r.t.l.wosyka@student.tue.nl

Tom Mulders
Eindhoven University of Technology
t.r.j.mulders@tue.nl

Emmanuele Zambon
Eindhoven University of Technology
e.zambon@tue.nl

Luca Allodi
Eindhoven University of Technology
l.allodi@tue.nl

***Abstract*—The skill set of tier-1 (T1) analysts have a great influence on the day-to-day operations of a Security Operation Center (SOC). Therefore, it is critical for a SOC to be able to evaluate the relevant skill sets of incoming analyst at recruitment and throughout their progress at the SOC. In this short paper, we identify from extant literature the relevant skills an analyst needs, and devise a test to evaluate those in collaboration with a commercial SOC. We conduct a case study of this test with three aspiring analysts at the collaborating SOC over a period of three months. Our case study shows that the test can be used to evaluate different skills of an analyst and can give insights at the SOC on analyst progress and training effectiveness, opening avenues for a full validation of the testing framework in future work. We discuss results, limitations, and future directions of this work.**

I. Introduction

Security Operation Centers (SOCs) are organizations or business units that monitor the security of, typically, IT infrastructures. SOCs employ a mixture of network and host-level sensors to evaluate potentially malicious activities in the network traffic or the local activity of a host [1], [2]. These sensors generate alert data for human analysts to evaluate, oftentimes with some technological aid such as automatic correlation of potentially related alerts [2], [3].

The task of a SOC analyst is a complex one [4] and requires a number of hard and soft skills to be executed fully [3], [5]. Analysts need the technical competency to analyze security logs and alerts, relate them to attack patterns, identify additional evidence or relevant information from external sources, and identify relevant evidence to reconstruct an (ongoing) attack [1]. On the other hand, incident investigation is often a collective effort requiring orchestrated operations by multiple analysts [3] and communication plays a central role in alert escalation and incident response [6], [7]. As such, the profile of the ideal analyst is a multi-faceted one, where the skills that are needed and fostered are still unclear. Critically, junior 'tier-1 analysts' tasked with the 'first line' investigation of incoming alerts are inexperienced [5], [7], may come from different backgrounds, and have a relatively high turnover [8]. How to select, recruit, train, and monitor the progress of tier-1 analysts is an open problem that, to the best of our knowledge is not fully covered in the literature.

In this short paper we review the literature to identify which soft and hard skills are generally linked to professions in the cybersecurity domain, and cast these on the profile of the junior SOC analyst. To do so, we collaborate with a commercial SOC providing managed security monitoring services to SMEs in Europe. With their collaboration we identify relevant skills and devise a set of tests to evaluate (aspiring) junior analysts at time of recruitment, after training, and at after a period of practice at the SOC. We perform a case study of the devised test with three (from which two completed the training after recruitment) potential recruits interested in joining the SOC (as the test is prototypical, hiring decisions were *not* based on test outcomes), and showcase how the test can help SOC managers evaluate internal training procedures and progress of junior analyst profiles during their employment. We stress that the goal of this paper is to present a test for security analyst skills, rather than evaluating how the skill set of analysts evolves, affects analyst performance, or varies across SOCs.

This paper unfolds as follows: Section II discusses necessary background on relevant cybersecurity skills. Section III details the method followed to synthesize the test from the identified skills, whereas Section IV presents the final test(s). Finally, Section V discusses results from the case study application of the test, and Section VI concludes the paper.

Workshop on Security Operation Center Operations and Construction (WOSOC) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-0-4
https://dx.doi.org/10.14722/wosoc.2025.23001
www.ndss-symposium.org

II. Background

A. SOC and tier-1 analysts

A security operation center (SOC) is an organizational unit providing monitoring services of networks and infrastructures to detect, analyze and oftentimes respond to incoming cybersecurity incidents. The operations of SOCs are commonly narrated using the *People, Process* and *Technology* (PPT) framework [3]. More specifically, the SOC utilizes technology, such as network intrusion detection systems (NIDS) and endpoint detection to generate security events [1] that are fed to SIEM (Security Information and Event Management) systems which aggregate and present such events to human analysts for analysis and classification [3]. Analysis methods and *Processes* depend on the specific SOCs and the type of ingested data [1]. A common structure for the *People* and *Process* aspects of the SOC is a tiered system of SOC analysts [2], [9]–[11]. Tier-1 (T1) analysts tackle the majority of incoming security alerts and escalate the alerts possibly representing more severe incidents for evaluation from the higher tier analysts. Despite the high volume of incoming alerts, as T1 analysts' alert investigations is less in depth as other tiers, T1 analysts are commonly considered an entry level position within a SOC. Therefore, T1 analysts are more likely to be inexperienced than other SOC analysts [5], [7], and require initial training. Nonetheless, the role of a T1 analyst is critical in a hierarchical SOC as erroneously dismissed attack-related alerts may lead to delayed detection of the attack, leading to later responses and higher negative impact on the affected organization(s) [1]. Similarly, alerts escalated without good reason or communicated incompletely or imprecisely to higher tiers, cause critical inefficiencies in the investigation of the incidents that do matter. It is therefore crucial that T1 analysts possess the right skill set to analyze and communicate information on alerts efficiently and accurately.

B. Related work on analyst skills

Previous research [10], [12], [13] has stressed the importance of situational awareness (SA) for security analysts. Although SA has a wide interpretation depending on extant literature, in our work we consider the definition given by Ofte et al. [14]: "*(SA) refers to the process of gathering information about a situation and converting this information into an awareness that can differentiate between the suitability of potential actions*". Since analysts' SA can be improved upon through internal (e.g., by building tacit knowledge through work experience) and external (e.g., analyst training) factors, in our work we consider SA a high-level skill.

Considering the importance of being able to gather and navigate through information for SA, most of the literature reports skills directly related to information acquisition. For example, a key task for a SOC analyst is to navigate through the SIEM [3], [7], to find and interpret relevant logs [2], [15]. Additionally, the usage of domain specific tools such as OSINT tools, or sandbox environments are crucial to gain more information about attacks either through second-hand sources (e.g., forums) or hands-on testing of a malware. Moreover, research is a soft skill that supports all forms of gathering information from second-hand sources, and thus is considered a critical skill for analysts as well [16]. On top of the ability to gather information, knowledge of relevant concepts such as common attack patterns and commonly used protocols are crucial for analysts to interpret the complex network data that is observed [2], [17]. Without such knowledge, even if an analyst observes an evidence of an attack, the analyst may dismiss and wrongfully conclude that the network traffic is behaving normally. In addition to technical skills, many soft skills shown in Table I such as critical thinking and self-evaluation is crucial for an analyst to develop new knowledge themselves [3], [8] that in turn analysts can utilize in their alert investigations. Meanwhile, communication is critical in not developing new knowledge for oneself, however to share otherwise tacit knowledge towards other analysts or management [6]. Given the prevalence of tacit knowledge among SOCs [6], transforming tacit knowledge to explicit knowledge may significantly increase the SA of the SOC as a whole. Finally, the decision to escalate an attack or call the customer depends on the impact the possible attack may have on the customer. One attack may be catastrophic to one environment or organization, while being ineffective or inconsequential for another. Therefore, it is crucial to be able to to assess the risk associated to an attack, after conducting the investigation to perform the final classification of the alert. Table I provides an overview of skills described in the extant literature.

C. Related work on analyst evaluation

There is little research proposing systematic testing frameworks to evaluate SOC analysts whether it may be on performance during analysts day-to-day operations or skill sets used for training and recruitment. To our knowledge the study conducted by Agyepong et al. [20] is the only work proposing a systematic framework to measure the performance of a SOC analyst. Agyepong et al. [20] utilizes the Delphi method involving industry experts to devise "SOC Analyst Assessment Method" (SOC-AAM), a weighted approach to measure the performance of a security analyst. SOC-AAM categorizes the analyst's task into six main functions to measure 31 different KPIs and expect analyst's to conduct a simulated alert analysis to gather information relevant to each category [20]. The work is evaluated among SOC managers and received an overall positive evaluation. Importantly, SOC-AAM is devised as a performance evaluation framework for analysts beyond their initial training. In their work, the skill set of an analyst is assumed to be constant and therefore focuses on measuring the quality of the security analysis and reporting [20] as opposed to the skill set required to be or become a well-performing T1 analyst. Moreover, the authors of SOC-AAM argue that their framework applies to the generic SOC analysts and claim their framework to be best suited for non-hierarchical SOCs [20].

TABLE I
IDENTIFIED SKILLS NEEDED FOR T1-LEVEL ANALYSIS

Skill	Definition	References
Communication	The ability to communicate information to other people, whether they are other analysts or not.	[3], [6], [7]
Critical Thinking	The ability to think logically and to understand the situation before making judgments.	[3]
Research	The ability to perform research and gather information. This also includes knowing where to gather information, and discerning when the gathered information might be sufficient.	[16]
Self-Evaluation	The ability to recognize what the analyst themselves did well, and where the analyst could improve.	[8]
Risk Assessment	The ability to assess the risk of a situation, event, or alert in order to make accurate decisions.	[3]
Use of OSINT Tools	The ability to use OSINT tools, and to know which one to use in a given situation.	[3], [16]
Use of SIEM Tools	The ability to utilize the SIEM environment effectively to collect information, help with analysis, keep track of history, etc.	[3], [5], [7], [18]
Log Analysis	The ability to use a variety of logs to gather information about and understand an alert.	[2], [3], [7], [15]
Use of Sandbox Environments	The ability to test suspicious files in sandbox environments in order to better analyse them.	[3]
Knowledge of TCP/IP Stack and Network Control Flow	Knowing the basics of the TCP/IP stack and knowing what common protocols exist and its normal usage.	[2], [3], [16]
Knowledge of Common Attack Patterns	Knowing how cyber attacks usually work. This involves general knowledge of attacks, not necessarily in-depth insight into the flow of a specific attack.	[3], [19]

D. Problem statement and contribution

Because of the importance of T1-level analysis in SOC operations, it is crucial that SOC managers are aware of the relevant skillet that their (potential) analysts possess (or lack of) to, for example, decide whether to recruit an aspiring analyst, to tailor training to specific skill gaps, or for analysis prioritization among analysts. Although, Agyepong et al. [20] proposes a comprehensive testing framework for SOC analysts as a whole, their framework is designed to measure mature SOC analysts who have already undertaken recruitment and the necessary initial training. To our knowledge, there is no work aimed to evaluate the *skill set* of an analyst, especially in the context of recruiting and training analysts. Considering that junior analyst oftentimes start as a T1 analyst in hierarchical SOCs (i.e., T1 analyst is an entry level position), it is crucial to devise a test framework which takes into account the recruitment and the initial training process of SOCs.

Although the skill set reported in Table I is general and applicable across SOCs, different SOCs employ different procedures, and collect and investigate different data. Therefore, a specific test suitable to all SOCs cannot be realistically devised. Differently, in this work we collaborate with a commercial SOC to operationalize the analyst skill set defined in Table I by developing a test to evaluate analyst skill sets at recruitment time, and throughout their evaluation period. We design and implement the test, and showcase its application at the collaborating SOC. We note that the proposed test can then be adapted to specific SOC/SIEM technologies for replication by, for example, changing score weights and prompt log data relevant to a specific SOC. Importantly, by tying the proposed test to the overall framework identified in Table I, replicating SOCs and researchers can select, remove, or modify specific test items as best fitting to the relevant environment.

III. TEST DEVELOPMENT AND EVALUATION

The test is built in collaboration with a commercial SOC. The SOC provides managed network security monitoring services to one medium-to-large sized European university and multiple SMEs operating in health and IT sectors. The collaborating SOC permanently employs 7 employees (from which 4 conduct security monitoring) and employs at a given moment 2-6 interns acting as junior T1 analysts. This study involved two tier-3 analysts (one of which doubling as the Chief Technology Officer at the SOC), a tier-2 analyst, and the R&D director at the SOC. Further, several T1 analysts provided input to the test development. The two main researchers involved in this study were embedded in the SOC for a period of three months to develop on-the-job experience on the tasks and competencies of T1 analysts.

A. Methodology

The test design process followed an iterative approach. The skill set provided in Table I was used as the basis of a series of iterative meetings with the collaborating SOC to 1) discuss the relevance of each skill to the SOC operations, and 2) discuss how to formulate the test so that it is representative of operations at the SOC. Bi-weekly meetings were scheduled over a period of four months with the SOC management, including head of R&D, a tier-3 analyst with more than 15 years of experience on security monitoring, a tier-2 analyst with more than 4 years of experience, and several (3-6, depending on availability) junior T1 analysts. The purpose of these bi-weekly meetings was to brainstorm specific skills

from Table I and conceptualize them with the group. Whereas the role of the R&D director and tier-3 analyst was mainly of moderating and steering the conversation to assure a smooth development of the process, the tier-2 and T1 analysts provided the necessary input to map the skills to operations and data at the SOC. Further, weekly meetings were setup between the two main researchers and the tier-2 analyst to monitor the implementation of the decisions taken in the bi-weekly meetings. The overall work schedule was setup by iteratively discussing and reviewing the implementation of the skill set from Table I. The last-to-final test(s) were piloted by the tier-3 analyst and the R&D director, who provided feedback to finalize question formulation and test execution. A second pilot with two T1 analysts was run on the final tests to evaluate any final adjustment on the implementation, for example to highlight areas of ambiguity in specific questions and taken time to complete the test.

As the test goal is both to evaluate analyst skill set at recruitment and their progress during (the first few months of) employment, we split the test into three sub-tests: a 'recruitment test' to be used to interview analysts, an 'initial test' to evaluate hired analysts' skill set after receiving the onboard training from the SOC and a 'final test' to evaluate analysts' skill set progress after three months of employment. Whereas themes were recurrent, questions across the three tests are different (i.e., not asked twice at different test moments). The pilot setup described above provided full coverage of the implementation, so feedback was collected on all items.

B. Skill selection and test design

Based on the literature research, the identified list of skills needed by a T1 analyst in a SOC comprised of 12 skills. However, as the tests are aimed to evaluate the performance of analysts working at a real SOC, the list was partially modified to fit the SOC better. For example, the use of sandbox environments skill was deemed non-essential for this specific SOC (which focuses on network monitoring, and therefore seldom requires running potentially malicious samples in a sandbox) and therefore removed from the list. Furthermore, the skill knowledge of TCP/IP stack and the skill knowledge of network control flow were considered similar from a testing viewpoint, and combined into a single question. In contrast, the communication skill was divided into two distinct cases, analyst-to-analyst communication and analyst-to-customer communication. This was deemed important as the level of details and the conveyed information varies significantly for 'technical internal communications' generally aimed at alert investigation, and communications aimed at providing actionable information about an incident to inform possible remediation/response activities.

C. Case study

A case study at the SOC was conducted to evaluate the Recruitment, Initial, and Final tests. The participants in this study were three university students with a background in Computer Science requesting to join the SOC for an internship as T1 analysts. To alleviate the workload of SOC employees and to simulate an environment where time pressure is considerable due to the high volume of incoming alerts, the subjects were instructed to not take more than 2 hours to complete the test. The Initial and Final tests were undertaken by only two subjects as one dropped off the internship program. All test answers were graded by the SOC's tier-2 analyst, adhering to the grading rubric described in Subsection IV-A. To ensure correctness of the grading process, any uncertainties regarding the participants' responses were reviewed and discussed with a tier-3 analyst at the SOC.

D. Ethical considerations

This research was conducted under ethical approval from our institution's ethical review board under approval number `ERB2022MCS20`. We gained informed consent from all subjects to use the results of their tests for research purposes. For the purpose of this research, the identity of the subjects are anonymized to the researchers. For the purposes of recruitment and operations, internal records at the SOC are de-anonnymized. Due to the small sample size for the purpose of the case study presented in this paper, we refrain from disclosing detailed demographic information on the subjects to avoid de-anonymization risks. As the goal of this paper is not to evaluate security analysts skills, but to present a test that can serve that purpose, we consider the de-anonymization risk not commensurate to the intended contribution.

IV. Overview of question items and scoring

Table II gives an overview of the identified skills, examples of asked questions, the number of questions present per test, and in which of the recruitment, initial, and final test they are covered. In total, the recruitment, initial and final test contain 44, 47 and 68 questions respectively. The three tests predominantly feature multiple-choice questions with a single correct answer. A few multiple-choice questions include multiple correct answers and participants must select all correct options to receive the points.

The test first asks **self-evaluation** questions requiring T1 analysts to evaluate their own skills on a scale of 1 to 5. These are meant as controls to evaluate the gap between self-assessment and emergent skills.

The **research and use of OSINT** tools skill tests are the only components that allow the use of the internet for finding answers. For the research skill, the analysts are given a vulnerability identifier in the form of a Common Vulnerability and Exposures (CVE) ID, and are assessed based on their ability to gather detailed information about it, such as affected systems, proof of concept, or vulnerability type. Similarly, use of OSINT tools evaluates their proficiency in using various tools to navigate and find relevant information regarding a given domain name and hash value, such as the location of the IP the domain resolves to or the size of the hash file. These questions gauge the respondent's ability to independently identify key information about security threats and related contextual information.

TABLE II
OVERVIEW OF ALL THE SKILLS MEASURED IN THE THREE TESTS. * R, I, F REPRESENT THE RECURITMENT, INITIAL, AND FINAL TEST RESPECTIVELY.

Skill	**Question example**	**no. Qs**	**Test***		
			R	I	F
Self-evaluation	How confident are you in risk assessment? The risk assessment skill refers to the ability to judge the risk of a situation, event, or alert in order to make more accurate decisions.	10	✓	✓	✓
Research	Why can the vulnerability be exploited with no interaction?	6	✓		✓
Knowledge of common attack patterns	You notice unusual activities on a network host such as keystroke logging, recording of internet browsing history and login details. Further investigation shows that this data is periodically sent to an external IP address. What attack pattern is possibly associated with this behavior?	6-7	✓		✓
Risk assessment	Rule: ET EXPLOIT_KIT Balada Domain in DNS Lookup (specialcraftbox .com). A WLAN user made 9 DNS requests to 4 different domains known to be related to the Balada Injector Malware. The DNS requests got resolved successfully.	5		✓	✓
Use of OSINT tools	Using VirusTotal, find out what the threat category label of the given hash is.	9	✓		✓
Use of SIEM tools	Which IP had the highest number of unsuccessful SSH authentication attempts on 17/09/2023 between 05:00-08:30?	6		✓	✓
Log analysis	Which of the following logs indicates a successful TCP connection?	6		✓	✓
Analyst-to-analyst communication	You observe an interesting alert, and you want a second opinion about it. Based on the given information, write a short (max 150 words) analysis that you would communicate to a fellow analyst in order to get help. ... Your question for the fellow analyst is the following: ”Based on the information I found, should this alert be reported?”	1	✓	✓	✓
Analyst-to-customer communication	Write a customer incident report (max 250 words) for the following scenario of an alert. The report should include a description of the event that occurred and possible mitigations.	1		✓	✓
Critical thinking	You observe numerous alerts regarding DGA domains that got NXDOMAIN. After inspecting the alerts, you notice the domains are not malicious and not DGA, what do you do?	6		✓	✓
Knowledge of TCP/IP stack & network control flow	What is the correct response type to the request query “PTR 41.249.3.86.in-addr.arpa”?	11-12	✓	✓	✓

The **knowledge of common attack patterns** skill test gauges the analyst's understanding of various attacks. These questions can be either theory-based, such as 'What is the primary purpose of active scanning?', or scenario-based such as 'You observed a suspicious external network request following which numerous files were uploaded to a suspicious file sharing platform. What attack pattern is typically associated with this behavior?'. In a similar fashion, the **critical thinking** skill test employs multiple-choice, scenario-based questions aimed at evaluating the ability of the respondent to link attack patterns to investigation actions. In practice, the analyst has to indicate which would be the appropriate next step in a given investigation among a range of options.

The **analyst-to-analyst communication** and **analyst-to-customer communication** skills are measured with one open-ended question each, and require the junior analyst to write a short paragraph of max 150 words and 250 words respectively. These questions provide information regarding an attack and task the analyst to write an incident report based on the given information. For anonymity purposes, the contexts of these questions are omitted in Table II. These questions aim at evaluating the analyst's ability to synthesise and communicate technical information to the two main stakeholders in an investigation (i.e., the SOC itself, and the customer).

For the **risk assessment** skill test, analysts are asked to assign a severity level to different attack scenarios. The analysts can assign one out of five possible labels, ordered from least to highest risk. Since risk perception is subjective to a degree, risk levels immediately below and above (if any) to the one assigned by the SOC are considered acceptable.

The **log analysis** and **use of SIEM tools** skill tests require the use of a SIEM tool (in this case Security Onion), to investigate

logs and alerts. For the log analysis skill, the analysts are given various links to logs (HTTP, SSL, SSH, conn, or file logs) in the SIEM. For the use of SIEM tools skill, analysts are required to demonstrate their ability to navigate the SIEM interface, by writing custom queries for given time frames, filtering, and sorting logs to find the correct answers. These tasks assess not only the T1 analyst's technical skills in using SIEM tools but also their ability to interpret the data and extract relevant information from it. As proficiency with the specific tool is not expected before recruitment, these two skills are only tested after the initial training.

Lastly, the **knowledge of TCP/IP stack & network control flow** skill test involves analyzing two packet capture files using Wireshark. These questions cover topics regarding specific protocols (such as TCP, DNS) and require the analyst to identify a range of information, including the packet number of the Server Certificate exchange in the TLS handshake, or DNS answers to specific requests to demonstrate their understanding of features of network communication protocols.

A. Answer evaluation

Each multiple-choice question is by default equally weighted (base weight of 1 point). As the skills analyst-to-analyst communication and analyst-to-customer communication are assessed based on a single open-ended question each, and are of higher complexity and importance, they are weighted at 20 and 10 points respectively. Analyst-to-analyst communication is weighted more heavily than analyst-to-customer as T1 analysts rarely communicate with customers (oftentimes tier-2 or higher analysts communicate with the customers) while T1 analysts are expected to communicate clearly with other analysts during hand over meetings and alert escalation procedures. Both communication related skills are graded using a rubric with 5 criteria, each outlining specific information that should be present in the short report. For each correct criterion included, the analyst is given 4 points (for the analyst-to-analyst communication) and 2 points (for the analyst-to-customer communication). Contrarily, if the analyst includes information that is not related to the given scenario, 1 or 2 points are deducted per piece of information. The total points realised by a candidate represent the overall score, which can then be normalized over the total.

B. Skill assignment to Recruitment, Initial, and Final tests

Whereas all skills are relevant to the final evaluation of an analyst (i.e., after training and a practice period), not all skills are deemed critical or necessary at all stages. A SOC may for example decide that some level of experience or training is needed to address certain skill sets (e.g., communication to customers). In these cases, related questions would only increase the burden on the subject (and the assessor) without adding information to the assessment. Further, the 'initial' test should focus on skills analysts have received training for since their recruitment test, to avoid double-testing and unnecessary burden. In the case of the collaborating SOC, the skill set on risk assessment, use of SIEM tools, log analysis, and analyst-to-customer communication were thought not to be relevant at recruitment time as they require knowledge of specific internal procedures. All these skills are then included in the Initial tests to evaluate recruited analysts uptake during training. On the other hand, skills that receive no training such as research or use of OSINT tools do not need to be re-tested. The final test includes all skills.

V. Case study application at the collaborating SOC

Table III reports the results of the three prospective analysts. We note that Subject 1 dropped out of the recruitment process, resulting in only Subject 2 and 3 continuing to the subsequent tests. The participants took an average of 95 minutes to complete test. The discussion below is not meant to report analyst performance or specific insights on the recruitment process at SOC. Differently, it serves as an example of the type of considerations a SOC can make by employing the proposed test for the identified skill set throughout the initial period of employment of newly recruited analysts, including at recruitment time.

Overall, Subject 1 and Subject 3 performed similarly at the Recruitment test, with Subject 2 showing a bigger gap on analyst-to-analyst communication. The poor performance of Subject 2 is due to misunderstanding the task, which led to their inability to answer the question correctly, resulting in no points. Regardless, none of the subjects performed well on the communication skill, suggesting the SOC may want to focus training efforts on communication. With the exception of this skill, all three analysts perform similarly over all tested skills, with a recurrent gap (particularly for Subject 1 and 2) on the Research skill set. Technical knowledge on TCP/IP and network control flow and knowledge of attack patterns seems good and uniform across subjects.

The Initial test provides insights on the importance and effectiveness of the training recruited analysts currently receive. Scores on previously untested items (e.g., risk assessment) indicate the training informs analysts well enough of internal procedures (e.g., what type of security event does the SOC consider "high risk"). On the other hand, communication skills seem 'stickier' in that the training does not seem to substantially improve analyst-to-analyst communication. On the other hand, Subjects 2 and 3 perform well on the analyst-to-customer communication skill, suggesting that junior analysts may find it hard to effectively select and communicate relevant technical information (characteristic of analyst-to-analyst communication). Technical training on network protocols does not seem to improve outcomes, suggesting either the test is unbalanced or that the current training is not effective enough on this skill.

The Final test provides insights on the progress of analysts over the period they spent at the SOC. Whereas a direct comparison between Recruitment/Initial and Final tests is not possible because the tested skills are not fully overlapping, an indication can be provided by looking in Table III at the

TABLE III
FINAL TEST RESULTS

Subject	Skill	Test							
		Recruitment		Initial		(Interim)		Final	
		Grade	Total	Grade	Total	Grade	Total	Grade	Total
Subject 1	Research	2/7	35/54 (64.8%)	-	-	2/7	-	-	-
	Knowledge of common attack patterns	6/7		-		6/7		-	
	Risk assessment	-		-		-		-	
	Use of OSINT tools	7/9		-		7/9		-	
	Use of SIEM tools	-		-		-		-	
	Log analysis	-	-			-		-	
	Analyst-to-analyst communication	11/20		-		11/20		-	
	Analyst-to-customer communication	-		-		-		-	
	Critical thinking	-		-		-		-	
	Knowledge of TCP/IP stack & network control flow	9/11		-		9/11		-	
Subject 2	Research	2/7	25/54 (46.3%)	-	44/69 (63.7%)	2/7	61/92 (66.3%)	2/8	66/92 (71.7%)
	Knowledge of common attack patterns	7/7		-		7/7		5/6	
	Risk assessment	-		4/6		4/6		3/6	
	Use of OSINT tools	8/9		-		8/9		6/9	
	Use of SIEM tools	-		2/7		2/7		4/7	
	Log analysis	-		8/8		8/8		8/8	
	Analyst-to-analyst communication	0/20		12/20		12/20		20/20	
	Analyst-to-customer communication	-		8/10		8/10		8/10	
	Critical thinking	-		4/6		4/6		5/6	
	Knowledge of TCP/IP stack & network control flow	8/11		6/12		6/12		5/12	
Subject 3	Research	5/7	43/54 (79.6%)	-	60/69 (86.9%)	5/7	71/92 (77.1%)	8/8	80/92 (86.9%)
	Knowledge of common attack patterns	7/7		-		7/7		6/6	
	Risk assessment	-		5/6		5/6		6/6	
	Use of OSINT tools	7/9		-		7/9		7/9	
	Use of SIEM tools	-		5/7		5/7		4/7	
	Log analysis	-		7/8		7/8		7/8	
	Analyst-to-analyst communication	14/20		12/20		12/20		18/20	
	Analyst-to-customer communication	-		8/10		8/10		9/10	
	Critical thinking	-		6/6		6/6		5/6	
	Knowledge of TCP/IP stack & network control flow	10/11		9/12		9/12		10/12	

column 'interim test', representing the union of recruitment and initial (i.e., representing the overall skill level of the analyst after training). We observe that overall both subjects improve over the period, with Subject 3 showing the largest gap between the 'interim' and the Final test. We observe that communication skills improve significantly for both subjects during the period at the SOC, suggesting initial training may benefit from a learn-on-the-job approach (e.g., in a blue team exercise). We observe that Subject 2, differently from Subject 3, does not seem to improve on skills related to research and technical network knowledge suggesting that subjects who join the SOC with limited knowledge on these domains may not uptake these skills.

A. Limitations and future work

Whereas the presented test targets key skills with multiple questions, the extent to which each skill is covered by each question is hard to evaluate. A full validation is left for future work, where (final) test results will be matched against an independent, blinded evaluation from SOC managers on all skills. We note that due to the specificity of SOC environments, the proposed questions may not be suitable to test the relevant skill in any and all SOCs. On the other hand, the skill set is general and the specific instances can be modeled over the proposed questions. Further, with the advent of AI-support for security analysis, it comes into question what type of skills will be required to effectively operate AI-enabled technologies in this environment.

VI. Conclusions

In this paper we presented a test evaluating the skills that junior SOC analyst require to perform entry-level security analysis in a professional environment. These skills are derived from the literature and synthesized in collaboration with a commercial SOC. We showcased the test with three potential recruits at the SOC to showcase the type of insights a SOC can derive both on their employees, but also on the effectiveness of their own training procedures.

Acknowledgment

This work is supported by the SeReNity project, Grant No. cs.010, funded by Netherlands Organization for Scientific Research (NWO), by the INTERSECT project, Grant No. NWA.1162.18.301, funded by NWO and by the CATRIN project, Grant No. NWA.1215.18.003 funded by NWO. The authors thank the ESH-SOC for its collaboration in this work.

References

[1] L. Kersten, T. Mulders, E. Zambon, C. Snijders, and L. Allodi, "'give me structure': Synthesis and evaluation of a (network) threat analysis process supporting tier 1 investigations in a security operation center," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 97–111.

[2] A. D'Amico and K. Whitley, *The Real Work of Computer Network Defense Analysts*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 19–37. [Online]. Available: https://doi.org/10.1007/978-3-540-78243-8_2

[3] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 227 756–227 779, 2020.

[4] E. T. Greenlee, G. J. Funke, J. S. Warm, B. D. Sawyer, V. S. Finomore, V. F. Mancuso, M. E. Funke, and G. Matthews, "Stress and workload profiles of network analysis: Not all tasks are created equal," in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed. Cham: Springer International Publishing, 2016, pp. 153–166.

[5] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, Jul. 2015, pp. 347–359.

[6] S. Y. Cho, J. Happa, and S. Creese, "Capturing tacit knowledge in security operation centers," *IEEE Access*, vol. 8, pp. 42 021–42 041, 2020.

[7] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched socs: A qualitative study on security operations center issues," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1955–1970. [Online]. Available: https://doi.org/10.1145/3319535.3354239

[8] S. C. Sundaramurthy, J. McHugh, X. Ou, M. Wesch, A. G. Bardas, and S. R. Rajagopalan, "Turning contradictions into innovations or: How we learned to stop whining and improve security operations," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 237–251.

[9] R. Sadoddin and A. Ghorbani, "Alert correlation survey: Framework and techniques," ser. PST '06. New York, NY, USA: Association for Computing Machinery, 2006. [Online]. Available: https://doi.org/10.1145/1501434.1501479

[10] C. Zhong, J. Yen, P. Liu, R. F. Erbacher, C. Garneau, and B. Chen, *Studying Analysts' Data Triage Operations in Cyber Defense Situational Analysis*. Cham: Springer International Publishing, 2017, pp. 128–169. [Online]. Available: https://doi.org/10.1007/978-3-319-61152-5_6

[11] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A tale of three security operation centers," in *Proceedings of the ACM Conference on Computer and Communications Security*, 11 2014.

[12] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth, "Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 49, 09 2005, pp. 229–233.

[13] R. Gutzwiller, S. Fugate, B. Sawyer, and P. Hancock, "The human factors of cyber network defense," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 59, pp. 322–326, 09 2015.

[14] H. J. Ofte and S. Katsikas, "Understanding situation awareness in socs, a systematic literature review," *Computers Security*, vol. 126, p. 103069, 2023.

[15] C. Zhong, J. Yen, P. Liu, and R. Erbacher, "Learning from experts' experience: Toward automated cyber security data triage," *IEEE Systems Journal*, vol. PP, pp. 1–12, 05 2018.

[16] A. Szarvák and V. Póser, "Review of using open source software for soc for education purposes – a case study," in *2021 IEEE 25th International Conference on Intelligent Engineering Systems (INES)*, 2021, pp. 209–214.

[17] J. Yen, R. Erbacher, C. Zhong, and P. Liu, "Cognitive process," *Advances in Information Security*, vol. 62, pp. 119–144, 10 2014.

[18] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *IEEE Security Privacy*, vol. 12, no. 5, pp. 35–41, 2014.

[19] A. Applebaum, S. Johnson, M. Limiero, and M. Smith, "Playbook oriented cyber response," in *2018 National Cyber Summit (NCS)*, 2018, pp. 8–15.

[20] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "A systematic method for measuring the performance of a cyber security operations centre analyst," *Computers Security*, vol. 124, p. 102959, 2023.