Building a Human-Centric SOC: A New Framework for Success

Mwangi, J., Wall, Julie ORCID logoORCID: https://orcid.org/0000-0001-6714-4867, Ismail, U. and Al-Nemrat, A. (2025) Building a Human-Centric SOC: A New Framework for Success. In: 16th International Conference on Global Security, Safety & Sustainability, ICGS3-24, 15-27 Nov 2024, Newcastle, UK.

Building a Human-Centric SOC: A New Framework for Success

John Mwangi1, Julie Wall2, Umar Ismail3 and Ameer Al-Nemrat4
University of East London, London E16 2RD, UK

Abstract. The Security Operation Centre is a hub where the Information Security Team monitors, detects, analyses, and prioritizes events from critical digital assets on an ongoing basis. The objective is to ensure that any malicious activities, indicators of attack are stopped and contained before having a major impact to an organization. Early detection is very important when trying to combat cyber threats. The Security Operation Centre is equipped with intelligent tools and skilled analysts that help detect such events. With a focus to constantly improve Security Operation Centre effectiveness, a thorough understanding of human factors and human errors that may lead to potential security breaches need to be investigated. Incorporating artificial intelligence and machine learning technologies has gone a long way to compensate for human error in the Security Operation Centre, through automation of routine tasks and incorporation within Security, Orchestration, Automation and Response. This has led to better rapid threat anomaly detection, incident response and a reduction of Security Analysts' cognitive load. That said, the existing literature suggests a lack of a systematic approach, for example in assessing Security Analysts' performance. There is a gap in the research regarding human factors and the limitations of human error within the Security Operation Centre, particularly given that it operates as a socio-technical environment where social interactions and technological systems are closely integrated. Effective collaboration, communication, and teamwork are essential in such a setting, and this research looks to further bridge that gap.

Through a case study, current practices within the Security Operation Centre will be explored from the personnel perspective. In addition, investigating transferable skills from other domains such as medical, aviation, and other sectors that manage complex environments under high stress are reviewed to determine if they offer valuable information. This paper utilizes Secure Tropos to produce the Security Operation Centre meta model. This novel approach forms the basis of a new proposed framework that looks to identify relationships and security requirements within the Security Operation Centre entity. Human centric design that accounts for human factors and human errors within the Security Operation Centre is crucial for maintaining a robust cybersecurity posture. By better understanding current practices within the Security Operation Centre, this research intends to contribute towards a more human centric approach.

Keywords: Secure Tropos Methodology, Human Factor Engineering, Security Operation Centre, Security Requirements Engineering.

1 Introduction

The 21st century has witnessed the most technologically sophisticated threats that the world has seen such that cyber security incidents have asymmetrically evolved and threats to individuals, institutions and governments are high [1]. Maintaining Confidentiality, Integrity and Availability, the CIA triad, when it comes to business data is a high priority for the majority of organizations [1]. As such, Security Operation Centres (SOC) play a crucial role in safeguarding organizations by seeking to stay ahead of cyber threats [2]. They achieve this by continuously monitoring, detecting, and responding to cybersecurity threats. Armed with intelligent tools such as Security Information and Event Management (SIEM) systems, threat intelligence feeds, and intrusion detection/prevention systems along with skilled security analysts, they help contain / stop malicious activities. This prevents data breaches, protects sensitive information, minimizing financial loss, whilst maintaining the overall security posture of an organization. Having the latest tools and advances in technology is not the only consideration to ensure the SOC remains effective. There is a social dynamic requirement as the SOC ecosystem involves teamwork, which needs clear communication and collaboration [1].

Creating an effective SOC involves drawing insights from various related works in the field [11]. Organizations often adopt established frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or International Organization for Standardization (ISO) 27001 to structure their SOC operations effectively [34]. The People, Process, and Technology (PPT) Framework is also closely as- sociated with the SOC from past research [31]. That said, this framework is not unique to the SOC and is used in various technology topics such as knowledge management [16] and customer relationship management [17], to list a few. SOC vendors within industry use this framework to summarize and structure their products and offerings. The existing PPT framework was expanded to integrate Governance and Compliance (PPTGC), elevating them from often subordinate processes to essential components within the SOC, reflecting their growing importance [5]. This framework has evolved (see Fig. 1).

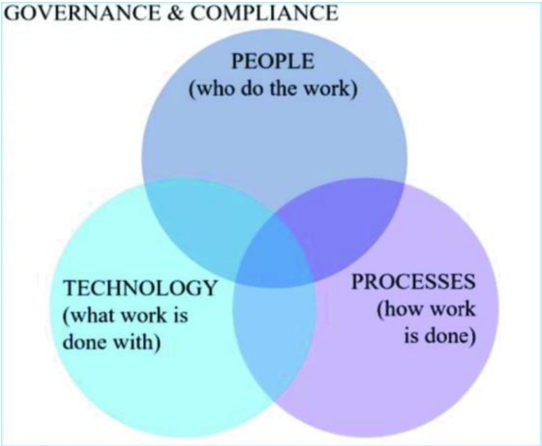


Fig 1. Extended Framework representing People, Processes, Technology, Governance and Compliance [5]

Considering humans have a major role to play within the SOC, there is currently a gap to fully understand and resolve human factor challenges. The existing frameworks such as PPT, PPTGC do not account for human factors. Our research looks to address this gap by proposing a new framework which is anchored on the Secure Tropos Methodology. As a high-stakes, high pressure environment, SOC analysts' decisions could have critical operational impact to the organization. The volume of security events that a SOC analyst analyses in a day is high. Decisions need to be made quickly as to what is a false positive or negative. They also need to factor in how much time to dedicate to these events to reduce spending valuable time investigating events of little value. Consequently, getting this evaluation wrong could lead to a breach. In 2013, the retailer ‘Target' was affected by a major cyber security breach where the SOC initially detected infiltration. However, for an unknown reason, they decided not to investigate further which consequently allowed the threat actors to execute their objective [11]. The weight of getting decisions wrong whilst playing such a crucial role may at times leave SOC analysts feeling stuck in a 'thankless task' [22]. Due to the high pressure and at times lack of information that leads to the creation of a much clearer picture of events ongoing, erroneous decisions may lead SOC analysts to make errors [23]. Also, SOC environments can contain unwittingly vicious cycles that impact morale, causing burnout thus leading to low retention of SOC analysts [22].

This paper seeks to introduce a novel approach to establishing a Human-Centric SOC that aligns with the principles of the Secure Tropos methodology [20]. By leveraging insights from human factor engineering, which looks at how people use technology, and incorporating principles that consider human limitations, ability and expectations, our model incorporates user-centred design principles to minimize errors and improve incident response.

Efficiency is paramount in SOC operations, where timely detection and response to security threats are critical [6]. Considering this, this paper looks to investigate the following hypotheses:

H1: Integrating the Secure Tropos methodology into SOCs will lead to a more comprehensive identification and prioritization of security requirements, resulting in enhanced alignment with organizational goals and improved security posture. The intention is to examine the potential benefits of integrating the Secure Tropos methodology into SOCs.

H2: The adoption of the Secure Tropos methodology in SOCs will result in more effective collaboration between security stakeholders, leading to improved communication, coordination, and implementation of security requirements. The intention is to as- sess the potential impact of implementing the Secure Tropos methodology within SOCs.

In this paper, we utilise a modelling language which is part of ongoing research to create a framework for holistically modelling a secure SOC environment, which is anchored on security requirements but also considers the roles humans play within the SOC thus creating a more human centric model. Our proposed model emphasizes automation, orchestration, and integration of security tools to streamline workflows and optimize resource utilization.

The contributions of the paper are as follows:

Human-Centric SOC Meta-Model Integration - We propose a Human-Centric SOC Meta-Model that amalgamates concepts from security requirements engineering,

human factor engineering, and the current SOC model. This meta-model serves as the foundational framework for designing and implementing security operations tailored to human behaviours and interactions within a SOC environment. By integrating human-centric considerations into the core of the SOC architecture, we aim to enhance overall security resilience by mitigating the impact of human errors and vulnerabilities.
Enhanced Definitions for SOC Environments - Our model provides comprehensive definitions for SOC concepts, relationships, and properties, with a focus on addressing the unique challenges of securing a SOC environment. These definitions encompass not only technical aspects but also human-related factors such as cognitive biases, decision-making processes, and behavioural patterns. By capturing these elements, our model enables a holistic understanding of the security landscape within SOC operations, facilitating more effective risk assessment and mitigation strategies.

By reducing manual tasks and automating routine processes, analysts can focus on high-priority threats and strategic security initiatives. In response, this paper presents a human-centric SOC model based on the Secure Tropos methodology, aiming to mitigate human errors, enhance effectiveness, and ensure privacy in multi-tenant environments. Multi-tenancy concept is explored in greater detail in the related works section. By utilizing the Secure Tropos methodology, this paper looks to extend the Secure Tropos concept within a SOC setting by identifying deeper interdependencies and relationships to better capture and analyse SOC security requirements.

The remainder of this paper is structured as follows: Section 2 describes the related work and Section 3 outlines the methodology. The proposed framework is explained in Section 4 and the results are presented and discussed in Section 5. Finally, we conclude the proposed approach and discuss future directions in Section 6.

2. Related Work

There exist two viewpoints when it comes to SOCs, industry and academic [12]. The academic viewpoint appreciates that the topic has a lot of drive from industry. There is also a lot of ambiguity within industry when referring to the SOC. That said it is important to note that there is agreement within the research community on the SOC capabilities but there is lack of consensus when it comes to what constitutes a SOC. There has been more work focusing on characteristics of the SOC without necessarily paying much attention to the overall picture. The lack of a commonly agreed holistic definition of the SOC and its composition can be a major challenge for both researchers and organizations [12]. There is a need for a commonly agreed terminology to advance the SOC research field further as lack of consensus hinders the development of efficient SOCs but also from a research point of view hinders further future innovation.

In [3], the SOC has been defined as the organizational unit at the heart of security operations. They argued that it is not a single entity or system but rather a complex structure that manages and enhances an organization’s overall security posture whose core function is to detect, analyse and respond to cybersecurity incidents and threats whilst employing PPT. However, traditional SOC models often overlook human factors, leading to inefficiencies and human errors remaining a significant challenge in cybersecurity [2]. These errors may be down to fatigue, due to the volume of security events SOC analysts deal with daily, the by-pass of processes when investigating active incidents, misalignment in configuration, and the ever-changing Tactics, Techniques, and Procedures (TTPs) that threat actors use to deliver exploits, etc. Management of human risk factors will never be 100% effective considering you can only moderate human fallibility rather than eliminate it. During a review of the aviation and medical domains, it was concluded that human rather than technical failures represented the greatest threat to complex and high-risk systems [28]. Considering the earlier definition of SOC as a complex structure [3], there is a case for comparison. The review carried out by [3] categorized errors into two groups: information-handling problems and violations (motivational problems). It also stated that different error types have different underlying mechanisms that occur in different parts of the organization and require different approaches for risk management. They also categorized mistakes as either rule-based or knowledge based. The study also looked at failures which can either be active or latent. In the medical domain, for example, active failures may be committed by people in direct contact with the patient. In contrast, latent failures, whose adverse effects may take longer to become evident, arise within the management and organizational sphere.

There is an argument that decisions made by senior management can create conditions in the workplace that subsequently promote individual errors and violations. Consequently, the likelihood of an unsafe act being committed is heavily dependent on the nature of the task and by the local workplace conditions, which in turn, are the product of "upstream" organizational factors [28]. Technology should amplify human capacity and capabilities to be creative and apply critical thinking to tasks and problems. Increasing automation helps decrease the number of mundane tasks [36, 37] by deploying tools. Automating specific tasks can also help increase operational efficiency. A counter argument by [28] states that automation and advancement in equipment is not a panacea for human factor problems as this merely relocates them. In contrast, training people to work effectively in teams incurs relatively low costs but has achieved significant enhancements of human performance within the aviation industry.

As mentioned earlier there is a lot of ambiguity when it comes to the commonly agreed holistic definition of the SOC and its composition [12]. In their research [3] sought to find the definition of the SOC, the design / architecture and its constituent parts. Their study broke the literature found into two distinct categories:

- General Aspects – This included SOC definitions, operational models and architecture.
- Building Blocks – Composition of the SOC.

From the SOC architecture perspective, three general architectural approaches applied to the SOC design were identified [3]:

- Centralized – Data is sent from different locations and subsidiaries to a central SOC for further analysis and processing [4,5].

- Distributed – Resembles a single system operating across subsidiaries [6,7]. From a user’s perspective this may appear as if dealing with one entity. Such distributed systems enable all entities to retrieve, process, combine and provide security information and services to other entities [8,9] allowing the workload and data to be spread evenly.
- Decentralized – Combines elements of both centralized and distributed design approaches [10]. A few SOCs possibly with limited capabilities report to a centralized SOC, either one or more.

From the security requirements capture perspective, it is important to map out the composition of the SOC and how each piece interacts, not forgetting the humans within the environment. Early SOC models, proposed over 15 years ago, were comprised of five modules [4, 5], which included an event generator, event collector, message database, analysis engine and reaction management software. This has moved on and there is the incorporation of digital forensics and proactive capabilities to prevent attacks in modern SOCs. For the SOC architecture, it has been suggested that this consists of a generation layer, acquisition layer, data manipulation layer and an output or presentation layer [10].

SOCs operation can be internal or external to a business [11, 12, 13, 14]. Five different operational models based on the size of organizations and authority have been proposed by [15]. These include Virtual, Large, National, Small and Tiered SOCs, which can be further clustered into four main categories; Dedicated, Virtual, Outsourced and Hybrid. Each model has advantages and disadvantages. Considerations should be made before choosing a model suitable to an organization. Factors such as company strategy, industry / sector in which the organization operates, size of organization, implementation costs, inhouse setup timescales versus outsourcing the whole service, regulations (based on sector), privacy, jurisdiction, availability requirements, management support considering the criticality of the business, integration and how well this service plugs into the existing infrastructure, and data loss concerns considering the vast amounts of data that converged in a central point for processing. It is also challenging to recruit and retain SOC experts, and all the above key points should help in determining the type of SOC an organization takes up.

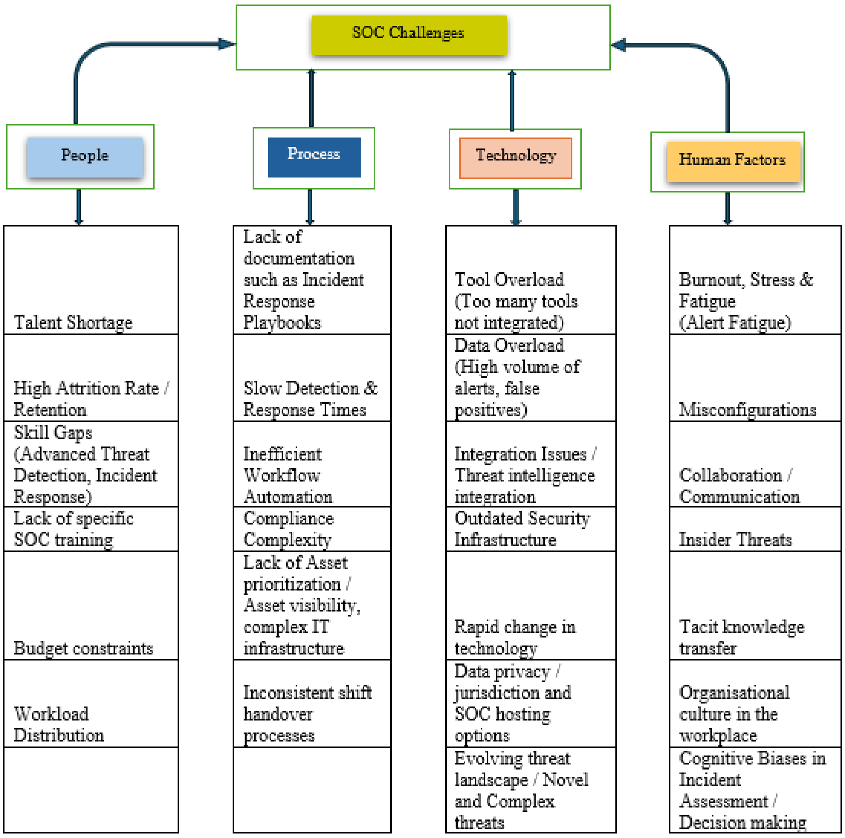
Managing security, especially in outsourced multi-tenanted environments, presents unique privacy challenges [25]. Multi-tenancy, in the context of cloud services, refers to a software architecture where a single instance of the software application serves multiple customers, or "tenants." These tenants share the same underlying infrastructure and resources while remaining isolated from each other logically. In a multi-tenant environment, each tenant typically has its own set of customizable configurations, data, and user access controls, ensuring privacy and security [20]. This approach allows cloud service providers to achieve economies of scale by efficiently utilizing resources across multiple customers while providing cost-effective services [20]. Multi-tenancy is commonly used in cloud-based Software-as-a-Service (SaaS) applications, where it enables the provider to serve a large customer base efficiently while offering scalability.

and flexibility to individual tenants. It is important to ensure segregation between tenant instances from a security and privacy perspective [20].

Multi-tenancy is mostly relevant to Managed Security Service Providers (MSSP), who offer SOC services to multiple organizations under one tenancy. Tools used to monitor these different organizations in most cases are hosted in a tenant managed by the MSSP. Even though there are technical controls in place to ensure segregation of one organization environment from the next, there are privacy risks that would need to be addressed [20]. SOC analysts within an MSSP may have access to multiple environments as part of their job when it comes to the monitoring approach. Our proposed Meta-Model looks to highlight the need to capture security requirements whilst adopting privacy-by-design principles, ensuring that sensitive data is adequately protected, and access controls are strictly enforced. Encryption, anonymization, and data segregation techniques are employed to prevent unauthorized access and mitigate the risk of data breaches across tenant boundaries.

2.1 SOC Open Challenges

The number of cyber security related breaches is on the increase, and it is thought that the number of unreported cases could be higher than the reported ones [11]. The annual cost of a cyber-attack has also risen. The mean time to detect a cyber-breach is roughly 196 days as of 2018, with a further 69 days to contain the attack, which could be seen as ineffective detection and mitigation [3]. This also demonstrates how cyber breaches can go undetected for long periods and could be an indication of how complex it can be for an organization to fully understand assets that need protecting and what technology to implement that would result in effective controls. As part of the review, this paper, along with references [11], [17], and [53], summarizes several challenges facing the SOC. Fig. 2 also includes the proposed human factor category from our research. The challenges are outlined (see Fig. 2).



People	Process	Technology	Human Factors
Talent Shortage	Lack of documentation such as Incident Response Playbooks	Tool Overload (Too many tools not integrated)	Burnout, Stress & Fatigue (Alert Fatigue)
High Attrition Rate / Retention	Slow Detection & Response Times	Data Overload (High volume of alerts, false positives)	Misconfigurations
Skill Gaps (Advanced Threat Detection, Incident Response)	Inefficient Workflow Automation	Integration Issues / Threat intelligence integration	Collaboration / Communication
Lack of specific SOC training	Compliance Complexity	Outdated Security Infrastructure	Insider Threats
Budget constraints	Lack of Asset prioritization / Asset visibility, complex IT infrastructure	Rapid change in technology	Tacit knowledge transfer
Workload Distribution	Inconsistent shift handover processes	Data privacy / jurisdiction and SOC hosting options	Organisational culture in the workplace
		Evolving threat landscape / Novel and Complex threats	Cognitive Biases in Incident Assessment / Decision making

Fig 2. Summary of SOC challenges from [11], [17], [53] and our contributions, with a focus on human factors as a critical addition to the PPT Framework

Also, the PPTGC framework [5] frames open SOC challenges into the four categories of People, Process, Technology, Governance and Compliance. This is a more logical way to consolidate and categorize to better address and look to resolve issues.

People

Challenges include a lack of understanding of how a SOC analyst decides to investigate an incident and how much time to dedicate to it [26]. Many attempts to improve efficiencies within the SOC are not informed by a decision-making theory or even input from SOC analysts [27]. Improvements seem to be derived from organisational level methods through the intervention of governance structure, interconnectivity between business units, and the delegated authority of the SOC [5]. Even though the approaches are valid without a firm understanding of the cognitive and emotional nature of the SOC role, it is difficult to ensure that analysts are best equipped to make effective decisions. This also means there is little consideration for subjective factors such as fatigue and stress that affect SOC analysts.

To address the time limitation, cyber deception technologies such as honey pots are becoming more common [25]. They could be used as a tactic to buy more time so SOC analysts can reach decisions while under less pressure. The way this works is by simulating a real environment where the threat actor reveals their intentions in a safe environment. Cyber deception technology is increasingly becoming part of an active defence toolkit as it has the potential to increase uncertainty and fear in attackers such that they make mistakes, waste resources and leak information about their TTPs [25].

There is a need to understand the link between the decision making and behaviour of both threat actor and defender. Most cyber deception research tends to build from a computer science perspective where the scope is often truncated to misdirecting a threat actor on a network rather than impacting decision making and behaviour as suggested by [25]. A study by [22], which involved training several computer science students before embedding them in three different SOCs by applying an anthropological approach, found evidence that rather than the parallel process expected in normative decisions, many SOC analysts followed a "hunch", which in most cases are accurate despite the intuitive non-analytical nature of the approach. It may also be the case that due to the highly dynamic nature of the constant evolving threats, SOC analysts rely on skilled intuition. This type of decision-making process has the characteristics of being quick and heuristics are also often highly adaptive and effective [30]. These sorts of decisions are described as Type 1. Type 2 decisions are often ‘rational’, much slower and deliberate and on some occasions less effective in contrast to Type 1 [30]. Due to the high volume of alerts that need investigating and which are mostly false positive, it would be unrealistic to assume that SOC analysts would treat these alerts equally [31]. There is a tendency to fall back to Type 1 decisions to cope with the large volume of alerts.

The application of tacit knowledge within the SOC was investigated by [32]. This is often described as knowledge that is difficult to articulate or transfer. The application of tacit knowledge can be seen in other domains such as medicine and is beneficial in expediting problem-solving procedures during an emergency response. Within an IT setting, there is a lack of understanding when it comes to tacit knowledge [32]. During post-incident review within the SOC, and especially when reviewing the Root Cause Analysis (RCA), opportunities to identify areas where tacit knowledge have been applied may come to light. Also, the best way to integrate technologies like cyber detection into established SOCs is unclear, especially since analysts rely on tacit knowledge and have developed valuable habits over time to perform their roles effectively.

The role of a SOC analyst is cognitively demanding due to the myriads of activities they are responsible for [33]. Such activities require constant monitoring of security alerts and being in a state of perpetual vigilance. To better understand the quality of alerts produced by security tools, [33] carried out a series of interviews and an online survey with 20 SOC analysts. The findings indicated that most alarms were attributed to benign triggers or events that could be explained as being legitimate within an organisational context. The downside to this, from a SOC analysts' perspective, was high levels of stress. Each alert, false positive or not, involves some level of investigation. Thus, SOC analysts risk reprimand should they misattribute an alert as benign. It is important that the tools deployed within the SOC are tuned to reduce the number of false positive detections, which would then impact the SOC analysts' cognitive load.

As for training, this may take many forms, from vendor specific for all the various tools the SOC analyst interacts with daily, to learning whilst doing the job, such as shadowing a senior or more experienced colleague. There may be a need to develop a system that models triage actions of senior analysts to aid junior colleagues dealing with similar cases [40]. Playbooks provide an overview of actions and tasks based on the experience of senior SOC analysts [41]. When it comes to training, the creation of knowledge graphs / training matrix representing domain knowledge and gaps can help focus areas that need attention [42].

Processes

Within the SOC, processes are based on a framework, such as the Incident Response Lifecycle as the main goal is to prepare and respond to incidents [43, 44, 45]. The NIST

Incident Response Lifecycle consists of four steps, “Preparation”, “Detection and Analysis”, “Containment, Eradication and Recovery” and “Post-Incident Activity”. The view on processes based on the systematic literature review from [3] is that technical steps within the Incident Response Lifecycle are dealt with intensively, whilst those surrounding them are treated sporadically, highlighting an area for further research [3]. Their observation is based on the lack of SOC specific scientific publications especially relating to “Post-Incident Activity”.

Preparation – Focuses on data collection but there is a lack of uniformity of steps composing this process [3]. As part of their investigation, [47] conducted interviews with 13 SOC professionals from 5 SOCs and concluded that SOC analysts relied on having the right toolsets to understand the data.

Detection and Analysis – A huge volume of data is collected within the SOC, and it can become overwhelming to even seasoned security experts. The focus here is to make sense of what has been collected by turning it into useful information [45]. This step also includes alert prioritization / triage, which serves two main purposes; ensuring that the most severe incidents are treated as a priority and looks at the distribution of incidents based on available resources.

Containment, Eradication and Recovery – The focus here is to stop harmful events in their tracks, then look to eradicate and recover. Several frameworks can be adopted during this stage of tackling incidents such as the Observe, Orient, Decide, Act (OODA) loop, which is an analytical framework for decision-making [48]. One could also adopt the Plan, Do, Check, Act loop [45].

Technology

Levels of data collection within the SOC vary from one organization to another depending on their scope, size, operational model, and architecture [3]. Prioritization of assets that need to act as sources of security events need to be determined prior to data collection. There is a fine balance to be struck when it comes to collecting too much or too little data to be presented to the SOC analyst. Collecting too much may impact operational efficiency, conversely collecting too little may mean malicious events are missed. Other elements that come into play include data retention, privacy, and regulations. Organizations need to determine the sensitivity of the data captured and look at ways to minimize the risk around it [3].

The integration of advanced technologies, like SIEM, SOAR (Security Orchestration, Automation, and Response), and threat intelligence platforms is crucial for enhancing SOC capabilities [18]. Critical data sources and assets must be configured to transmit security events to tools such as a SIEM [3]. These sources of data may include firewalls, Intrusion Protection Systems (IPS), Intrusion Detection Systems (IDS), antivirus software, identity and access management platforms, switches, routers, servers, or virtualized environments such as hypervisors [3]. It should be noted that people also play a major part as a data source. In the article by [49], they look at humans being employed as a sensor. In Human-as-a-Security-Sensor, [49] look at human abilities to detect anomalies, which at times are not detected by automated processes.

Governance and Compliance

Having SOC governance and compliance is key [3]. Governance is responsible for setting out the effective and efficient use of IT systems. This is achieved by providing strategic direction, which is reinforced by policies, standards, and procedures. Compliance focuses on the ability to abide by external regulations. The SOC lacks holistic standards or industry specific guidelines to help organizations to make decisions [50]. That said, the SOC can ensure that certain compliance requirements are met by following standards that focus on specific tasks [51, 52].

A SOC should have controls in place that are regularly audited to assess the current level of maturity, SOC capabilities and operational effectiveness. The Capability Maturity Matrix (CMM) is a framework for assessing the maturity of organizational process consisting of five stages: non-existent, initial, repeatable, defined process, reviewed and updated, and continuously optimized [14]. A recommendation by [19] would be to adopt this approach to assess how well SOC building blocks have been implemented.

Summary

The SOC continues to face several challenges. Key gaps identified in the review include difficulties in identifying SOC components, issues with security capture including the identification of relationships and interaction between SOC components, and challenges related to human error. Considering the SOC is a socio-technical environment where social interactions and technological systems are closely integrated, addressing human factor gaps may result in further creation of effective collaboration, communication, and teamwork, which are essential in such a setting. This paper aims to address security capture challenges using Secure Tropos and provide further insights into human error by conducting a case study.

3. Methodology

As seen in the related work section, different study methods have been used to conduct SOC research, such as semi-structured interviews, onsite visits, case studies, and ethno- graphic field work [19, 11, 53]. This project utilized two phases. A case study in phase one focused on the role human factors and human error plays within the SOC. Phase two utilized Secure Tropos to extend the PPT framework to include human factors. This novel approach in phase two provides a means for both security experts and software / system designers to better visualize and integrate security requirements as part of the SOC design process. Other frameworks such as PPT, do not offer the same level of visualization achieved through the creation of a meta-model. Visualization through meta-models, which can be further decomposed to reveal detailed interactions between various entities, appears to be a more effective approach for creating deeper understanding of the SOC environment. The proposed framework focuses on ensuring that the human factors, are accounted for and central to the architecture's design, with security needs embedded into every layer of the SOC ecosystem.

The Secure Tropos methodology, as a concept, refers to a high-level abstraction used to represent recurring patterns or structures within the system being modelled [4]. Concepts help to simplify the modelling process by capturing common characteristics and relationships among elements in the system. They provide a way to modularize and organize the system's components, making it easier to analyse and reason about the system's behaviour and security requirements. Concepts can include various elements such as actors, agents, goals, dependencies, capabilities, trustworthiness, security requirements, threats, attacks, and countermeasures [20]. These concepts are used to model the system's architecture, interactions, and security aspects, enabling stakeholders to understand and address security concerns throughout the development process.

The Secure Tropos methodology is used in software development and requirements engineering and extends the Tropos Framework by incorporating security consideration into the early stages of software development. The Secure Tropos methodology focuses on developing secure software solutions by considering and incorporating security from the onset ensuring it is not an afterthought that gets bolted on at the end [21]. It provides the ability to define and identify high level goals and ways to further secure systems from external threats. The additional benefit for our proposed model is that it can be adopted to review existing SOC deployments as part of a risk-based continuous assessment lifecycle but also review how new tools deployed to the SOC would affect the overall posture. Secure Tropos is also used to identify relationships and security requirements within the SOC entity by generating a Meta-Model. Lucid Chart, which has a Unified Modelling Language (UML) module, is also used in the production of the Meta-Model proposed in this paper.

Secure Tropos, which can be used to identify security constraints, is an Actor (agent) oriented methodology that can be used to identify and model different actors and how they interact with the solution or system under development [21]. Actors can be systems, organisations, or humans. It delves deeper into understanding the dependencies on actors and the goals, they are looking to achieve. These goals can relate to functionality, security, or other aspects of the solution or system. Our approach takes on the “social perspective” by considering the involvement of humans and their organisational behaviours and the social phenomenon around them. It is an approach that focuses on security concerns and issues that might affect systems security. Security assets are resources used to protect against concerns. Through modelling, Secure Tropos also allows configuration of security policies and rules that govern how systems should behave to ensure security. Traceability and risk assessment are also included where developers can trace, for example, security goals and requirements back to the processes and actors they originated from. Identification of risk and prioritisation is handled via risk management. As security needs regular revaluation rather than a onetime concern, Secure Tropos supports this approach by being incremental and iterative during the development cycle.

For a qualitative survey, [55] suggest a range of (4-50) participants due to the volume of data collected and the appropriateness of participants based on their knowledge of the research topic. Considering this, our study utilised a mix of 6 experts and SOC analysts. For the case study, we utilized a qualitative research design consisting of an online questionnaire sent out to 15 SOCs within the UK targeted at Subject Matter Experts (SMEs) from industry. Questions included a mixture of closed and open-ended questions. The questions aimed to elicit an understanding of current SOC practices and how human factors have affected SOC effectiveness. The average time to complete the questionnaire was 47 min (min: 27, max: 57). Ethical approval for this research was provided by the University of East London Ethics Committee. The participants represented various roles within a SOC, MSSPs providing services to both public and private organizations. We believe this provided a solid breadth of perspectives in our sample.

4. Proposed Extended PPT Framework

This section introduces the proposed mapping for a Human-Centric SOC in the context of the Secure Tropos methodology. Based on our research and on the literature review, the following Secure Tropos constructs, and terminology have been identified as essential. Table 1 outlines the language and constructs derived from Secure Tropos, such as actors, relationships, and goals. Table 2 outlines each agent or entity with specific goals to accomplish, detailing their characteristics and relationships with other agents. Table 3 details the dependencies between each agent and other agents, while Table 4 outlines various risks identified in a SOC environment and their corresponding mitigation strategies.

To effectively structure SOC operations, our proposed framework adopts an approach similar to NIST, with particular emphasis on considerations starting from the design phase, as highlighted in the introduction section when describing incident handling. Our proposed framework consists of the following stages / levels with an anchor to Secure Tropos Methodology.

Conceptual – Similar to what we have covered in this research, this stage involves the proposing or describing the entire ecosystem of SOC and identifying what is in SOC. This also includes the capture of the composition of SOC operations ensuring SOC resources (Analysts, Managers etc) understand SOC boundaries and any limitations that may be present.

Logical – This stage involves the creation of the Meta model (see Fig. 3) identifying the relationships between People, Process, Technology and Human Factors interacting with each other.

Implementation – This stage looks to address technical elements that enhance the effectiveness of SOC operations. This could be the implementation of different technologies can be used to enhance the SOC operations. It also includes for instance the use of Artificial Intelligence and Machine Learning techniques in detection, monitoring and event analysis. Other considerations that facilitate the implementation of a human centric SOC such as gamification which ensures SOC Analysts remain engaged when investigating events are implemented here.

Validating this new framework may take several forms such as seeking expert opinion, conducting a SOC Maturity Assessment using similar frameworks such as NIST, reviewing Key Performance Indicators (KPI) and other Metrics. As part of future research, our model could go through further validation by extending it use to a wider audience.

Table 1. Secure Tropos Terminology (Language and Constructs) for SOC.

Category	Element	Description
Language	Goals	Objectives that agents aim to achieve.
	Tasks	Specific activities that agents perform to achieve goals.
	Resources	Assets and capabilities required by agents to accomplish tasks and achieve goals.
	Agents	Entities (individuals, groups, or systems / software components) that have goals and perform tasks.
	Actors	A subset of agents, typically referring to people or groups, / software components within the SOC.
	Relationships	Interactions or dependencies between agents, tasks, and resources.
	Constraints	Conditions and limitations that affect how tasks are performed, or goals can be achieved.
	Risks	Potential events or conditions that could prevent achieving goals or performing tasks effectively.
	Mitigations	Strategies or actions taken to reduce risks.
Constructs	Goal Models	Illustration of goals of SOC agents and the tasks required to achieve them.
	Actor Mapping	Visual representations of SOC agents, their roles, and their relationships.
	Relationship Mapping	Illustrations of how SOC agents depend on each other for resources, tasks, and goal achievement.
	Risk Models	Table outlining potential risks and mitigations.

Table 2. Goal Models - Description of Agents, Their Characteristics, Goals, and Relationships

Agent	Characteristics	Goals	Relationships
Security Analysts	Skilled in threat detection and response, continuously trained, work under high pressure	Efficiently detect and respond to security incidents, minimize false positives, maintain situational awareness	Collaborate with IT staff, communicate with management, utilize tools and threat intelligence, and monitor end-user activities, share threat intelligence with external partners.
IT Staff	Technical expertise in infrastructure management, responsible for implementing security controls	Maintain and secure IT infrastructure, ensure seamless operation of security tools, support SOC operations	Support security analysts, manage hardware and software assets, interact with cloud providers, report infrastructure status to management, maintain tools.
Management	Strategic oversight, responsible for resource allocation, ensure compliance with regulations	Oversee SOC effectiveness, align SOC activities with business goals, ensure regulatory compliance, allocates resources	Communicate with analysts and IT staff, make decisions based on SOC reports, interact with external auditors, and provide training to end-users.
External Partners	Provide specialized expertise, threat intelligence, and incident response support	Enhance SOC capabilities, offer additional resources and knowledge, assist in incident response	Share threat intelligence with SOC, assist in incident response, provide external audits, collaborate with management on compliance assessments.
End-Users	Employees whose activities are monitored for security, potential internal threat vector	Perform their job functions securely, adhere to security policies, increase security awareness, reports anomalies	Receive training and awareness programs from management, follow security guidelines set by SOC, report anomalies to security analysts.
Threat Actors	Individuals or groups with malicious intent, constantly evolving tactics	Exploit vulnerabilities, disrupt operations, steal data	Adversarial relationship with SOC, targeted by threat modelling and defence mechanisms, pose risks that SOC mitigates through continuous monitoring and response strategies.

Table 3. Dependency Graph - Identifying SOC Dependencies

Agent	Dependency
Security Analysts	Depend on IT Staff for infrastructure support and tools maintenance, depend on Management for strategic direction and resources.
IT Staff	Depend on Management for resource allocation, depend on Security Analysts for feedback on tool effectiveness.
Management	Depend on Security Analysts for incident reports and metrics, depend on IT Staff for infrastructure status.
End-Users	Depend on Management for training and awareness programs, depend on Security Analysts for incident response.

Table 4. Risk Models – SOC Risks and Mitigations

Risk	Description	Mitigation
Human Error	Mistakes made by SOC staff or end-users that could lead to security breaches.	Regular training and awareness programs, automated checks, and balances.
Burnout	High stress levels leading to decreased performance among security analysts.	Implement stress management strategies, rotate shifts, provide mental health resources.
Evolving Threats	Constantly changing tactics by threat actors.	Continuous threat intelligence updates, regular training, adaptive security measures.
Resource Shortage	Insufficient resources (staff, tools, budget) to maintain SOC operations.	Strategic resource allocation by management, prioritize critical operations, leverage external partnerships.

Fig 3 represents the proposed extended PPT Framework. We used Lucid chart to produce the Meta-Model, which details the composition, interactions and checks to ensure CIA is maintained. The diagram also shows key considerations, which can further decompose into their own topics. For example, under “Technology”, it is important to consider where hosting takes place. Is this in the cloud or on premise? What sort of risks are present with the options chosen and how does that impact privacy concerns. Other considerations, such as the location of where business data will reside / jurisdiction and regulations are also key.

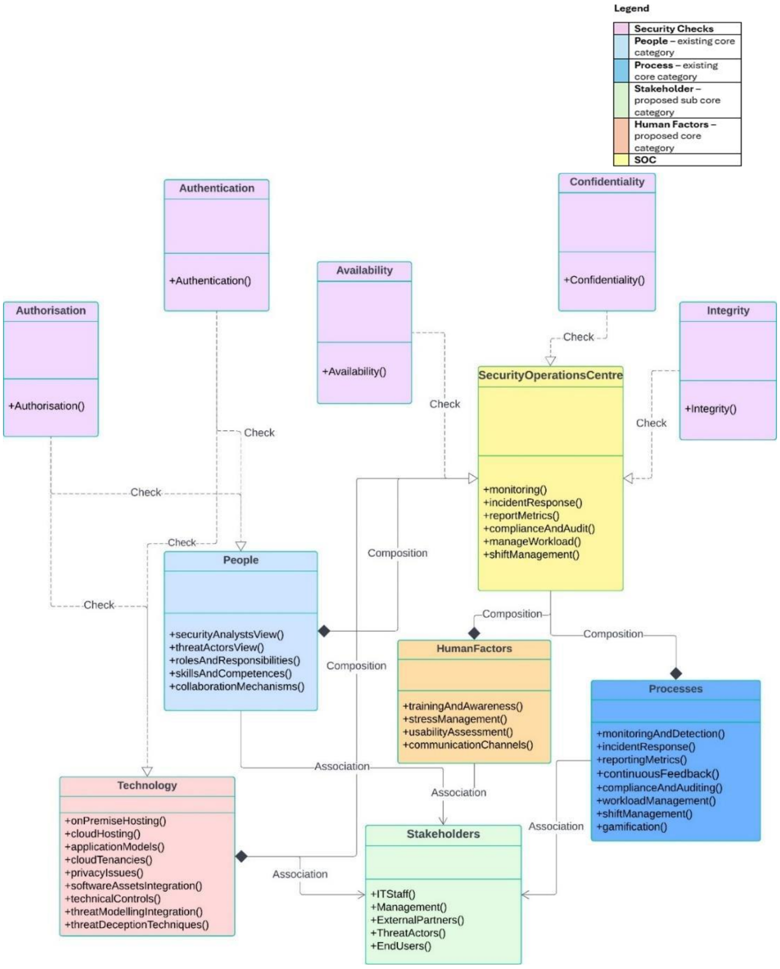


Fig 3. Proposed Extended Framework representing People, Processes, Technology, and Human Factors

5. Results and Discussion

R Studio's Text Mining module was used to qualitatively analyse the case study results. A sample of some of the questions posed during this study included "In your opinion, what are the primary causes of human errors in the SOC?". It was clear that some SOC analysts felt pressure was one of the contributors for human error. Pressure was either associated with a rush to close tickets, which also led to steps in set processes being skipped or having to deal with a huge volume of security events which needed analysing quickly. Figure 4 displays the feedback following this question.

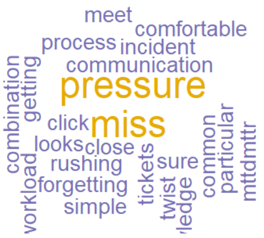


Fig 4. Question response displayed using word cloud.

When asked "How effective is the communication and coordination processes within the SOC in preventing human errors?", some analysts felt it was not effective.

❝ Not very effective (communication need improvement). ❞
~ SOC Analyst

We also asked, "Are there any specific tasks or activities within the SOC that are more prone to human errors?". Event analysis and response was highlighted predominantly due to the volume of events that each analyst was dealing with daily.

❝ Event analysis & response (Situational Awareness) ❞
~ SOC Analyst

A question on shift patterns revealed that half the respondents had an equal mix of days and nights. A third were mostly on day shift and the remainder had a broad range of activities to support the team and provide continuity between shifts in periods of absence. When it came to handing over from one shift to another, results revealed different SOCs approach this differently, with one SOC outlining high priority security events during the shift and the customers that were affected. Other used email with bullet points. It was also evident from the response for time allocated for shift handover, that not all SOCs had dedicated slots with one response indicating:

❝ There is no set time, this can be different from day to day. ❞
~ SOC Analyst

Based on the case study results, a SOC would benefit from having a protected slot for handover with a clear set of processes and procedures on how and what needs to be covered during the handover, ensuring the transfer of responsibility is clear from one shift to the next. This is also in contrast if compared to the medical and aviation industries. Results from the case study indicated that the SOCs were conducting training on tools they used. Also, SOC analysts were learning from past events. Where appropriate and available they were utilising automation to try and reduce human error.

After implementing the Secure Tropos methodology to address current challenges facing the SOC, our proposed framework could offer significant improvements across key areas such as the capture of security requirements during the design stage of the SOC but also conducting assessments on existing SOC deployments. The adoption of Secure Tropos creates a proactive approach to threat mitigation, enabling SOC teams to identify and address potential threats more effectively through dynamic threat modelling and automated security controls. This is in support of the hypotheses H1 and H2 as described in the introduction section. Moreover, Secure Tropos promotes visualisation, identification of clear goals, objectives and relationships, collaboration and communication among SOC stakeholders, leading to improved coordination and alignment of security initiatives with organizational goals. This enhanced collaboration enhances overall efficiency and effectiveness within the SOC. Additionally, the methodology facilitates the efficient capture and integration of security requirements into SOC operations, ensuring that security efforts are prioritized based on their impact on security posture and organizational objectives. Overall, the findings underscore the effectiveness of Secure Tropos in enhancing SOC capabilities and strengthening an organization's overall security posture.

6. Conclusion

The proposed Human-Centric SOC model offers a comprehensive framework for enhancing security within the SOC. Extending Secure Tropos concepts and creating a detailed view of the relationships between components provides a better understanding. By integrating human factor engineering, efficiency enhancements, and privacy considerations within the Secure Tropos methodology, organizations can establish resilient and effective security operations tailored to the needs of diverse stakeholders. This paper has also shown the importance of addressing the human element within the SOC as reliance on technology alone cannot resolve the existing issues. It is important to address social dynamic requirements within the SOC ecosystem as it involves teamwork, which also needs clear communication and collaboration between different groups.

This paper proposed to explore the development of a human-centric SOC that would integrate human factors and security requirement factor engineering while using the Secure Tropos methodology. This study faced minor limitations and challenges which included the complexity of integrating multidisciplinary concepts such as human factor engineering, limited prior research in human factors engineering within the SOC, and the need for long-term evaluation, which can be an area of future development. Despite these limitations, addressing these challenges could lead to significant improvements in SOC design and security outcomes, underscoring the importance of navigating these limitations effectively to ensure the validity and practicality of the research findings. Tailored to the needs of diverse stakeholders. Our model would also be useful in evaluating established SOCs, considering it is adopted to a risk-based continuous assessment approach. Without time limitation our study could benefit from wider worldwide engagement for further validation. This could be achieved in the future. The following areas have also been identified as potential topics for future research in the SOC context; tacit knowledge transfer, SOC specific training methods, targeted data collection and the utilisation of data protection techniques such as anonymization and pseudonymization.

7. References

1. Tetrick, L.E., Pfleeger, S.L. and Horne, W.G. (2024) GMU Cybersecurity Incident Response Team Social Maturity Handbook updated 10.20.16, Scribd. Available at: https://www.scribd.com/document/527834317/GMU-Cybersecurity-Incident-Response-Team-Social-Maturity-Handbook-Updated-10-20-16 (Accessed: 01 September 2024).
2. Robinson, N. (2023) ‘Human Factors Security Engineering: The future of cybersecurity teams’, EDPACS, 67(5), pp. 1–17. doi:10.1080/07366981.2023.2211429.
3. Vielberth, M., Bohm, F., Pernul, G. and Fichtinger, I., 2021. Security Operations Center: A Systematic Study and Open Challenges. [online] Ieeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/document/9296846> [Accessed 2 September 2024].
4. R. Bidou, J. Bourgeois and F. Spies, "Towards a global security architecture for intrusion detection and reaction management" in Information Security Applications, Berlin, Germany:Springer, vol. 2908, pp. 111-123, 2004.
5. Shahjee, D., and Ware, N. (2022). Integrated network and security operation center: a systematic analysis. IEEE Access 10, 27881–27898. doi: 10.1109/ACCESS.2022.3157738
6. A. Karim Ganame, J. Bourgeois, R. Bidou and F. Spies, "A global security architecture for intrusion detection on computer networks", Comput. Secur., vol. 27, no. 1, pp. 30-47, Mar. 2008.
7. J. Bourgeois and R. Syed, "Managing security of grid architecture with a grid security operation center", Proc. Int. Conf. Secur. Cryptogr., pp. 403-408, 2009.
8. R. H. Syed, J. Pazardzievska and J. Bourgeois, "Fast attack detection using correlation and summarizing of security alerts in grid computing networks", J. Supercomput., vol. 62, no. 2, pp. 804-827, Nov. 2012.
9. R. H. Syed, M. Syrame and J. Bourgeois, "Protecting grids from cross-domain attacks using security alert sharing mechanisms", Future Gener. Comput. Syst., vol. 29, no. 2, pp. 536-547, Feb. 2013
10. N. Miloslavskaya, A. Tolstoy and S. Zapechnikov, "Taxonomy for unsecure big data processing in security operations centers", Proc. IEEE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW), pp. 154-159, Aug. 2016.
11. F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, et al., "Matched and mismatched SOCs", Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 1955-1970, Nov. 2019.
12. Chamkar, S.A., Maleh, Y. and Gherabi, N. (2022) ‘The human factor capabilities in security operation center (SOC)’, Advances in Information, Communication and Cybersecurity, pp. 579–590. doi:10.1007/978-3-030-91738-8_53.
13. D. Forte, "An inside look at security operation centres", Netw. Secur., vol. 2003, no. 5, pp. 11-12, 2003.

14. P. Jacobs, A. Arnab and B. Irwin, "Classification of security operation centers", Proc. Inf. Secur. South Afr., pp. 1-7, Aug. 2013.
15. C. Zimmerman, "Ten strategies of a world-class cybersecurity operations center", 2014.
16. G. D. Bhatt, "Knowledge management in organizations: Examining the interaction between technologies techniques and people", J. Knowl. Manage., vol. 5, no. 1, pp. 68-75, Mar. 2001.
17. J. Bourgeois, A. Ganame, I. Kotenko and A. Ulanov, "Software environment for simulation and evaluation of a security operation center" in Information Fusion and Geographic Information Systems, Berlin, Germany:Springer, pp. 111-127, 2007
18. B. Hámornik and C. Krasznay, "A team-level perspective of human factors in cyber security: Security operations centers" in Advances in Human Factors in Cybersecurity, Cham, Switzerland:Springer, vol. 593, pp. 224-236, 2018.
19. S. Schinagl, K. Schoon and R. Paans, "A framework for designing a security operations centre (SOC)", Proc. 48th Hawaii Int. Conf. Syst. Sci., pp. 2253-2262, Jan. 2015.
20. Mouratidis, H., Shei, S. and Delaney, A. (2019) 'A security requirements modelling language for cloud computing environments', Software and Systems Modeling, 19(2), pp. 271–295. doi:10.1007/s10270-019-00747-8.
21. Salnitri, M. et al. (2019) 'Modelling the interplay of security, privacy and trust in Sociotechnical Systems: A computer-aided design approach', Software and Systems Modeling, 19(2), pp. 467–491. doi:10.1007/s10270-019-00744-x.
22. S. Sundaramurthy, "An anthropological study of security operations centers to improve operational efficiency", 2017.
23. Schinagl, S., Schoon, K., and Paans, R. (2015). A framework for designing a security operations Centre (SOC). In: Paper Presented at the 2015 48th Hawaii International Conference on System Sciences.
24. Plachkinova, M., and Maurer, C. (2018). Security breach at target. J. Inf. Syst. Educ. 29, 11–20.
25. Ashenden, D., Black, R., Reid, I. D., and Henderson, S. (2021). Design thinking for cyber deception. In Paper Presented at the 54th Hawaii International Conference on System Sciences, Hawaii.
26. Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., and Doupé, A., & Ahn, G.-J. (2019). Matched and mismatched SOCs: a qualitative study on security operations center issues. In: Paper presented at the Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, United Kingdom.
27. Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., and Brummel, B. J. (2022). Organizational science and cybersecurity: abundant opportunities for research at the interface. J. Bus. Psychol. 37, 1–29. doi: 10.1007/s10869-021-09732-9
28. Reasons, J. "Understanding adverse events: human factors.", Proc. 48th Hawaii Int. Conf. Syst. Sci., pp. 2253-2262, Jan. 2015.
29. Reeves, A., Delfabbro, P., and Calic, D. (2021). Encouraging employee engagement with cybersecurity: how to tackle cyber fatigue. SAGE Open 11:215824402110000. doi: 10.1177/21582440211000049
30. Kahneman, D., and Klein, G. (2009). Conditions for intuitive expertise: a failure to disagree. Am. Psychol. 64, 515–526. doi: 10.1037/a0016755
31. Feng, C., Wu, S., and Liu, N. (2017). A user-centric machine learning framework for cyber security operations center. In Paper presented at the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI).
32. Cho, S. Y., Happa, J., and Creese, S. (2020). Capturing tacit knowledge in security operation centers. IEEE Access 8, 42021–42041. doi: 10.1109/access.2020.2976076

33. Alahmadi, B., Axon, L., and Martinovic, I. (2022). 99% false positives: a qualitative study of SOC analysts' Perspectives on security alarms. Paper presented at the 31st USENIX security symposium, Boston, MA, United States.
34. N. Miloslavskaya, "Security intelligence centers for big data processing", Proc. 5th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW), pp. 7-13, Aug. 2017.
35. Strategies for Building and Growing Strong Cybersecurity Teams: Cybersecurity Workforce Study, Clearwater, FL, USA, 2019.
36. C. Islam, M. Babar and S. Nepal, "Automated interpretation and integration of security tools using semantic knowledge" in Advanced Information Systems Engineering, Cham, Switzerland:Springer, vol. 11483, pp. 513-528, 2019.
37. Y. Kanemoto, K. Aoki, M. Iwamura, J. Miyoshi, D. Kotani, H. Takakura, et al., "Detecting successful attacks from IDS alerts based on emulation of remote shellcodes", Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC), pp. 471-476, Jul. 2019.
38. Wiegmann, D.A. and Shappell, S.A. (2017) 'Human error perspectives', A Human Error Approach to Aviation Accident Analysis, pp. 20–44. doi:10.4324/9781315263878-2.
39. T. Sander and J. Hailpern, "UX aspects of threat information sharing platforms", Proc. 2nd ACM Workshop Inf. Sharing Collaborative Secur., pp. 51-59, 2015.
40. C. Zhong, T. Lin, P. Liu, J. Yen and K. Chen, "A cyber security data triage operation retrieval system", Comput. Secur., vol. 76, pp. 12-31, Jul. 2018.
41. A. Applebaum, S. Johnson, M. Limiero and M. Smith, "Playbook oriented cyber response", Proc. Nat. Cyber Summit (NCS), pp. 8-15, Jun. 2018.
42. A. Pingle, A. Piplai, S. Mittal, A. Joshi, J. Holt and R. Zak, "Relext: Relation extraction using deep learning approaches for cybersecurity knowledge graph improvement", Proc. IEEE/ACM Int. Conf. Adv. Soc. Netw. Anal. Mining, pp. 879-886, 2019.
43. A. Chin-Ching Lin, H.-K. Wong and T.-C. Wu, "Enhancing interoperability of security operation center to heterogeneous intrusion detection systems", Proc. 39th Annu. Int. Carnahan Conf. Secur. Technol., pp. 216-221, 2005.
44. M. Nabil, S. Soukainat, A. Lakbabi and O. Ghizlane, "SIEM selection criteria for an efficient contextual security", Proc. Int. Symp. Netw. Comput. Commun. (ISNCC), pp. 1-6, May 2017.
45. M. H. Khyavi, "Isms role in the improvement of digital forensics related process in soc's", arXiv:2006.08255, 2015, [online] Available: https://arxiv.org/abs/2006.08255.
46. Guest, G., Bunce, A. and Johnson, L. (2006) 'How many interviews are enough?', Field Methods, 18(1), pp. 59–82. doi:10.1177/1525822x05279903.
47. R. Bridges, M. Iannacone, J. Goodall and J. Beaver, "How do information security workers use host data? A summary of interviews with security analysts", arXiv:1812.02867v1, 2018, [online] Available: https://arxiv.org/abs/1812.02867.
48. F. Osinga, Science Strategy and War: The Strategic Theory of John Boyd, London, U.K.:Routledge, 2007.
49. M. Vielberth, F. Menges and G. Pernul, "Human-as-a-security-sensor for harvesting threat intelligence", Cybersecurity, vol. 2, no. 1, pp. 35, Dec. 2019.
50. J. R. Goodall, E. D. Ragan, C. A. Steed, J. W. Reed, G. D. Richardson, K. M. T. Huffer, et al., "Situ: Identifying and explaining suspicious behavior in networks", IEEE Trans. Vis. Comput. Graphics, vol. 25, no. 1, pp. 204-214, Jan. 2019.
51. C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy", Proc. Int. Conf. Cyber Situational Awareness Data Analytics Assessment (CyberSA), pp. 1-10, Jun. 2015.

52. N. Miloslavskaya, "SOC-and SIC-based information security monitoring" in Recent Advances in Information Systems and Technologies, Cham, Switzerland:Springer, vol. 570, pp. 364-374, 2017.

53. D. Crémilleux, C. Bidan, F. Majorczyk and N. Prigent, "Enhancing collaboration between security analysts in security operations centers" in Risks and Security of Internet and Systems, Cham, Switzerland:Springer, vol. 11391, pp. 136-142, 2019.

54. Jacobs, P. Arnab, A. and Irwin, B. 2013. "Classification of Security Operation Centers," Information Security for South Africa, pp. 1-7, doi: 10.1109/ISSA.2013.6641054

55. Quick, J. and Hall, S. (2015) 'Part Two: Qualitative research', Journal of Perioperative Practice, 25(7–8), pp. 129–133. doi:10.1177/1750458915025007