IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 26, 2019, accepted January 21, 2020, date of publication February 24, 2020, date of current version March 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2976076

Capturing Tacit Knowledge in Security Operation Centers

SELINA Y. CHO[1], JASSIM HAPPA[2], AND SADIE CREESE[1]
[1]Department of Computer Science, University of Oxford, Oxfordshire OX1 3PR, U.K.
[2]Information Security Group, Royal Holloway, University of London, Egham TW20 0EX, U.K.

Corresponding author: Selina Y. Cho (selina.cho@cs.ox.ac.uk)

This work was supported in part by the New College, University of Oxford, and in part by the FS-ISAC EMEA BCD Scholarship.

ABSTRACT The use of tacit knowledge has previously been shown to help expedite problem-solving procedures in the setting of medical emergency responses, as individuals can use past experiences in present and future challenges. However, there is a lack of understanding in its application in IT and socio-technical management. This paper examines the thought processes observed in Security Operational Centre (SOC) analysts facing threat events to lay the groundwork for tacit knowledge management in SOCs. Based on Sternberg's fieldwork in tacit knowledge, we conducted semi-structured interviews with ten analysts to explore the key artefacts and individual traits that aid their approach to communication, and to examine the thought processes under hypothetical incident handling scenarios. The results highlight a unanimous pursuit of Root Cause Analysis (RCA) upon the outbreak of an incident and stages of decision-making when escalating to third party support providers. Using Business Process Modelling and Notation (BPMN), we show the procedural elements of tacit knowledge from several scenarios. The results also suggest that simulation environments and physical proximity with analysts and vendors can facilitate the transfer of tacit knowledge more effectively in SOCs.

INDEX TERMS Communication theory, DIKW, incident response, knowledge management, security operation center, sense-making, tacit knowledge.

I. INTRODUCTION

Tacit knowledge is a type of knowledge, insight, and intuition that comes from years of experience. It is influenced by an individual through means such as the human intelligence, sensorial experience [1] and the cultural background which facilitates the process of digesting new information. A person may learn to better tackle a problem at hand from experiences by adopting strategies that had been used before, and thereby saving both time and effort.

Security Operation Centres (SOC) house a team to monitor, detect and react to security threats across company networks [2]. An effective SOC establishes real-time interaction and coordination between people, technology, and processes to respond against threats. Through experience, analysts develop an ability to prioritise threats, which enables them to make faster and more effective decisions when containing the attacks. The challenge in capturing tacit knowledge is that over time it becomes harder for an experienced analyst to articulate, or even recognise, the precise expertise underpinning decision-making processes as one's tacit knowledge inherently exceeds what can be expressed [1], [3]. Without means to externalise or transfer implicit knowledge to others, much of knowledge remains unused.

To understand the different dimensions of tacit knowledge and its relevance in streamlining work processes, it is necessary to analyse thought processes that are triggered by incidents as a way to understand the style and chronological flow of thinking. Our paper provides a basis from which SOCs can improve their incident handling capabilities and capacities through tacit knowledge management. For new analysts, a lack of context renders the overall communication redundant or incomprehensible at the initial detection phase of threats, and may delay the containment process. Different analysts end up prioritising different tasks, causing them to either dismiss or investigate too much on a case that has already been explored by someone else in the past.

A. OBJECTIVE

In a SOC, an analyst's familiarity with a task can be much more informative than the insight of many novices,

The associate editor coordinating the review of this manuscript and approving it for publication was Lu An.

especially given the limited span of time. Novices may use heuristics and brute force to understand their problems, whereas experienced analysts may know the answer to these problem almost immediately. This makes tacit knowledge a valuable and underexplored topic of research for the organisations, even well beyond the SOC context, and calls for a need to understand what dimensions of tacit knowledge exist from a more granular level of every day experiences and encounters of people, artefacts, and incidents. Clarifying the case-specific incident response strategies can promote a more succinct and time-efficient communication across a team of experienced and new analysts. By learning strategies used by established experts and understanding the environment better, new incoming set of talents more easily transition into the niche field that require years of hands-on experience.

Based on the tacit knowledge fieldwork by Sternberg [4], this study uses semi-structured, in-person interviews and case scenarios to garner the underlying tacit dimensions of analysts, tasks, and communication media. It aims to achieve so by primarily exploring different forms of thought processes that occur among analysts when an incident breaks out. The threat scenarios are used to enquire the analysts on the initial line of actions and procedures that would be undertaken in response to detecting an incident, in order to be able to understand their flow of conceptualising the incident. Further, the interview questions probe for general sentiments regarding current state of the knowledge transfer mediums that affect the operation, and the real-life examples the analysts had previously encountered. The study aims to investigate how tacit knowledge can be externalised and transferred to others by studying existing communication and operational mediums and challenges.

B. RESEARCH QUESTIONS

This research builds on the assumption that an individual's thought process develops from their tacit knowledge and experience – professional, academic, and personal. It also builds on the assumption that senior analysts have accumulated tacit knowledge over time that novice analysts do not possess. Probing the analysts on their perception and background in incident response cases will allow one to use the observation as a foundation to understanding implicit knowledge present specifically in SOCs, an area that had not previously been addressed in this aspect. The research aims to answer the following questions:

1) *Are there any identifiable patterns in thought processes between analysts with similar academic or professional experience?*
2) *Do analysts prioritise incidents based on principles or social factors?*
3) *Do media exist in communicating threat and defence knowledge?*
4) *What are the desirable traits of an effective SOC analyst?*

Question 1 sets out whether analysts with similar academic or professional backgrounds think alike. Questions 2 and 3 aims to address which factors, principles, and artefacts play a role in one's prioritisation and task-solving skills. Question 4 asks attributes that are to be most desirable in new SOC analysts, given that they lack the same insight and experience. Probing the perception of experienced analysts can reveal the valuable personal traits that had previously been helpful in appropriately handling incidents.

C. PAPER CONTRIBUTIONS

This study investigates the aforementioned research questions through observation of how given threat scenarios are perceived differently by each analyst, and enquiring how one communicates, utilises and absorbs new knowledge from past encounter with analysts and clients, office artefacts, experience. The focus of the investigation is not so much on whether one's choice is more effective than another, but understanding whether choices differ at all and, if so, the influencing factors behind such choices. Specifically, the core contributions of this paper are:

- **An in-depth analysis of current SOC practices** from semi-structured interviews with ten mid to senior-level SOC analysts.
- **An investigation on generalising tacit knowledge of incident response** based on the interview findings and Business Process Modelling and Notation.
- **An in-depth discussion on the applications and limitations of tacit knowledge** in SOCs.
- **A list of recommendations** for this field of study.

II. TACIT KNOWLEDGE IN ORGANISATIONS

A. TACIT KNOWLEDGE AS A CONCEPT

Tacit knowledge is commonly associated with cognitive skills such as subjective insights, intuition [5], and mental models [6], as well as "*know-hows*" or skills gained through repeated exposure to hands-on work [7]. Without the corresponding context, the holder of the tacit knowledge may not even be aware of the existence of such knowledge. Capturing tacit knowledge in either a written or verbal form is thus a challenge. Explicit knowledge on the other hand is any objective or rational knowledge that can be expressed in a variety of context-free formats such as words, sentences, numbers, or formulas. The nebulous boundaries of what constitutes a tacit knowledge in each context, and thereby how one can measure and record it as explicit knowledge, has been a challenge in both academia and industry [8], [9].

The notion of tacit knowledge is often attributed to Michael Polanyi who first explored the impact of personal experience in human knowledge [1], [10]. Polanyi claims all creative thoughts and knowledge, including those based on mathematical logic, relies on personal feelings, judgements, and commitments. He depicted a pre-logical phase of knowledge which comprised a range of sensorial or conceptual information that are brought together by an individual to fully digest an information and become aware of its meanings in depth [11]. Because of the fundamental cognitive features embedded in the newly acquired knowledge, which are

intangible and out of plain sight, he claimed that ''*we know more than we can tell*''. Schacter notes that for such knowledge to be made accessible, there has to be a degree of ''encoding'' and retrieval procedure made available that help relate to the previously established representations [12].

Nonaka extended the concept [13], [14] by incorporating it into an organisational framework, and explored how employees can share knowledge in a work setting. He, along with several other researchers around the time [3], [15], [16], claimed that implicit, or tacit, and explicit learning are not completely separate, and that they are part of an interactive or cooperative process in continuity, which ultimately produces appropriate knowledge for an organisation. Nonaka also distinguished tacit knowledge as those that can either be codifiable – i.e. convertible to explicit knowledge - or not codifiable. Based on the Japanese concept of *ba* [14], he emphasised the importance of a shared space – whether physical, virtual, or mental – and socialisation in it as a means to converting tacit knowledge into more explicit forms.

The cross-cultural perspective from the two major pioneers of knowledge management provides a multifaceted understanding of the nature of tacit knowledge. Due to the variety of contexts in which it can be applied, the term tacit knowledge is at times inadequately referred to as any kind of knowledge that cannot be formally recorded. Hazel [17] offers an aggregate summary of tacit knowledge conceptualisations that has been offered so far by different authors.

B. KNOWLEDGE GENERATION

Tacit knowledge is acquired as an individual engages in first-hand experience, during which one observes and learns the skills needed to accomplish a task [4]. In business, tacit knowledge can be produced either from tools, environments, personal relations or social institutions [18], or from various sensorial experiences that affect an individual's perception of a value of given data or information. Ackoff [19] had combined the concepts of Data, Information, Knowledge, and Wisdom (DIKW) into one formula, as a hierarchical order of thinking about the relations between data and ways to put into use cases. Its pyramid shape is shown in Figure 1. For the scope of this related work section, ''understanding'' from Ackoff's model has been omitted as subsequent work on his model have not included it.

Data is the product of observations that have no value until they are processed into a usable form. It can come in the form of signs, such as numbers, words, or other signs that represent discrete facts. Information provides context to data, consisting of interrogative angles as ''who'', ''what'', ''where'', ''when'', or ''how''. Refining information with meaning and purpose gives knowledge. The experiences, values, and insights provide a subjective dimension that enables one to justify the decision-making process, which can be expressed in conceptual frameworks and theories.

Ackoff claims that this is the stage at which one is able to efficiently control the information. The upper tier of the pyramid is reached when knowledge is used to provide a wholesome judgement and insight under a specific circumstance. Wisdom is the ability to distinguish not only how to do things, but *why* they should be done in a certain manner due to their long-term consequences.

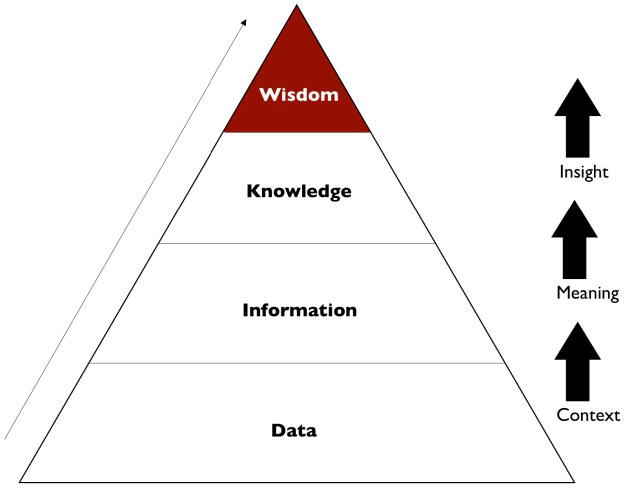


FIGURE 1. DIKW pyramid shows how observations can lead to an insight where the higher the level, the more abstract the reasoning becomes.

Sense-making [20] is a process by which people give meaning to their experience. Those with proficient sense-making abilities are able to map a credible route through an uncertain situation, and refine it according to new relevant information. Dervin [21] claims that sense-making is a gap bridging activity (see Figure 2) that aims to fill the gap of questions and unknown quagmires encountered in real life situations. The verbings represent dynamics of information that must be addressed using the ''bridges'' of intuition and ideas that help an individual overcome the unknowns.

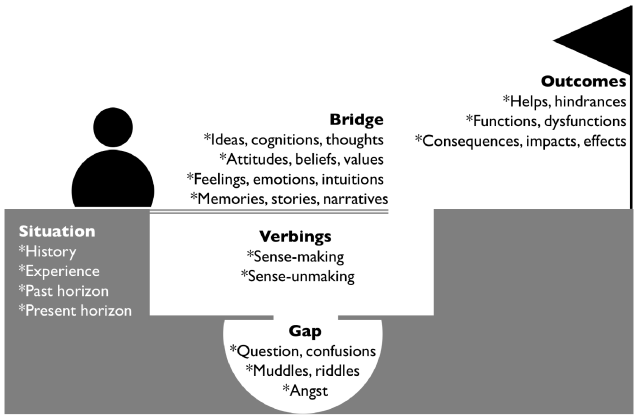


FIGURE 2. Dervin's sense-making metaphor, redrawn from Dervin [21].

The sense-making process encompasses both the psychological component – such as creativity, curiosity, comprehension, mental modeling and situational awareness – and the actionable component, where one devotes a ''*motivated, continuous effort to understand connections. . . among people,*

places, and events... in order to anticipate their trajectories and act effectively" [22].

C. KNOWLEDGE TRANSFER

Once tacit knowledge is created in an individual, this knowledge must be disseminated among others to make it usable. Practical transfer techniques for tacit knowledge have mainly been identified as mentoring, metaphor, analogy, storytelling, prototyping, and incident studies [13], [23]–[25]. Techniques for explicit knowledge have been identified through more formal training measures as schools, libraries, books, data media, written rules, and procedures [24], [26]–[28]. Other factors include boot camps, job shadowing, in-house training modules, games, simulations, "question of the day" bulletins, and storyboards.

The Socialization, Externalization, Combination, Internalization (SECI) model, proposed by Nonaka and Hirotaka [29], combines all of the above knowledge transfer methods in a conceptual manner, as seen in Figure 3. The model depicts the four different phases of a learning spiral, during which tacit and explicit knowledge interact with each other.

1) **Socialisation**: Tacit knowledge belonging to one person is transferred to other employees through direct contacts. e.g. an individual shares experience and episodes felt from using a specific business software product during a meeting.
2) **Externalisation**: Tacit knowledge is made comprehensible to others through various modes of expression, such as images, words, or metaphors. The instant feedback and exchange of new ideas help clarify the familiar experience and knowledge one has. e.g. the individual writes out a report on the benefits and disadvantages of using the product with visual screenshots.
3) **Combination**: New and existing explicit knowledge is now combined to tackle the existing problem or task. The documentation (of explicit knowledge) becomes widely disseminated, modified, or updated within the company. New ideas about the product in question are discussed based on the reports among employees and suppliers to cater to their views. e.g. the reports are uploaded on the internal company database where employees can access the media to see the report and learn how the software product works.
4) **Internalisation**: The new explicit knowledge is converted back to tacit knowledge when an individual uses the information from this report into his own work practice. e.g. After several repetitive exercises, a new employee develops a better gist of using the software product, and uses it without having to depend on the report medium anymore. Individuals who have viewed the document media can also request to meet with the original contributor to discuss in person about their experience.

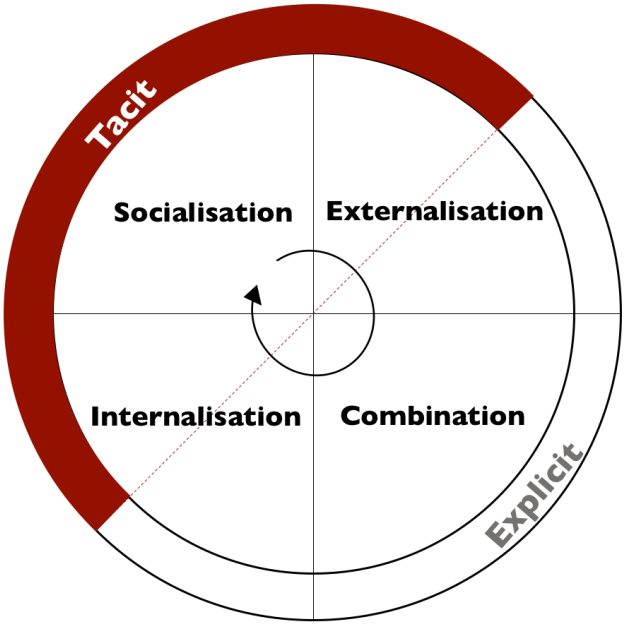


FIGURE 3. Nonaka's SECI-model depicting stage of knowledge creation and transfer in an organisational learning cycle, redrawn from Nonaka and Takeuchi [29].

This model is a spiral, and not a cycle, because one absorbs knowledge differently during each successive cycle, enabling the learner to continuously grasp knowledge at deeper levels [30]. Nonaka's notion of *ba* [14] is an integral part of the SECI model because it provides the space for the knowledge to be shared, created, and utilised within a community.

Despite the demonstration, there is still a need to clarify how the tacit and explicit knowledge can be systematically combined. This original model lacks in articulating the two most important conversion stages, externalisation and internalisation, and is left relatively too high-level for companies to practically implement it at workplace. Sternberg *et al.* [4], [23] claim that because tacit knowledge is a procedural activity, tacit knowledge cannot be acquired through explicit instructions; it is something that enables one to *do* something rather than learn about something, and therefore such knowledge cannot be indirectly transferred to someone who has not carried out the act before.

1) ARTEFACTS FOR KNOWLEDGE TRANSFER

Given the ubiquity of ICT in today's organisations, the in-person contact largely lacks the means to convey the sensory information, feelings, and context that manifest tacit dimensions [31], [32], and the employees simply do not get enough exposure with each other for the desired level of productivity. Roberts [32] claims that the degree of dispersity of teams is determined by "the degree of trust required, the proportion of implicit knowledge and the complexity of the project". Problem-solving strategies are still largely bolstered by interpersonal communication media, and neglecting the cultural aspects of non-verbal communication can hamper the organisation from agile information exchange, especially in projects on a transnational scale. In both of these works [31], [32], there is a prolonged emphasis on the concept

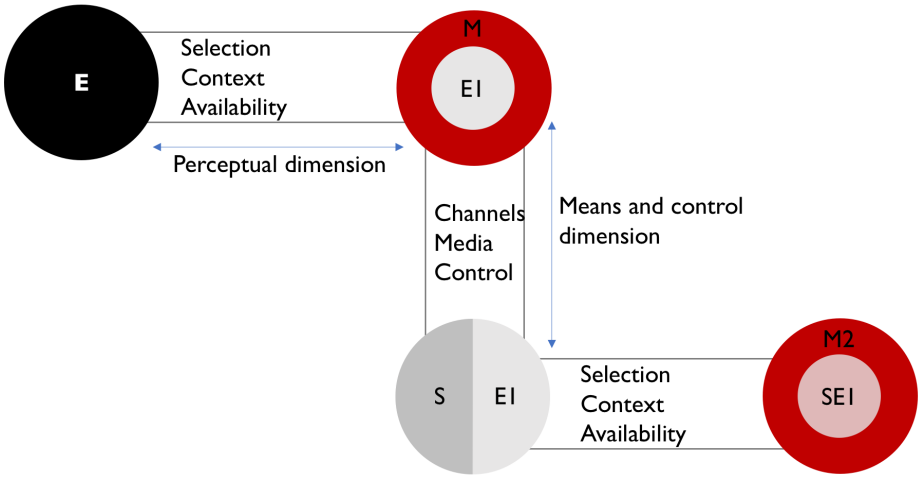


FIGURE 4. Gerbner's model, redrawn from Gerbner [33].

FUNCTION TYPE	KNOWLEDGE TYPE	RECIPIENT TYPE	VISUALISATION TYPE
Coordination	Know-what	Individual	Sketch
Attention	Know-how	Group	Diagram
Recall	Know-why	Organisation	Image
Motivation	Know-where	Network	Map
Elaboration	Know-who		Object
New Insight			Interactive Visualisation
			Story

FIGURE 5. Burkhard's Knowledge Visualization Framework embodies four main perspectives: The aim of visualization, the content of knowledge to be visualised, the recipient of the knowledge visualization and the medium to visualise the knowledge. Redrawn from Burkhard [34].

of shared space - much alike Nonaka's - asserting that the transfer of tacit knowledge requires the establishment of a shared virtual location that is backed by technology.

Gerbner's model [33] depicts how reliance on a variety of communication media can skew the content objectiveness of an event over time. His communication model in Figure 4 distinguishes the perceptual and control dimension in a horizontal and vertical outline. When an event *E* occurs, a man *M* perceives it and learns the meaning of it according to the criteria of selection, context, and availability, which potentially lends itself to bias or prejudice of *M*. *M*'s interpretation of *E*, *E1*, is expressed through the available channels, media, and control in a specific form *S*, which is then perceived by the next man *M1*. As this horizontal-vertical link continues over time, particular messages dominate and are adopted as the truth to subsequent recipients.

2) KNOWLEDGE VISUALIZATION

Knowledge visualization helps depict the flow of knowledge in a visual format that enable the viewer to better understand the relations between different, and sometimes unlikely, thoughts.

Burkhard [34] proposes knowledge visualization as a new field of its own, and points out the lack of research on knowledge transfer in the business context. He set out a Knowledge Visualization Framework (see Figure 5) that consists of four perspectives to be considered when creating visual representations that aims to transfer knowledge.

There are a variety of ways in which visualization can be realised, from sketches, clip arts [34], timeline maps [35] and flow charts to advanced geometric modelling [36] and geovisualization [37]. Eppler in particular discusses how the variation of knowledge mapping style, such as tables, cartographic, diagrammatic or metaphoric, can suit different purposes [35], [38], whether it be for developing, sharing or marketing the knowledge. Table 1 demonstrates his selection matrix for knowledge maps, which incorporates three features: 1) The desired knowledge associated with concepts, documents, or individuals; 2) How the knowledge map will be used; 3) The appropriate format of the knowledge map that caters to the previous two features.

The three content types used in the following knowledge map in Table 1 are: 1) Concepts (*c*) which include ideas, theories, insights or their labels, descriptions, and references; 2) Documents (*d*) which include patents,

TABLE 1. Eppler's knowledge map selection matrix. Redrawn from Eppler [35].

K Map Format	Table	Cartographic	Diagrammatic	Metaphoric
Creation of knowledge	(c)	c	c	C
Assessment/Audit of knowledge	e		e	(e)
Identification of knowledge		c, d, e	c, d, e	c, d, e
Development/Acquisition of knowledge		c	c	C
Application of knowledge	c, d, e	c, d, e	c, d, e	c, d, e
Sharing knowledge		c, d	c, d	c, d
Marketing of knowledge		c, d, e	c, d, e	c, d, e

method descriptions, lessons learned, and practice documents; and 3) information about experts or groups (*e*) which include photos, coordinates, homepages, and CVs.

D. KNOWLEDGE ARCHIVES

Knowledge archives are fundamental assets of an organisation because it provides relevant insights to individuals about a task at hand, and thus allows them to better prioritise work processes. An effective knowledge management system should distinguish and capture different types of knowledge that encompass both the tacit and explicit dimensions. The common types that provide key contextual information are declarative (know-what, know-about), procedural (know-how), causal (know-why), conditional (know-when), relational (know-with), and pragmatic (useful knowledge) knowledge types [34], [39].

SOCs often have wikis, playbooks, runbooks, and use case scenarios to convey information on general operations and identified threats. They provide information that analysts need for referencing quickly during an investigation, including configuration records, vulnerability databases, policies and a FAQs section. Some analysts have previously emphasised the importance of knowledge base usage as a learning process for future reference [40], where employees build, access, and share knowledge instead of having to repeat the same process of threat recognition. However, the existing ones are known to have update and maintenance issues, or only adopt generic use cases, that may render some analysts to abstain from using it as much as it was originally intended.

III. RELATED WORK

Capturing and recording tacit knowledge has been a challenge in research. It is contradictory for one to try to investigate the concept of knowledge which is known to be hard to articulate in the first place. In order for one's personal tacit dimension of a knowledge to be made transferable to others, the individual must first acknowledge it, or at least be able to exercise an action that can validate to others one's possession of that knowledge.

Sternberg's two main approaches in investigating tacit knowledge are ''critical incident technique'' and ''simulation approach'' [4], [41], [42]. In the former, he interviewed individuals with experience in the relevant domain and enquire information about tasks that were performed well or poorly. He queried the participants through realistic scenarios on the type of decisions that would be made in situations requiring soft knowledge. In the latter approach, he directly observes the individuals undertaking the tasks.

Heuristics based on on-set actions or scenarios akin to real-life circumstances [4], [43] tend to be more effective in helping participants acknowledge their knowledge because of the freshness of the experience in participants' memory. The fieldwork must convey the realistic constraints such as time pressure, risk, incomplete and ambiguous information, and the need to coordinate actions within the context. Tacit knowledge observation in IT is particularly difficult due to the lack of physical presence to observe [42].

Despite the criticisms that ensued regarding the methodology [3], his approach renders more feasible in practice because it focuses on the participants being in their usual workplace and recalling from their familiar artefacts - as opposed to a more restrictive control groups and testing that would detract the familiarity from the participants. Related to Sternberg is the work of Busch *et al.* [44], [45] which ran a survey based on likely workplace scenarios and questionnaires on the participant demographics, and demonstrated the relations using a visual mapping.

Leprohon and Patel [43] decided to follow through the participants' actions live, when they were investigating nurses in an emergency telephone triage. The researchers communicated with the nurses immediately after the completion of emergency phone calls, ensuring all the actions and decisions were fresh on the participants' minds. Although the actions taken by the nurses were appropriate, the explanation they gave for taking the actions were often inaccurate, indicating a disparity between their knowledge and action. The urgency-specific environment also meant that the nurses were familiar with prioritising high urgency cases and ensuring necessary interventions were sought after. The researchers of the study claim that individual nurses, over time, form their own categories of urgency which result in making same decisions in same situations; these however correspond to different knowledge structures as their knowledge and perception had been influenced by unique experiences. Their work corresponds with the ideas from Benner and Tanner [46] who suggest that the decision-making abilities of nurses cannot be categorised under a formal or normative model, and that they require a more holistic approach including a ''*deep grasp of the culture and language*''.

A. TACIT KNOWLEDGE IN CYBER INCIDENT HANDLING

SOCs operate on a sense of urgency and real-world complexities that are similar to other sectors that operate on high urgency establishments [43]. The time urgency is essential, in particular, as decisions have to be made as soon as possible based solely on partial or unreliable information. Analysts need to know what people, tools, and information are known, available, and utilisable at any point in time of their shift [47] so they can take immediate actions. Collaborative team work in physical environments have been suggested as most effective in increasing threat resolution capabilities [14], [40] where, in an event of an unexpected threat, all analysts should be willing to contribute to resolving it as soon as possible.

Ahrend *et al.* [47] examine ways to convert *Threat Intelligence* (TI) experts' tacit knowledge into more "*actionable*" TI, where the actions mainly refer to recognising threat alerts, containing damage, and obtaining situational awareness. The paper introduces the term *Threat Defence Knowledge* (TDK) to refer to an analyst's tacit knowledge about defence and threat features. The study shows that an analyst forms a relationship with the new-found information through three successive phases, where the analyst: 1) becomes aware of the existence of TDK, 2) validates the artefact that resulted in TDK, and 3) correlates the seed information of the investigation with the TDK artefacts according to its relevance.

Using semi-structured interviews and diary studies, Ahrend *et al.* find the lack of accessibility to knowledge about relevant TDK reduce analysts' ability to be effective in actionable TI. They find that the tacit nature of the practices makes it difficult to retrieve meaningful insights from second-hand or abstract accounts of one's actions, and advise diary studies for recalling the participants' daily routines for further investigation. Another challenge is that the nature of the work that analysts conduct tends to be more sensitive against the public eye. Some may not even support the concept of documenting tacit knowledge due to the potential risk of leaking confidential information about the business operation to its competitors.

Sundaramurthy *et al.* [48] took an anthropological approach by partially working at the SOC themselves for over 15-months to have a close monitoring of the operational challenges, and observe potential tacit dimensions among analysts. They discuss how contributing to the team work and delivering tangible tool enhancements, as well as working on-site over a long time span helped earn the trust of the team members and allow them to see the participants as they are in more natural forms. In the study, they expanded upon Nonaka's SECI model (see Figure 6) by incorporating apprenticeship in Socialization, and questioning, reflection, and reconstruction in Externalization, building new tools in Combination, and using the tool as a social vehicle in Internalisation (see Figure 3). Finally, they also highlight the paradox of fieldwork where, in order to capture accurate results on the underlying concepts of tacit knowledge, they have to essentially become the subject matter themselves and fully immerse in the environment.

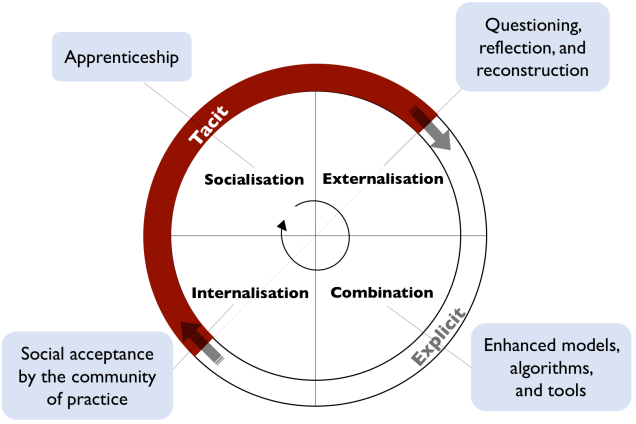


FIGURE 6. Tool-oriented SECI model, redrawn from Sundaramurthy *et al.* [48].

IV. STUDY METHODOLOGY

Based on the design of the fieldwork on tacit knowledge of Sternberg [4], this research focuses on a questionnaire and real-life scenario formats that will probe for the analysts' experiences at work and thinking processes upon facing different incidents. Our research followed a descriptive approach using semi-structured interviews, with ten participants from six different organisations in the UK. The organisational sectors varied over education, telecommunication, defence contractor, and IT. To reduce interpersonal biases among analysts of different positions, all interviews were carried out individually. Each interview lasted approximately 40 minutes. Six interviews were held in a meeting room within the team's building, three interviews were carried out in a public cafe, and one interview was done remotely over Skype. The interviews had been audio-recorded, with consent, except for two instances where the participants preferred to talk off the recording.

A pre-interview survey sheet was given out right before the interview for the researcher to have a broad understanding of the SOC background of the participant. The criteria for choices were potential influencing factors on role and team familiarity. The years were incorporated to understand how different years of field experience may later indicate patterns in thought processes [49]. Participant profile, Table 2, is shown below with the variables:

- *O*, organisation;
- *P*, participant;
- *Size*, number of people in team;
- *Position*, position in current team;
- *c*, years in current team;
- *p*, years in previous SOC team(s);
- *Professional*, professional background;
- *Academic*, academic background.

The inclusion criteria are that the participant is currently on the technical or managerial position of the team and that they have been at a SOC for at least one year, including any previous experiences of same nature. The exclusion criteria are that either the participant is not a full-time employee or

TABLE 2. Participant demographics.

O	P	Size	Position	c	p	Professional	Academic
O1	P1	>20	SOC Manager	10-15	10-15	IT	IT & Computer Science
O2	P2	>20	SOC Architect & Manager	<1	5	IT	IT & Computer Science
	P3	5-10	Security Consultant	1-5	0	Electronic Engineering	Electronic Engineering
O3	P4	5-10	Tier 1, 2 & Incident Response SysAdmin	1-5	0	IT	IT & Computer Science
O4	P5	10-15	Lead SOC Analyst	1-5	1-5	IT	IT & Computer Science
	P6	15-20	Lead SOC Engineer	5-10	1-5	IT	IT & Computer Science
	P7	10-15	Tier 2 & Lead SOC Analyst	<1	10-15	IT	None
O5	P8	15-20	Lead SOC Analyst	5-10	<1	Policy & Misc	Political Science
	P9	15-20	Lead SOC Analyst	<1	0	IT	Mathematics
O6	P10	10-15	SOC Manager	1-5	1-5	IT	IT & Computer Science

that they have never had any incident handling experience academically or professionally prior to this interview.

For the scope of this study, a participant was considered to be a mid-senior or higher if they had been in a SOC, including both past and present teams, for nearly 5 years or more in total. The outlier in the sample were three participants who have had no SOC experience prior to joining the current team, and have been working in the area for less than five years. The existence of outliers was acknowledged during thematic coding, which also included their views in incident handling in specific accounts of knowledge base and communication. While relatively new to the SOC role, P9 has had over 20 years of industry experience in finance and IT among other fields. Although P3 was the only participant without hands-on duty on incident response handling, they help manage analyst training in SOCs and ensure that the newly recruited analysts become integrated with the tools being used in the team.

A. STRUCTURE

The whole interview comprised of three parts, lasting approximately 15 minutes, 10 minutes, and 15 minutes respectively. The content of the interview involved breaking down themes as employee management, recruitment, culture, handover, knowledge base, and communication media to give an overview to the participant's working environment. These concepts are presumed to be influenced by the organisation's goal, size, client, and business processes that will be identified over the discussions. The interview questions were structured in a way that it targeted for these themes. Short guideline questions were given for multiple questions and threat scenarios – regarding tool usage, communication methods, and any advice for victims – to help the participants stay on track of the case scenario discussion. Three hypothetical cases were picked because they are some of the most recent and widely reviewed cases currently impacting the security industry; there was no prior knowledge on whether the participants had dealt with such cases before. The multiple choice questions and threat scenarios are listed in the Appendix.

1) INTERVIEW

The interview contained short administrative questions about the participant's workplace and his day-to-day incident handling operations. It enquired the participant about his opinion on the importance of in-person communication in SOC capability and any frustrations experienced with respect to the existing communication media. Some interviews had more emphasis on the recruitment aspects, and all of the participants briefly explained what their knowledge base would be used for in incident handling tasks. In order to assess how the participants feel about the present communication method in the team, the participants were asked how they communicate and to share any episodes regarding communication delays and hindrance.

2) MULTIPLE CHOICE

The participants were then given a multiple choice questionnaire about steps to take when resolving a DDoS attack, with the assumption that a nationwide grocery retailer was the SOC's victimised client. The questions involved to whom the participant would communicate with or with what the participant will attempt to analyse the situation. The multiple choices had been inspired from the published guidance from the UK National Cyber Security Centre (NCSC) and the US National Institute of Standards and Technology (NIST). After completing the questionnaire, the participant was then updated that one of its clients was under a DNS reflection DDoS attack situation, and probed on what actions they would take to address it. It was assumed prior to the interview that each analyst will offer his own unique approach on the problem-solving, and that the experienced analysts may have answers that do not strictly adhere to the step-by-step manuals [47].

3) THREAT CASE SCENARIO

The last part of the interview consisted of two threat case scenarios, inspired from well-known Stuxnet and WannaCry. The interviewer narrated a hypothetical account on what abnormalities the participant has experienced, provided with visual aids on A4 sheets: the first one for Stuxnet consisted of an overview of a power plant facility, and the second one for WannaCry consisted of a user alert sign.

The Stuxnet scenario had three main points of suspicion: 1) sudden increase of alerts to access the industrial control system (ICS) maintenance over the recent days; 2) an IT

employee in the ICS maintenance team experiences reboot loop on his laptop; 3) a malware is discovered on his laptop that is known to use fraudulent digital certificates, affiliated with another recently hacked facility. The WannaCry scenario described a large UK hospital where an increasing number of employees were witnessing ransomware alerts on their work devices within a span of one day. Participants had been clarified that alerts were free from false positives.

V. STUDY FINDINGS

The recordings of interviews were transcribed and analysed, using NVivo12, to demonstrate the thought process of analysts during an incident response. After completing the axial coding of the ten interview transcripts, a total of 17 nodes[1] were organised, including six parent categories, from the discussion about the SOC operation and analyst traits. Three separate nodes were created for the three threat scenarios, and five more nodes were created to distinguish between validation, containment, remediation, future work, and miscellaneous processes identified during participants' threat scenario response.

Business Process Modelling and Notation (BPMN) and Decision Model and Notation (DMN) were used subsequently to investigate whether such aspects of the incident handling process can be codified as procedural elements of tacit knowledge in incident handling. These models are graphical notations commonly used for documenting business processes, and it has been known to help resolve ambiguities found in textual process specifications [50]. We make use of start and end events, tasks, and gateways (decision points) [51].

A. THOUGHT PROCESS AND RESPONSE

Four different BPMN diagrams have been formed to capture the identified thought processes:

- **Overview**: The overview of the thought process extracted from the three threat scenarios (Figure 7).
  - **DNS attack against a grocery retailer**: A client platform is inaccessible due to a DNS reflection attack (Figure 9).
  - **Malware in the critical infrastructure**: Malware using stolen digital certificate is found in a critical infrastructure maintenance site (Figure 10).
  - **Ransomware in the healthcare sector**: Ransomware alerts are rapidly spread in hospital computers (Figure 11).

As seen in Figure 7, the general thought and decision-making process of the threat cases followed the 'detect, contain, and remediate' components in order. Depending on whether or not the incident had been witnessed before, or it is under the team's tool capacity, the analyst would decide whether it should seek external support from third-party vendors or local IT teams.

[1]In NVivo, a node is a collection of references about a specific theme or case.

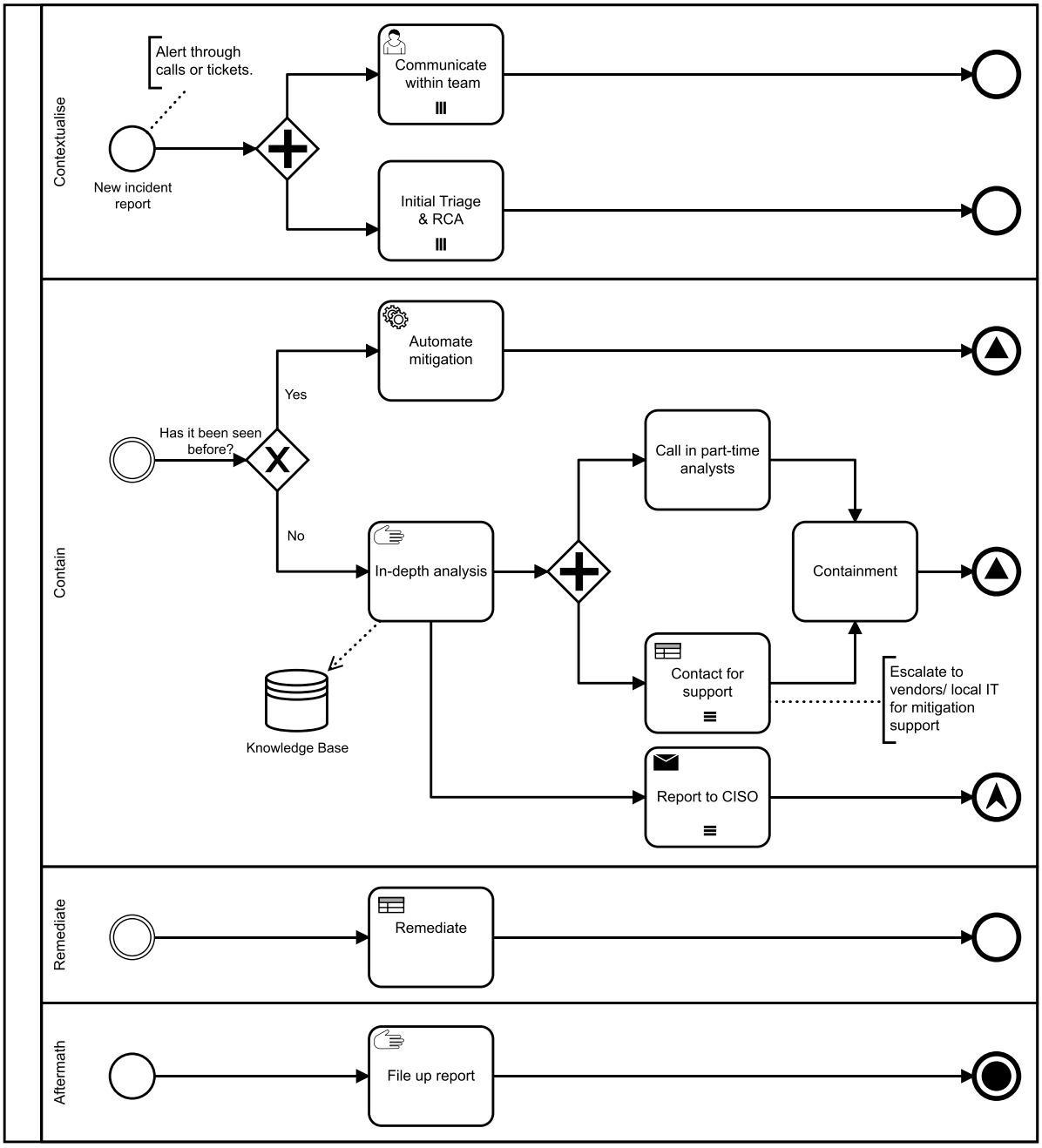
When a suspicious activity or incident is reported, the analysts often immediately verbally communicate with team members who are sat in the same office area. Analysts who were sat near their colleagues in particular claimed to be content with how easily they can inform people across different positions immediately. Upon detection of a critical threat, there would be a brief discussion about the presently affected situation, including the assets at risk, and delegation of particular tasks. This takes place simultaneously with the initial triage - the insights into who and what is affected, how far it has been affected, and since when this has been occurring - and Root Cause Analysis (RCA) - the interrogative aspects of what happened, how it happened, and why it happened - to decide how it can be contained and remediated subsequently. Sources of knowledge come primarily from SIEM monitoring tools but others also include direct contact with local IT support teams, victims, or wiki knowledge base. The relations table below the BPMN image in Figure 7 shows an expanded view of the point of contact that would be sought after. The *U* column depicts different rules for decision-making. Depending on the current state from the incident, an analyst can understand who would be the appropriate person to contact for support. The Chief Information Security Officer (CISO) would rarely be contacted without any validation of the facts in order. However, if any critical assets appeared to be at stake that could affect the overall business operation, the CISO, or a person of similar rank, would be alerted about the incident immediately.

After the investigation, if an analyst recognises this type and scale of impact has previously occurred and been controlled before, they will run it through a mitigation technology in the team. If it has not been seen before, or has previously needed external help, the task would be escalated for third-party vendor support, and all part-time analysts on call would be contacted to come into the team office.

Containment and remediation aspects have been simplified on purpose as the scenarios only enquired about the analysts' first line of action and thought process upon incident detection. Once an incident has been contained, remediated, or both, so that the business operation is getting back on track, analysts would file a report about this incident for the senior-level managers detailing what and how it had been addressed.

1) FIRST SCENARIO: DNS REFLECTION ATTACK

The results from the preliminary DDoS survey is demonstrated as stacked bars in Figure 8, where only the answers in majority has been indicated in blue or red. Upon receiving a call about a client's business platform being inaccessible, over half of the participants had agreed that the first reaction is to check the log or contact the network support team. The two participants who indicated they would check for logs also said this differs from what they should do, and three participants who indicated they would block some traffic said this differs from what they should do.



Contact for Support		
U	Current State	Point of Contact
1	Unusual network traffic	Upstream Internet Service Providers
2	Unusual network traffic and/or not sufficient existing tool or human resource	Local operations and networks team
3	Existing tool not sufficient for mitigation	Tool vendors
4	Unknown infection	Forensics team
5	Potential data loss and/or business disruption	Backup data centre
6	Critical infrastructure operation under threat	Law enforcement

FIGURE 7. Overview: Thought process extracted from the three threat scenarios.

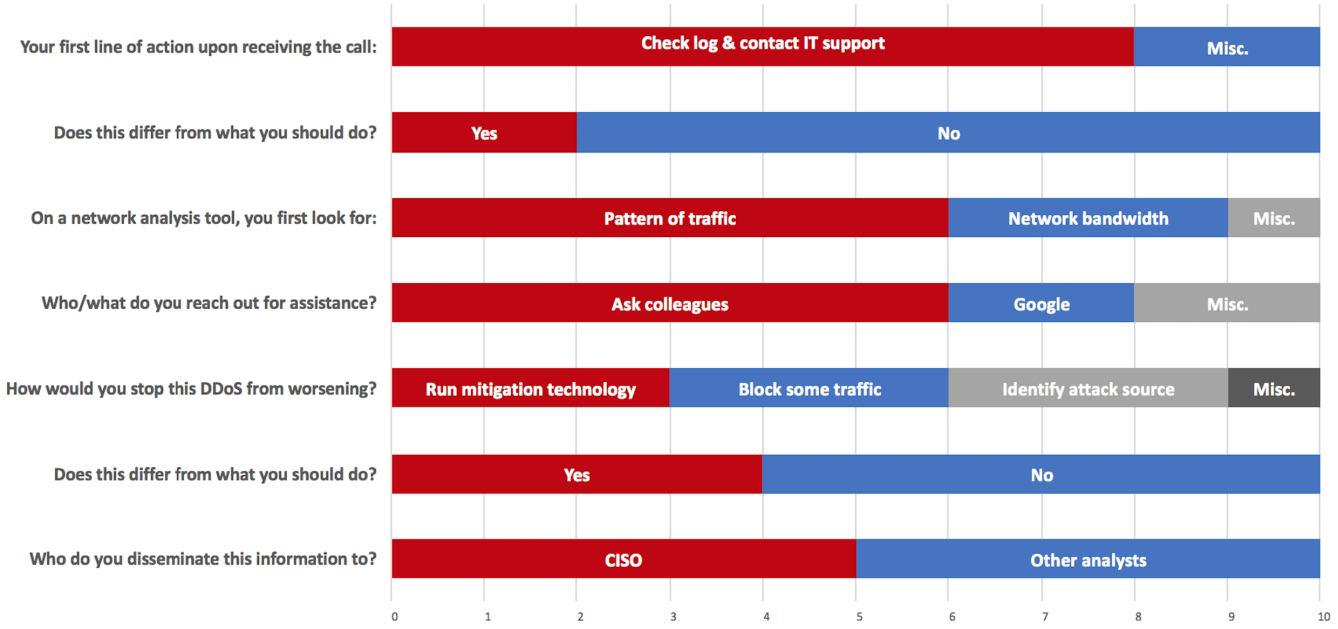


FIGURE 8. Preliminary DDoS survey results with the questions presented in a chronological order.

Figure 9 below shows the breakdown of the processes of how the participants claimed to address a DDoS attack if it had been enabled by spoofed source IP address of its client. From the outset, half of the participants replied that they would start the case by identifying the scale of the DDoS impact to get an overall picture of this incident, which involves finding who or what has been affected and where this spoofed server is located - to identify how much of the DNS infrastructure had been compromised, using the SIEM monitoring tool. Analysts would be communicating this across the team verbally and online meanwhile. If the situation was to involve critical assets and potentially public image, the team would alert the situation to the CISO. P6 claims that the team has to "*let (the) management know, for this specific one. Because at some point (it has) to make a business decision, and it could be a strategic decision*". In that case, one would check whether the client organisation has other backup servers on which they can continue to operate their business while the current one is inaccessible. Otherwise, it is advised to wait until one has confirmed and has all the facts in place to make a proper report to the senior-level executives.

If the analyst finds that this scale of attack is well within the existing tools' protection capacity, they will automate it through the team's DDoS mitigation tool. If it exceeds its protection capacity, they will inform the situation to the ISP, then see how the team can get assistance in balancing traffic from scrubbing services and local IT support teams, and check with backup centre for possibility to resume service there. The CISO may also be contacted about the updates on the operational issues if critical assets are at stake. In the meantime, the analysts would dig into in-depth triage and RCA of spoofed DNS structure using the SIEM tool and the existing knowledge base. P1 claims that one "*cannot just do remediation without knowing the root cause, and that is the mistake people usually make*". While managing the perimeter controls, the SOC team will communicate with the client organisation and ensure their business continuity and redundancy is in place. If the attacks are contained, the procedure comes to an end where one writes a report to send up to the manager or update the internal knowledge base about how this attack was addressed.

2) SECOND SCENARIO: CRITICAL INFRASTRUCTURE THREATS

The view as to whether the three suspicions - increase of alerts, laptop reboot loop, and malware discovery - was considered altogether a related event was split half and half among the participants. All however agreed that after confirming the presence of malware, immediate measures would be put in place. P5 was able to provide details on the things they would desire and expect in this situation: "*I would want logs, and I would want to bring in the FIR (Forensics) team. I'd want that host isolated from the network, I'd want the forensics guys to tell me what it is. I'd want to be confirmed with logs from various devices that are being affected by it.*"

Figure 10 shows how the procedure unfolds. First, the identified laptop and any other infected devices identified from the initial triage would be isolated from the internal network. While enquiring the victim employee's ICS team about any activities out of the ordinary that they have engaged with in the past 24 hours or more, including with the device in question, the analysts would try to have an understanding of how this malware was delivered and spread. These information will be disseminated across the team, and if there are critical assets at risk the CISO will be notified immediately,

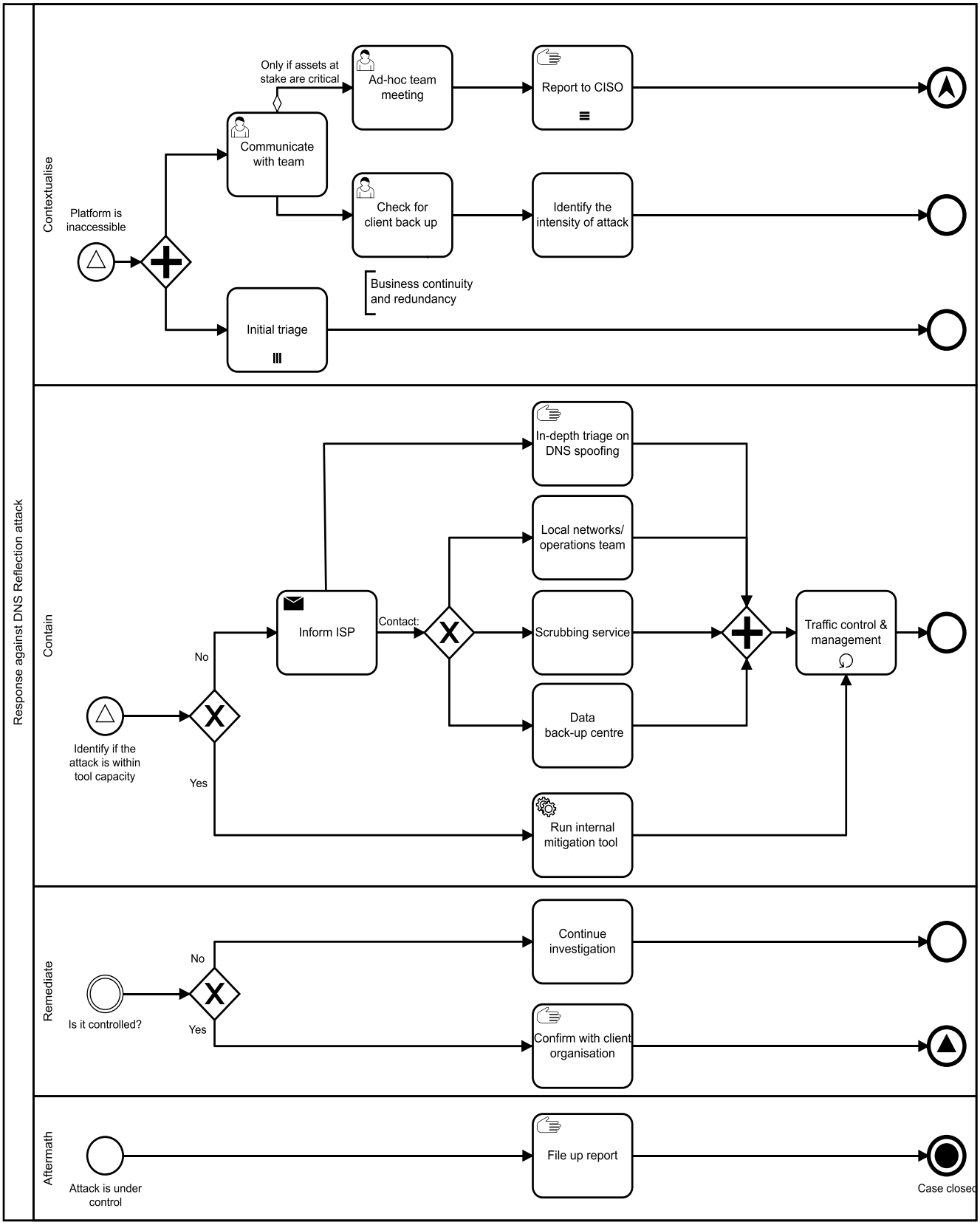


FIGURE 9. Scenario I: A platform of a grocery retail client is inaccessible due to a DNS reflection attack.

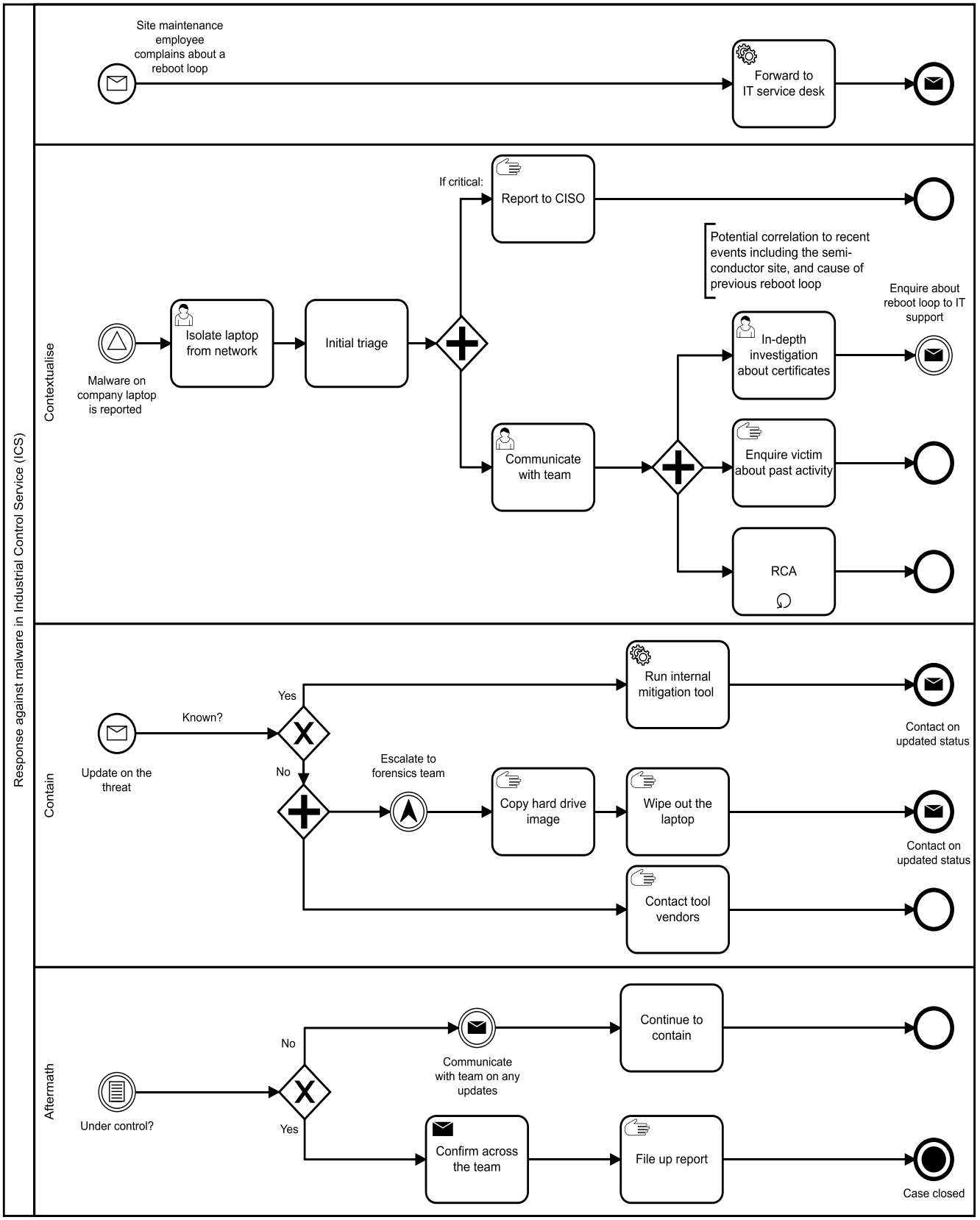


FIGURE 10. Scenario II: A malware using stolen digital certificate is found in a critical infrastructure maintenance site.

followed by a team meeting to discuss the situation. In terms of prioritisation and escalation, P8 added that "*if malware itself was fairly rudimentary and lacked in any direct interference capability, if we couldn't attribute it to some foreign state, it would be more a moderate priority event. It would definitely be escalated for internal team to handle, to pick up from that perspective. If we were able to positively attribute it, or there's any evidence to suggest it might have the ability to perform disruptive or destructive activity inside the ICS environment, then it would immediately elevate it to much higher priority.*" The analyst may then look further into the pattern and the consequence of the spoofed signature, the consequence of user credential exposure, and whether there are any signs of foreign attribution. While searching on the internal and external malware database, the analyst may subsequently contact the semi-conductor site to enquire about the certificate management.

Several participants reckoned that they would then take a copy of the infected laptop device, reach out for the forensics team to have an in-depth investigation of the infected device, and potentially clean the device into a blank slate. The investigation will continue until the team has a better picture of how to mitigate the root cause of the malware. The precise order or criteria of the steps at this point varied for many participants, from directly contacting the local networks team to calling up the hacked semi-conductor site to gain information about the digital certificate management. If the case could potentially be attributed to a foreign state, it would be directly escalated to the senior level management. If the malware was recognisable and of moderate criticality, it would be managed using the existing mitigation tools. Once the spread of the malware has been contained, four participants claimed that this incident would be filed up in a report. The tools and information used to address this case will also be recorded on the knowledge base.

3) THIRD SCENARIO: RANSOMWARE

If there had been no signs of ransomware at all previously, and it suddenly came to the analyst's attention that this was the case, it most definitely signals that something is spreading according to the majority of the participants. The immediate outbreak of the ransomware and the context of the hospital means that an analyst will attempt to head straight into containing the spread, instead of having to understand thoroughly about the malware for the time being. P10 claims that this will be a "*mayhem*" situation, and "*all the analysts will have to be coming in, even if they're on leave,*" making it an "*all hands-on situation*". The procedure is demonstrated in Figure 11.

Because the client organisation is a national health sector, more than half the analysts agreed that this case would have to be notified directly to the management level or the law enforcement to inform them this hospital's operation would inevitably be, if not already, disrupted. Amid the uncertainty, however, P5 claims that "*[at] the earlier briefings when you're still not sure what has happened, you're just giving the best information you can – at that stage there's probably no decisions to be made, because you're not in command of the full facts; you can't decide on the best course of action. You need to gather as much information as possible, as quickly as possible, and get that to the decision-maker*".

As the message is sent across to individuals outside the SOC team, the analysts would be carrying out an initial triage and RCA with T3 analysts while communicating with the victims and the hospital IT administrators to understand the scale of the ransomware impact and how this was enabled on their devices in the first place. The questions during identifying the root cause include: how is the malware spreading?; how was the malware delivered?; what activities did victims engage with in the past week?; what device are the victims running? The analysts would simultaneously be reaching out to any relevant third-party vendor services that this hospital uses.

The analysts would then disconnect the device - if it had not already been instructed by the analyst to the victim at the time of the initial report - to stop the spread first and foremost. In the case of a safety-critical system, the device would not be able to be simply disconnected, and this task would have to be escalated to the forensics team. Duplicate copies of infected devices would be escalated for further investigation, and, depending on the available budget, the employees would be stocked with new temporary devices in the meantime. Then, a decision will be made whether the infected device will be put on a kill-switch or be completely wiped out in blank state.

If a hospital has a solid backup resource, log retention, and network visibility, the employees will be able to resume their operation soon enough and the hospital will have their main health records data back on track. The worst case is when the hospital does not have a backup or such visibility as it will have very low chance of retrieving the data back. In this case, the SOC team will loop back into alerting the higher management and potentially the law enforcement.

In the long run, some analysts will advise the hospital to upgrade their hardware devices to future proof their operation from having a ransomware through a similar vector again.

B. KNOWLEDGE TRANSFER STAGES

Recurring themes in discussion about communication and training have been used to enhance Nonaka's SECI model [29] for the SOC environment. Figure 12 depicts these elements with the emphasis in the Socialisation and Externalisation stages.

The Socialisation stage consists of promoting more in-person contacts with the analysts across different team locations through business trips or initial training programme. This appeared to be significant source of gaining insight and building trust between different analysts, especially in the case of a global SOC operating across different countries. The interactions should not only be encouraged internally but also with third-party vendors and contractors to provide fresh

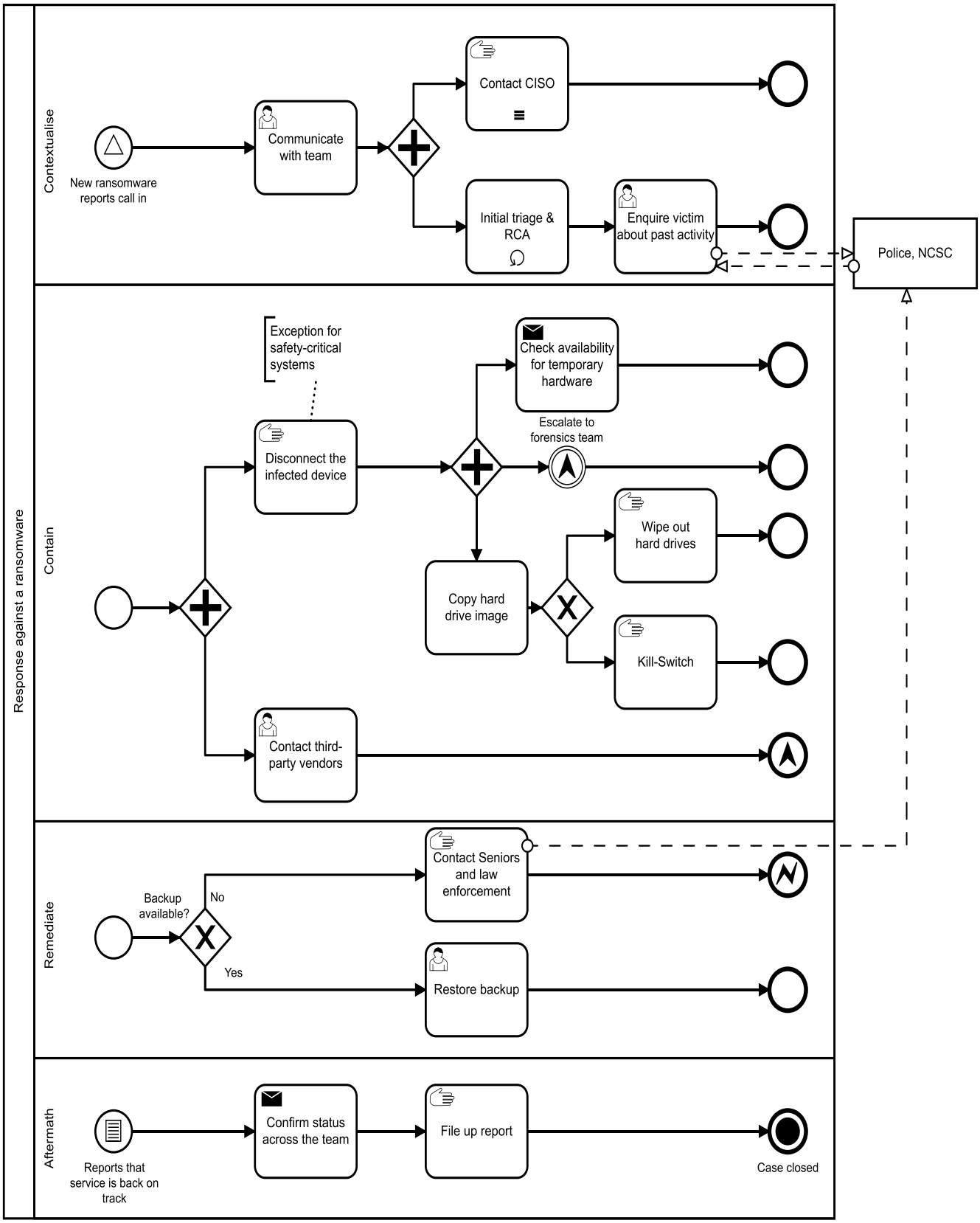


FIGURE 11. Scenario III: Ransomware alerts are rapidly spread in hospital computers.

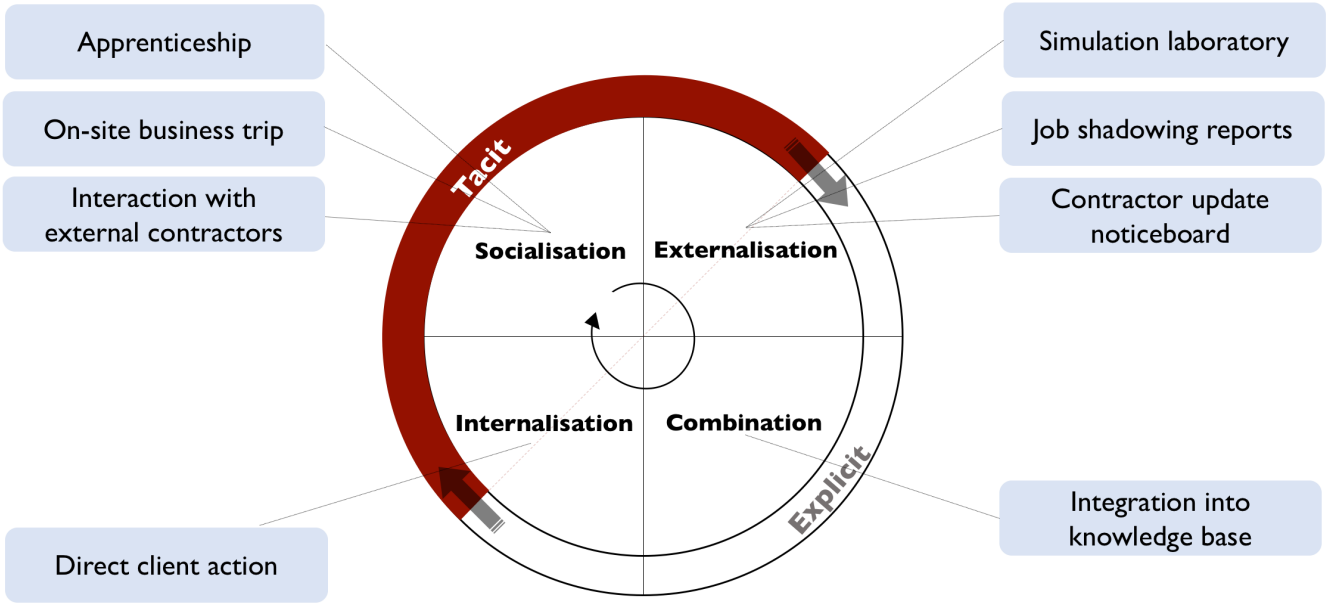


FIGURE 12. A revised SECI model with the emphasis on simulation environment and physical proximity with analysts and third-party vendors.

insights about any new findings and suggestions about the SOC operation that the team alone could not detect.

The aspect of apprenticeship highlighted in Sundaramurthy *et al.* [48] was frequently brought up as an important aspect of acclimatisation into the specific SOC environment. More than half of the analysts claimed that they prefer - what P10 called - the "*watch and learn*" method over merely reading off the text guidelines, for both effectiveness and ease of understanding. For the first few weeks upon entering the SOC, a newly recruited analyst would follow through job shadowing from his immediate senior, and observe what to look out for and what tools are used. P9, who has had his own share of job shadowing, claims that "*it really stresses [him] out but has also helped [him] a lot to get on track*".

The Externalisation stage includes an environment where new analysts can apply their newly acquired knowledge in action, and critique on the findings of their own or others. The simulation laboratories and quizzes provide a platform to transform previously acquired tacit knowledge into explicit forms by having performance scores and comments. The analysts can also write down what they had seen and learned during job shadowing sessions, which provoke him to reflect on the incident response procedures. P7 claims: "*sitting over someone's shoulder is good for a little while but you need to be really doing these yourself and be looking at the packets; you then start to understand it all.*"

On a different note, this Externalisation also caters for changing verbal communication into more explicit forms to ensure all analysts are on par of certain knowledge references. The contractors can keep the team informed of any changes to the tasks, systems, or knowledge base that are brought about during their time period, in a physical or virtual update bulletin board. An insight and work style of someone from outside the team can either enhance or hinder the existing work of the team. From the potential negatives, there may be duplicates of data that are created, or data that disappear, at the end of one's contract from the SOC causing operational nuisance. This is applicable not only to the contractors but also to anyone relevant to the team who may have edit rights without anyone responsible in place to manage the knowledge base. Thus, enforcing more frequent updates on collaborative platforms can ensure that there are no gaps of knowledge from one employee to another.

In the Combination phase, all the newly produced explicit knowledge documentation would then be combined with previous documentation in hard copies or online knowledge base, so that the analysts can use it as a reference point when learning about tools or past incidents. In the Internalisation phase, the junior analysts would be equipped to get involved with direct client action initially using the updated knowledge base, while the senior analysts continue their usual work routine.

1) COMMUNICATION

Various virtual media exist in SOCs to communicate incidents including email, online collaborative platforms, internal chat messaging, and phone calls. However, all respondents in the interview agreed that physical communication overbears all other available communication media, though for different reasons. Talking to a person face-to-face helps eliminate any misunderstanding of issues at hand, including the ones arising from language barriers or the lack of specific knowledge, and thus gets rid of redundant communication about a same concept. Some may misinterpret the tasks to focus on and cave into their own world about information that may be

peripheral to the team's much needed tasks at hand. In a large organisational sector, employees in different divisions of IT and operations may not comprehend certain concepts that is more specific to SOCs, so physically heading over to their office for discussion would reduce such hindrance. Face-to-face communication also included the aspect of working within the same proximity of others in an office, which help bond trust relationships. Being too distant from the co-workers or managers for too long may also generate lax attitude and less dedication in one's roles.

Cultural aspects played a big role in global SOCs, witnessed by analysts who often have to travel overseas for different SOC divisions. The respondents claimed that when interacting with other internationals, one needs to bear in mind the specific cultural norms to which they are accustomed, and analysts in some regions can be naturally more lax or alert than others. Social norms and labour regulations could influence the way an analyst perceives and prioritises an incident handling task, and thus even affecting the content communicated with other analysts. For instance, there were two episodes from the participants about employees who insisted on having an early leave from the office for a holiday, despite the highly stressful and urgent situation the team was in at the time.

Furthermore, one's culture may be directly tied to one's ability, or inability, to think out of the box. P1 explained the importance of free thinking in the context of SOCs: "*Free-thinking, in this example, is to correlate every indicator of compromise and build up a bigger picture. Like if I see an attack in (Country A), but at the same time I see a similar attack happening in (Country B), then the first thing I will think about is: 'is something wrong? is it a global attack?' [. . .] But if you don't have this free-thinking mindset, you will treat these two types of attacks in two different countries as stand-alone incidents – You won't correlate them.*"

2) KNOWLEDGE BASE

While the kind of knowledge base owned varied over different organisations, it was agreed by all respondents that a knowledge base is crucial for operational consistency across a SOC team. P1 claimed that it is the "*foundation*" of a SOC to deliver operational excellence. Using the knowledge base, analysts can share or learn the processes and procedures involved in triaging specific alerts. The use of internal wiki, runbooks, and external knowledge base about malware and threats were mentioned in threat scenarios to use during the triage and RCA processes.

Though these knowledge base tend to appear more useful for junior analysts, P5 claimed that the newly relocated analysts would also find it useful to figure out logistics relevant to the specific organisational setting, such as where to go next, how to get logs, and what logs are currently made available to them. This is also useful for analysts on a night-shift where the managers might not necessarily be present to explain the precise components of tools or work procedure. More than half of the participants agreed that within months of joining a team, most analysts eventually grow out of using playbooks and knowledge base, and rely more on their own gist when doing tasks on a usual basis.

In the case of playbooks, P2 claimed that today they are rather "*obsolete*" because their existence means the threat has already been witnessed previously. This was due to the assumption that the known threats should not be a trouble mitigating given the time and team's resource, and it is usually the unknown threats that cause more concerns. P8 claimed that rather than looking up specific indicators that has already occurred, his team "*proactively look(s) for how a set of behaviour, or attacker activity might appear on this network.*"

With regards to how useful knowledge base is to the team, some analysts found that if the team is not mature enough, there was not enough information to derive from that database alone. On the other hand, an organisation may have too much information to be consistently organised and maintained, which causes a delay in the retrieving process and also discourages employees from making a use of it for regular use.

The two main issues with a knowledge base appeared to be accountability and maintenance especially in large teams. Various individuals, mainly SOC analysts working across different roles (e.g. external contractors), tasks, or geographical locations may have rights to contribute without a set policy, potentially leading to concurrent copies of information or information loss. In this case, delegating someone to be accountable can help facilitate the maintenance. P1 claimed that the team can set each team manager responsible for specific sections of knowledge base, who can review the enquired content updates to decide whether they are appropriate for the section. Up until that point, the edit drafts are held on a different environment ("*pre-prod*") that is much akin to the original server. This ensures the quality of the information on the knowledge base has been screened by an authority, and that the updates are well integrated in the original knowledge base. With regards to the relevant roles, P2 noted that one should not confuse accountability with "*blame game*" as everyone is equally accountable for the tasks at hand, and that it's a matter of informing the right information to the right person in time.

3) INFLUENCE ON RECRUITMENT PREFERENCE

Recruitment preferences varied largely. Some participants were confident to train fresh graduates from bottom-up, whereas some would only recruit people who have been in the IT sector for at least two years. On the training aspect, some claimed that the thinking process essentially cannot be taught to others, and that process, procedures, and relevant knowledge bases exist only to equip the analyst with the team-specific technicalities. In discussing the properties of a good SOC analyst, P1 discussed one's ability to think in the "*whole end-to-end of the story, by doing a lot of thinking.*"

P2 claimed that years of experience do not necessarily dictate whether an analyst is effective or not in mitigation. They

claimed that due to the fast-changing dynamics of a threat landscape, it is more about how up-to-date one is with the latest threat trends rather than the sheer number of experience in the industry. The psychological aspect of an analyst was also briefly mentioned in pursuit of analysts' aptitude for SOCs:

"*(A person) went somewhere and found this wallet on the ground...If a person chooses to ignore it, there's a thinking behind it why they chose to ignore it. If a person picks it up, and goes to a police station, there is (also) a thinking behind it...Bring back these two psychologies to SOCs. If you see there is just one ICMP, a ping packet going to a server, you ignore it. But may be that one packet is a trigger to a small attack or a ping of death attack. Now a person of different psychology, even though there is no use case, he will go and see this packet. It's just mere curiosity.*"

P4 suggested that the mindset and the background of the people may be the most relevant aspects for this position. System administrators, for instance, have already had thorough experience in networks and operating systems, which makes it easier for them to adapt to the tasks involved in incident response teams.

VI. EVALUATION

Overall participants may have felt the need to help the interviewer and thus provided more generic type of answers in incident handling that might not necessarily reflect their real actions. This may be even more the case for participants who have less than two to three year of total SOC experience who are conscious of the eye of the audience, and want to ensure that all their tasks and decisions are correct and accurate. The participants with more total years of SOC experience were able to provide thorough reasons for the actions that they would take, and were flexible in providing different kinds of real-life examples on the spot to support their arguments. One thing to note is that whenever the participants were asked on the status of escalating to CISOs, the participants with less than five years swiftly answered that the incidents appearing in the corresponding case scenarios would have to be escalated to the higher levels, and did not seem to have a uniform threshold to decide what is and isn't worthy of classifying as high priority.

8 out of 10 participants had academic and professional backgrounds in IT, including IT security, prior to joining the current team, meaning that there was a lack of variety in the backgrounds to compare their impact on the thinking processes with those from different backgrounds.

It was however mutually agreed by majority of the participants that an analyst need not come from an IT background but rather have a versatile mindset that is apt for the niche tasks in SOCs. For a more detailed study in the domain of mindsets and stream of consciousness of the analysts, it may provide insights when observing the incident handling actions live as was done by Leprohon and Patel [43] in emergency rooms in hospitals.

While the overall validation, containment, and remediation stages unfolded in the threat scenarios largely followed the steps outlined in popular guidelines,[2] the post-mortem analysis was rarely mentioned. The interviewer had intentionally not asked the participants about it in the fear that the question would probe for a biased "*yes*" answer in following the standard protocol. Further, two participants claimed it is usually only applicable to very large organisations who could afford such resources and find the value in investigating the incident handling process in-depth. This may be due to the fact that once the clients' business has fully recovered from an incident, the findings from triage and RCA themselves serve as sufficient information for future references.

The result of the threat scenarios and discussions showed that participants have different conditions on which they prioritise incident tasks, such as the level of business risk, the scale of incident impact, or the urgency to deliver victim support. The senior managers and analysts essentially work together to make sure the "*crown jewels*" remain intact. Overall there was an agreement across the participants that the incidents had to be prioritised according to the potential risk and the magnitude of the incident at hand, as they are directly correlated with business operations when targeted.

When discussing the topic of knowledge media, nearly all the participants have mentioned the existence of knowledge bases, internal wikis, and runbooks; whether these are actually sought for in the times of crisis management was questionable. Although such information are useful as a guidance for new analysts, it appeared that it didn't apply to the interview participents in this study, most of whom had been based in SOCs for at least 2 years. The maintenance issue with vast knowledge base also seemed to deter the experienced analysts from referring to it when events have occurred.

The work culture, individual mental model, and personal traits are highlighted as main factors that contribute to how an analyst perceives an incident task. The previous or current work culture that an analyst was or is involved in affects with how much gravity the analyst views a task, which may cause him to neglect important alerts or over-analyse mundane ones. The mental model and personality broadly allude to the aspect of human psychology which was reflected in the participants' recruitment preference. The participants accentuated the importance of a curious, free-thinking, correlating, or analytical mind, where these characteristics provide hints of an individual being a good fit in a SOC operation, and that the knowledge base supplements such a mindset to assimilate to the team setting.

A. DISCUSSION

Over the years of exposure in incident handling, experienced analysts develop a strategy that primarily looks for the context of an incident and the business implications it has, rather than focusing solely on specific technical components, to help

[2]See NIST Special Publication 800-61, Computer Security Incident Handling Guide [52].

prioritise and delegate tasks from the start. In the case of managers who originally have a technical background, their understanding of how different people, process, and technology integrate allows them to ensure the team's day-to-day tasks are properly aligned with the overall team work and, more importantly, protecting the organisational assets.

It is worth noting from the threat scenarios that all participants instinctively searched for what they have already witnessed before. This effectively highlights the very human cognitive efforts to dissect and analyse a problem by reflecting on previous accounts that could potentially offer a faster solution.

In the third scenario on Ransomware, all the participants primarily aimed to contain the spreading damage, and no one had suggested a way to reverse-engineer the ransomware which is potentially what is expected to be done with the external forensics team. The participants focused on the concept of quarantine in both the second and third scenario; to capture the situation as is, discourage the victims from losing data, and ensure operational and business continuity.

Participants often sought to identify the interrogative aspects of what, who, how, and why that is in accordance with the DIKW pyramid - especially at the conversion point from information to knowledge - in Figure 1. This also supports the notion [21] that the mix of one's past experience, sense-making ability, and intuition help bridge the missing context of an incident and provide subsequent means to address it. If a threat was unknown or was appearing to exceed the capacity of the team, the incident would be escalated to different IT divisions or SOC team offices and third-party vendors. The question as to how open a company is to operating its own internal SOC as opposed to a fully outsourced SOC would not only depend on the available finances but also the working culture of the SOC and how open it is to integrating with the temporary contractors.

Trust came across as an issue in previous fieldwork by Sundaramurthy *et al.* [48], whereby the researchers tried to overcome it by physically working within the SOC themselves. Similarly, this study also found that some analysts felt more bonded and trusting with peer analysts if they had worked within the physical proximity. This alludes to the cultural aspects within the team that was covered on how co-working environments help address issues as language barriers, declining productivity, and passive communication among analysts.

Nonaka's SECI model is designed under the assumption that tacit knowledge can be captured and transferred. What the desired analyst mindset derives from and ultimately whether tacit knowledge is transferable to others is something that can be investigated further beyond this study. The findings support Nonaka's notion of *ba* [14] in that shared physical space is preferred when transfusing information and knowledge to others more clearly, as opposed to merely reading the textbook guidelines.

B. DESIGN LIMITATIONS

The two focuses of this study design was that it was focused on a sample of experienced analysts and that their thought processes were recorded as they confronted the threat case scenarios. The fact that the case scenarios were merely "*scenarios*" inevitably offered limits to observing what action the participants would have actually taken if the said suspicious activities really occurred; this was especially the case if an analyst had never encountered the problem before or it involved environments, such as national power plants from the second scenario, that seemed unlikely to pertain to their usual operations. The survey had briefly attempted to address this by probing whether some of their answers differed from what they *should* do, where around 2-4 people had answered it would differ. However, the participants were not further asked to give a reason in case they would feel discomfort speaking about it on the recording.

Senior level analysts were able to imagine how the proposed scenarios would manifest itself, and create flowcharts in their mind to explain what their actions would entail. If this study had focused solely on new or junior analysts, the threat scenarios might have been more challenging to follow through without more explicit guidelines, or it might have sounded more strictly along the lines of the team's playbook. For instance, the response steps taken by P3 for the case scenarios relied mostly on the team playbooks and policies - as they have not had much hands-on incident response task himself.

Another issue was that the sector of the participants' organisations varied so much in size that the participant's day-to-day tasks varied vastly, from managing phishing emails to attributing foreign states. The way each participant perceived and approached the threat scenarios differed a lot in terms of tools and expected roles. These meant that the format of the questionnaire and interviews had to clarify the assumptions being made by participants, including the sector or scale of a client organisation, or, for instance, the location of the server in question.

A sample of ten analysts were able to arrange and participate in the interviews. Not only was the sample size relatively small, but having the proportion of six different organisations for ten participants meant that it was a challenge to categorise the sparsely different experiences into common themes. Focusing on more team members from a small number of organisations may provide more insights involving inter-organisational procedures. With a larger sampling pool, double coding can be also implemented to reduce subjectivity of views in a long-term study.

C. FUTURE WORK

Based on the information of how senior-level analysts have addressed the threat scenarios, the subsequent work can target new or junior-level analysts on these scenarios to compare the analyses of their thought processes to that of the seniors. Should there be any recurring patterns of disparity between

juniors and seniors, it can further support the argument that tacit knowledge, or at least a specific angle of it, can be captured by comparing individuals with differing experience within the same domain of specialisation.

It will be necessary to understand how personal, academic, and professional backgrounds come to influence the responses upon analysts' incident detection. Besides the number of years that separate the seniors from the juniors, one can investigate how a background in, say, either mathematics or political science can have an impact in the way an analyst interprets incidents and perceives the overall team operation. If a study was extended on how the tickets were prioritised by analysts, and found that nearly all in a team prioritise only in one kind of incident tasks, that can signal the need to strategise analyst roles and responsibilities for load balance from the manager's point of view.

The thought-process diagrams offered an overview of minor and major tasks that would be taken as the scenarios were walked through by the participants. Breaking these tasks into components, and understanding how exactly a task component is established would provide a more in-depth insight about how each individual has their own manner of fulfilling a task, and who and what kind of procedures are involved. The focus can potentially be put more on the remediation aspects as those tend to be more context specific to sectors and post-incident state of the impact. Similarly, the term "*triage*" had been brought up by nearly all the analysts throughout the interview, but what it is comprised of varies greatly. It would be useful to distinguish what processes and procedures justify a triage phase within different sectors to understand how critical assets and priorities vary among SOCs.

VII. CONCLUSION

This study examined ways to probe for tacit dimensions relevant to incident response in SOC analysts as part of a groundwork for tacit knowledge management. It addresses the research questions by dissecting the differing perceptions of incidents in SOCs by current analysts, through interview questions and threat case scenarios. Our findings shed light onto the differing perceptions of same artefacts and incidents which may be the root to the lag or misunderstanding of activities within a team. Building on existing work on tacit knowledge in emergency teams and business organisations, these findings provide a foundation for further work on tacit knowledge management in SOCs. The findings also highlight the patterns and limitations of carrying out interviews with individuals as opposed to observing individual actions real-time. The study findings not only corroborate with the view on values of tacit knowledge, but also suggest novel ways to examine hidden dimensions of individual knowledge. The BPMN diagrams help visualise such flow of thinking to provide a more concrete understanding to the reader, and can be incorporated to design knowledge management frameworks in the future. The proposed revised SECI model is one way this can be realised.

ACKNOWLEDGMENT

The authors would like to express their gratitude to all the incident response experts for their valuable time spent in participating in the interviews. This research was approved by the Oxford Central University Research Ethics Committee (CUREC) (SSD/CUREC1A CS_C1A_18_019).

REFERENCES

[1] M. Polanyi, *Personal Knowledge: Towards a Post-Critical Philosophy*. Chicago, IL, USA: The Univ. Chicago Press, 1958.
[2] J. Muniz, G. McIntyre, and N. AlFardan, *Security Operations Center: Building, Operating, and Maintaining Your SOC*. Indianapolis, IN, USA: Cisco Press, Nov. 2015.
[3] A. S. Reber, *Implicit Learning and Tacit Knowledge: An Essay on the Cognitive Unconscious*. New York, NY, USA: Oxford Univ. Press, 1993.
[4] R. J. Sternberg, "What do we know about tacit knowledge? Making the tacit become explicit," in *Tacit Knowledge in Professional Practice: Researcher and Practitioner Perspectives*, R. J. Sternberg and J. A. Horvath, Eds. New York, NY, USA: Psychology Press, 19, pp. 231–23499.
[5] I. Nonaka and H. Takeuchi, "The knowledge-creating company: How Japanese companies create the dynamics of innovation," in *Harvard Business Review on Knowledge Management*. New York, NY, USA: Oxford Univ. Press, May 1995, pp. 8–9.
[6] E. Fischbein, "Tacit models and mathematical reasoning," *Learn. Math.*, vol. 9, no. 2, pp. 9–14, 1989.
[7] B. Lundvall and B. Johnson, "The learning economy," *J. Ind. Stud.*, vol. 1, no. 2, pp. 23–42, 1994.
[8] T. Haldin-Herrgard, "Difficulties in diffusion of tacit knowledge in organizations," *J. Intellectual Capital*, vol. 1, no. 4, pp. 357–365, Dec. 2000.
[9] M. S. Gertler, "Tacit knowledge and the economic geography of context, or the undefinable tacitness of being (there)," *J. Econ. Geography*, vol. 3, no. 1, pp. 75–99, Jan. 2003.
[10] M. Polanyi, *The Tacit Dimension*. Evanston, IL, USA: Routledge, 1966.
[11] R. Hodgkin, *Michael Polanyi-Prophet of Life, the Universe and Everything*. Times Higher Educational Supplement: London, U.K., Sep. 1991, p. 15.
[12] D. L. Schacter, "Implicit memory: History and current status," *J. Exp. Psychol.*, vol. 13, no. 3, pp. 18–501, 1987.
[13] I. Nonaka, "A dynamic theory of organizational knowledge creation," *Org. Sci.*, vol. 5, no. 1, pp. 14–37, Feb. 1994.
[14] I. Nonaka and N. Konno, "The concept of 'Ba': Building a foundation for knowledge creation," *California Manage. Rev.*, vol. 40, no. 3, pp. 40–54, 1998.
[15] J. R. Anderson, "Acquisition of cognitive skill," *Psychol. Rev.*, vol. 89, no. 4, pp. 369–406, 1982.
[16] D. C. Berry and Z. Dienes, *Implicit Learning: Theoretical and Empirical Issues*. Hove, U.K.: Lawrence Erlbaum, 1993.
[17] H. Taylor, "Tacit knowledge: Conceptualizations and operationalizations," *Int. J. Knowl. Manage.*, vol. 3, pp. 60–73, Jan. 2007.
[18] M. Szivos, "A practice-oriented classification of tacit knowledge for the research into creativity and innovation," *Polanyiana*, vol. 23, nos. 1–2, pp. 21–30, 2014.
[19] R. L. Ackoff, "From data to wisdom," *J. Applies Syst. Anal.*, vol. 16, no. 1, pp. 3–9, 1989.
[20] K. Weick, "Enacted sensemaking in crisis situations," *J. Manage. Stud.*, vol. 25, pp. 305–317, 1988.
[21] B. Dervin, "Interviewing as dialectical practice: Sense-making methodology as exemplar," presented at the Annu. Meeting Int. Assoc. Media Commun. Res. (IAMCR), Stockholm, Sweden, Jul. 2008.
[22] G. Klein, B. Moon, and R. R. Hoffman, "Making sense of sensemaking 1: Alternative perspectives," *IEEE Intell. Syst.*, vol. 21, no. 4, pp. 70–73, Jul. 2006.
[23] R. Sternberg, G. Forsythe, J. Hedlund, J. Horvath, R. Wagner, W. Williams, S. Snook, and E. Grigorenko, *Practical Intelligence in Everyday Life*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[24] J. C. Spender, "Organizational knowledge, learning and memory: Three concepts in search of a theory," *J. Org. Change Manage.*, vol. 9, no. 1, pp. 63–78, Feb. 1996.
[25] V. Ambrosini and C. Bowman, "Tacit knowledge: Some suggestions for operationalization," *J. Manage. Stud.*, vol. 38, no. 6, pp. 811–829, Sep. 2001.

[26] H. M. Collins, "The structure of knowledge," *Social Res.*, vol. 60, no. 1, pp. 95–116, 1993.
[27] F. Blackler, "Knowledge, knowledge work and organizations: An overview and interpretation," *Org. Stud.*, vol. 16, no. 6, pp. 1021–1046, Jul. 2016.
[28] A. Lam, "Tacit knowledge, organizational learning and societal institutions: An integrated framework," *Org. Stud.*, vol. 21, no. 3, pp. 487–513, 2000.
[29] I. Nonaka and T. Hirotaka, *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. New York, NY, USA: Oxford Univ. Press, 1995.
[30] G. G. von Krogh, I. K. , and I. Nonaka, *Enabling Knowledge Creation*. New York, NY, USA: Oxford Univ. Press, 2000.
[31] R. Boutellier, O. Gassmann, H. Macho, and M. Roux, "Management of dispersed product development teams: The role of information technologies," *R&D Manage.*, vol. 28, no. 1, pp. 13–25, Dec. 2002. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-9310.00077
[32] J. Roberts, "From know-how to show-how? Questioning the role of information and communication technologies in knowledge transfer," *Technol. Anal. Strategic Manage.*, vol. 12, no. 4, pp. 429–443, Dec. 2000, doi: 10.1080/713698499.
[33] G. Gerbner, "Toward a general model of communication," *Educ. Technol. Res. Develop.*, vol. 4, no. 3, pp. 171–199, Jun. 1956.
[34] R. A. Burkhard, "Knowledge visualization: The use of complementary visual representations for the transfer of knowledge. A model, a framework, and four new approaches," Ph.D. dissertation, Eidgenossische Technische Hochschule ETH Zürich, Zürich, Switzerland, 2005.
[35] M. J. Eppler, "Toward a pragmatic taxonomy of knowledge maps: Classification principles, sample typologies, and application examples," in *Proc. 10th Int. Conf. Inf. Visualisation*, London, U.K., Jul. 2006, pp. 195–204.
[36] M. Nickel and D. Kiela, "Poincaré embeddings for learning hierarchical representations," in *Advances in Neural Information Processing Systems* I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds. Curran Associates: Long Beach, CA, USA, 2017, pp. 6338–6347.
[37] A. M. MacEachren, M. Gahegan, W. Pike, I. Brewer, G. Cai, E. Lengerich, and F. Hardistry, "Geovisualization for knowledge construction and decision support," *IEEE Comput. Graph. Appl.*, vol. 24, no. 1, pp. 13–17, Jan. 2004.
[38] M. J. Eppler, "A comparison between concept maps, mind maps, conceptual diagrams, and visual metaphors as complementary tools for knowledge construction and sharing," *Inf. Visualizat.*, vol. 5, no. 3, pp. 202–210, Jun. 2006, doi: 10.1057/palgrave.ivs.9500131.
[39] M. Alavi and D. E. Leidner, "Knowledge management and knowledge management systems: Conceptual foundations and research issues," *MIS Quart.*, vol. 25, pp. 107–136, Mar. 2001, doi: 10.2307/3250961.
[40] R. T. Magaya, "Understanding decision making in security operation centres," Oxford Univ.: Oxford, U.K., Jun. 2017.
[41] R. K. Wagner and R. J. Sternberg, "Practical intelligence in real-world pursuits: The role of tacit knowledge," *J. Personality Social Psychol.*, vol. 49, no. 2, pp. 436–458, 1985.
[42] P. Busch, *Tacit Knowledge in Organizational Learning*. Philadelphia, PA, USA: IGI Publishing, 2008.
[43] J. Leprohon and V. L. Patel, "Decision-making strategies for telephone triage in emergency medical services," *Med. Decis. Making*, vol. 15, no. 3, pp. 240–253, Jul. 2016, doi: 10.1177/0272989X9501500307.
[44] P. Busch, D. Richards, and C. N. G. K. Dampney, "The graphical interpretation of plausible tacit knowledge flows," in *Proc. Asia–Pacific Symp. Inf. Vis.*, vol. 24, pp. 37–46, 2003.
[45] P. A. Busch, D. Richards, and C. N. G. K. Dampney, "Visual mapping of articulable tacit knowledge," in *Proc. Asia–Pacific Symp. Inf. Vis.*, vol. 9, 2001, pp. 37–47.
[46] P. Benner and C. Tanner, "Clinical judgment: How expert nurses use intuition," *Amer. J. Nursing*, vol. 87, no. 1, p. 23, Jan. 1987.
[47] J. M. Ahrend, M. Jirotka, and K. Jones, "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2016, pp. 1–10.
[48] S. C. Sundaramurthy, J. McHugh, X. S. Ou, S. R. Rajagopalan, and M. Wesch, "An anthropological approach to studying CSIRTs," *IEEE Secur. Privacy*, vol. 12, no. 5, pp. 52–60, Sep. 2014, doi: 10.1109/MSP.2014.84.
[49] V. L. Patel, G. J. Groen, and J. F. Arocha, "Medical expertise asa function of task difficulty," *Memory Cognition*, vol. 18, no. 4, pp. 394–406, Jul. 1990, doi: 10.3758/BF03197128.
[50] Object Management Group. *BPMN, CMMN and DMN Specifications at OMG (Object Management Group)*. Accessed: Aug. 8, 2019. [Online]. Available: https://www.omg.org/intro/TripleCrown.pdf
[51] Object Management Group. *Business Process Model and Notation BPMN Version 2.0*. Accessed: Dec. 2, 2020. [Online]. Available: https://www.omg.org/spec/BPMN/2.0/PDF/
[52] E. Aroms, *NIST Special Publication 800-61 Revision 1, Computer Security Incident Handling Guide*. Paramount, CA, USA: CreateSpace, 2012.

SELINA Y. CHO received the M.Sc. degree (Hons.) in information security from the Royal Holloway, University of London, in 2015. She is currently pursuing the Ph.D. degree with the Centre of Doctoral Training programme in cyber security, University of Oxford. Her master's dissertation elaborated on the concept of security through obscurity through the designs in cryptographic obfuscations and image steganography. Prior to her doctoral research, she worked as a Security Consultant at energy and startup sectors. Her research interests include several vectors of cyber-enabled crime, including money laundering, ransomware, and virtual goods and identity theft.

JASSIM HAPPA received the B.Sc. degree (Hons.) in computing science from the University of East Anglia, in 2006. He is currently pursuing the Ph.D. degree in engineering (computer graphics) with the University of Warwick, after a year of working as an Intrusion Detection System (IDS) Analyst. He is also a Lecturer in information security with Royal Holloway and a Visiting Lecturer with the Department of Computer Science, University of Oxford. He defended his Ph.D. in early 2012, and worked as a Research Fellow at Oxford, from late 2011 to 2019. In 2019, he joined Royal Holloway. In recent years, he has spent his research efforts on cybersecurity topics, such as analytics, visualization, threat modeling, situational awareness, risk propagation, resilience, decision support, privacy, and cyber threat intelligence. Teaching wise, he tutors and lectures a variety of computer graphics and security related-subjects at both Royal Holloway and Oxford.

SADIE CREESE is currently a Professor of cyber security with the Department of Computer Science, University of Oxford. She teaches threat detection, risk assessment, and operational aspects of cyber security. Her current research portfolio includes developing mathematical models for calculating cyber-value-at-risk for an organization, threat modeling, and intrusion detection, including insiders, visual analytics for understanding and communicating cyber security postures, logics for predicting risk propagation, resilience strategies, privacy vulnerability, threats to distributed ledgers, and understanding the nature of cyber-harm. She also researches what constitutes cyber security capacity for a nation, and how to deliver it, working with international organizations, nations, practitioners, and academics around the world. She is a Principal Investigator on AXIS Insurance Company-sponsored project Analyzing Cyber Value-at Risk focused on developing a method for predicting the range of potential losses arising from cyber-attacks taking account of risk control practices. She was the founding Director of the Global Cyber Security Capacity Centre (GCSCC), Oxford Martin School and continues to serve as a Director. She was the founding Director of Oxford's Cybersecurity network launched, in 2008, and now called CyberSecurityOxford, and is a member of the Advisory Board for the World Economic Forum's Centre for Cybersecurity. She is a Fellow of the Worcester College, Oxford.