# Capturing Tacit Knowledge in Security Operation Centers

Tacit knowledge is a type of knowledge, insight, and intuition that comes from years of experience. 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.

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.

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.

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.

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.

The study aims to investigate how tacit knowledge can be externalised and transferred to others by studying existing communication and operational mediums and challenges. The research aims to answer the following questions:

- Are there identifiable patterns in thought processes between analysts with similar experience?
- Do analysts prioritise incidents based on principles or social factors?
- Do media exist in communicating threat and defence knowledge?
- What are the desirable traits of an effective SOC analyst?

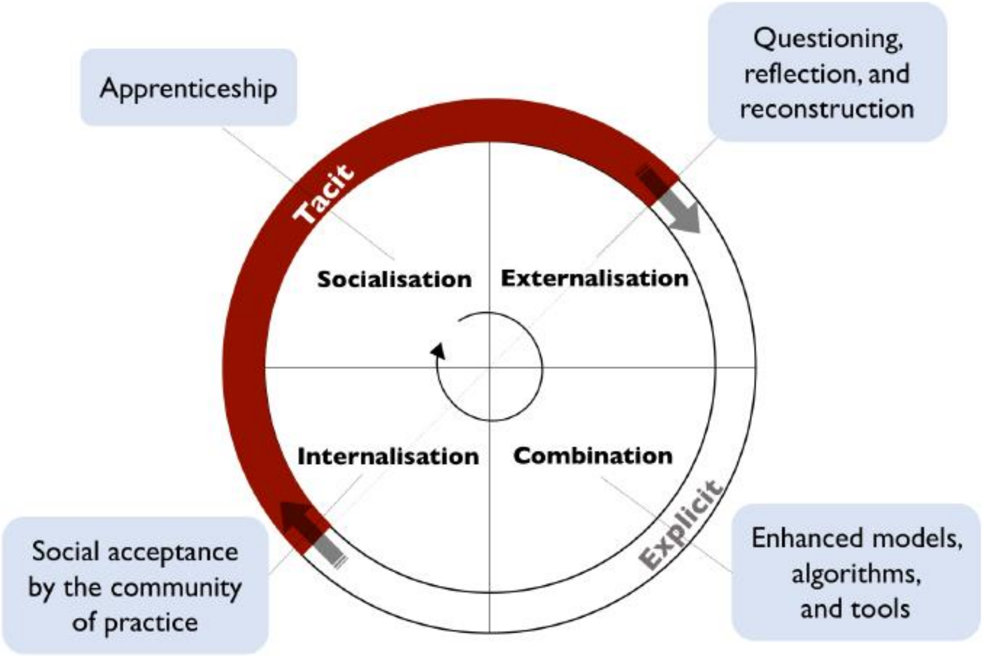
The focus of the investigation is not so much on whether one's choice is more effective than another, but understanding whether choices differ at all and, if so, the influencing factors behind such choices.

Tacit knowledge is commonly associated with cognitive skills such as subjective insights, intuition, and mental models, as well as ``know-hows'' or skills gained through repeated exposure to hands-on work. 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. 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.

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 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.

Sense-making is a process by which people give meaning to their experience. Those with proficient sensemaking abilities are able to map a credible route through an uncertain situation, and refine it according to new relevant information.

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. Techniques for explicit knowledge have been identified through more formal training measures as schools, libraries, books, data media, written rules, and procedures


Apprenticeship
Questioning, reflection, and reconstruction
Tacit
Socialisation
Externalisation
Internalisation
Combination
Explicit
Social acceptance by the community of practice
Enhanced models, algorithms, and tools

- **Socialisation**: Tacit knowledge belonging to one person is transferred to other employees through direct contacts.

- **Externalisation**: Tacit knowledge is made comprehensible to others through various modes of expression, such as images, words, or metaphors.

- **Combination**: New and existing explicit knowledge is now combined to tackle the existing problem or task.

- **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.

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.

The Socialisation stage consists of promoting more in-person contacts with the analysts across different team locations. This appeared to be significant source of gaining insight and building trust between different analysts. The interactions should not only be encouraged internally but also with third-party vendors and contractors to provide fresh insights about any new findings and suggestions about the SOC operation that the team alone could not detect.

Apprenticeship 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 one participant called - the ``watch and learn'' method over merely reading off the text guidelines, for both effectiveness and ease of understanding.

The Externalisation stage includes an environment where new analysts can apply their newly acquired knowledge in action. One participant 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.''

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.

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. 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.

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.

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 prioritise and delegate tasks from the start.

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.

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.