Formalizing and Integrating User Knowledge into Security Analytics

Knowledge Types

Explicit knowledge is mainly referred to as machine-based knowledge. Accordingly, this term denotes knowledge that machines can read, process and store. In the context of security analytics, we distinguish three types of explicit knowledge in the further course of the work, which can be distinguished from each other by their intended use for security analytics.

- **Models** for machine learning approaches, neural networks, and the like are primarily used for anomaly- based detection mechanisms. This knowledge allows a machine to detect outliers and evaluate them to some extent as to whether they indicate malicious or undesirable behavior.

- **Signatures and rules** are the basis for more traditional security analytics approaches such as SIEM systems and their correlation engines for detecting indicators of compromise (IoC).

- **Threat Intelligence and forensic** evidence describe the results of primarily manual, in-depth analysis of suspected or actual incidents and include extensive information on the attackers' modus operandi, identifiable traces, suspect groups or individual perpetrators, and many other details. Because of their level of detail, Threat Intelligence and Forensic Reports allow answering "how" questions.

Implicit knowledge can only be possessed by humans and is very specific to each individual. Humans improve their Implicit knowledge by combining new insights with existing knowledge. The existing knowledge itself can in turn be divided into, on the one hand, domain knowledge and, on the other hand, operational knowledge. In the domain of security analytics (SA), we also consider another new type of tacit knowledge to be highly relevant: situational knowledge.

- **Domain Knowledge**: Generally speaking, it describes what people know about a particular context or on a specific topic (the "domain"). In SA, this type mainly encompasses the concept of situational awareness.

- **Situational knowledge** describes the ability of any employee of an organization to perceive unusual events or suspicious behavior. The relevant events range from receiving suspicious mail, which represents a possible phishing attempt, to identifying a private storage medium connected to a corporate device.

- **Operational knowledge** in the context of SA refers to the ability of a human to operate specific systems. Specifically, employees with SA-related operational knowledge can adequately operate a company's security systems.

These three different subsets of tacit knowledge are necessary to detect and resolve both cyber and cyber-physical attacks as completely as possible.

Knowledge Conversion

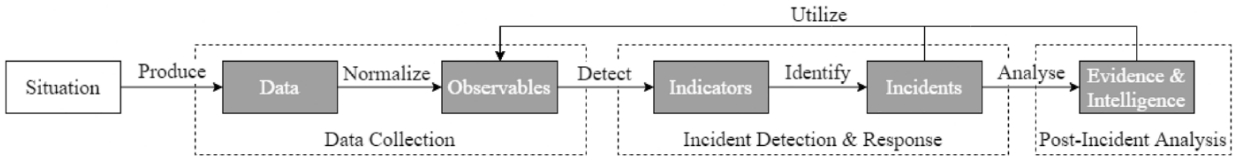
- **Internalization** describes the process of making explicit knowledge available to users, who can then perceive this knowledge using the implicit operational knowledge available to them and convert it into implicit security domain knowledge.

- **Externalization**: When tacit knowledge, especially implicit domain knowledge or implicit situational knowledge, is transferred into a form that can be processed by computers, we refer to this as the process of externalization. Externalized tacit knowledge can thus be read, persisted, and eventually processed by computers. Structuring and formalizing indicators, incidents, and corresponding evidence into CTI also represents a form of externalization.

- **Combination**: The conversion process of combination describes the exchange of knowledge from two or more explicit knowledge bases.

- **Collaboration**: this knowledge conversion specifies that people can learn from each other (i.e., increase their implicit knowledge) by collaborating.

We interpret the detection of security incidents, i.e., attacks on an organization's assets, to be the the essential task of security analytics. A cohesive approach to implementing this task requires comprehensive data collection combined with powerful analytical capabilities and the integration of any available knowledge base.



The Incident Detection Lifecycle is divided into three overarching phases, which are executed to detect, resolve, and understand incidents.

The starting point of the Incident Detection Lifecycle is some real event within an organization—that is, something that "happens"— which can be physical or digital.

The first of these phases is the Data Collection. Each situation produces raw data which could be relevant for the detection of possible attacks. These data are normalized (and sometimes standardized) in the first phase of the lifecycle, producing so-called observables.

This second phase of the lifecycle can be summarized under the terms Incident Detection & Response. This phase aims to detect actual incidents, capture the impact, and contain the incident as quickly as possible. The first step is the detection of indicators, which are often also referred to as Indicators of Compromise (IoC). These indicate potentially suspicious activities and behaviors.

However, IoCs can also indicate unusual but not malicious behavior. For this reason, a further step is necessary to identify actual incidents from detected indicators. For this purpose, it is necessary to correlate indicators with each other and possibly to include additional data or observables in the analysis process. If an incident is identified, direct measures for defense and containment must be initiated in this lifecycle phase.

After the initiation and implementation of countermeasures and containment actions, the third phase of the Incident Detection Lifecycle, the Post-Incident Analysis, is carried out. In this phase, careful and intensive analyses of an incident produce further vital artifacts. On the one hand, evidence which can be used in possible judicial proceedings is collected in this step through forensic analysis. On the other hand, threat intelligence is generated through the attribution of the identified incident.

With the use of explicit knowledge signatures only indicators and incidents that were known apriori and whose signatures were integrated into the system, can be detected. Behavior-based methods are better at classifying unknown indicators but often tend to generate a large number of false positives. By incorporating human domain experts, these two fundamental problems can be eliminated or at least mitigated to some extent.

Cyber-physical incidents are only detectable if knowledge about security incidents in general (security domain implicit knowledge) and knowledge about the physical aspects in particular are combined. In addition, situational knowledge is necessary for the incident to be recognized in the first place. Therefore, only incidents for which all three types of knowledge are combined can be detected. All incidents that do not reside on the intersection cannot be detected by humans, which is why these areas potentially constitute a blind spot in the Incident Detection Lifecycle and thus have to be minimized.

Three knowledge gaps limit the Incident Detection Lifecycle or prevent security incidents from being detected.

- The first gap that can be identified is the lack of possibilities to externalize implicit situational knowledge. For example, if an employee notices a security incident, they need to be able to contribute their observations to the Data Collection phase of the Incident Detection Lifecycle.

- The next gap stems from the lack of general implicit operational knowledge. Therefore, it must be ensured that the required implicit operational knowledge is reduced so that people without expert knowledge can operate security mechanisms.

- Collaboration between novices and experts within the Incident Detection Lifecycle is vital. Collaboration can help create a central knowledge base in the Incident Detection Lifecycle in which as much relevant information as possible is brought together.