Enhancing Collaboration between Security Analysts in Security Operations Centers

Damien Crémilleux, Christophe Bidan, Frédéric Majorczyk, Nicolas Prigent

Enhancing Collaboration between Security Analysts in Security Operations Centers

Damien Crémilleux[1], Christophe Bidan[1], Frédéric Majorczyk[1,2], and Nicolas Prigent[3]

[1] CentraleSupélec {damien.cremilleux,christophe.bidan}@centralesupelec.fr
[2] DGA-MI frederic.majorczyk@intradef.gouv.fr
[3] LSTI neeko@neekotech.fr

Abstract. Security Operations Centers (SOCs) collect data related to the information systems they protect and process it to detect suspicious activities. In this paper we explain how a SOC is organized, we highlight the current limitations of SOCs and their consequences regarding the performance of the detection service. We propose a new collaboration process to enhance the cooperation between security analysts in order to quickly process security events and define a better workflow that enables them to efficiently exchange feedback. Finally, we design a prototype corresponding to this new model.

Keywords: Security and privacy · Intrusion detection systems · Network security · Collaboration · Security Operations Center

1 Introduction

Most of the large information systems are monitored by a Security Operations Center (SOC). A typical SOC collects from thousands to millions of security events every day [1] with the objective of finding which of them require priority attention. The high volume of irrelevant security events and the way they are currently handled lead to the fact that real attacks are often missed and ignored. Consequently, there is a delay up to several months between an intrusion and its discovery. Security analysts in SOCs being put under pressure results in poor judgments when looking at security events and in a high burnout rate [2].

In order to improve efficiency of SOCs and solve the problems stated above, this paper proposes the following contributions:

- An analysis of the current limitations of SOCs, in Section 2. This paper describes SOCs with insight gained from interviews with security analysts.
- A new process to enhance the cooperation between the different security analysts, in Section 3. This process is established with the creation of rules to define security meta-events and the creation of a specific feedback loop between groups of security analysts.
- A design to support our new process, in Section 4. The limitations and the feedback from the evaluation we performed help our design of a prototype for a visualization tool dedicated to a better collaboration.

2 Security Operations Centers and their limitations

We interviewed twelve security analysts, all male with one to ten years of experience in the field, in one-to-one interviews. During the interviews, experts provided insights regarding the collaboration happening in SOCs between Tier 1 and Tier 2 analysts. Tier 1 analysts, the biggest category in number, are responsible for continuously monitoring the alert queue, and for the quick triage of the security alerts. If there is a procedure in the knowledge base for a given event, they follow it, resulting in a qualified incident or a false positive. Otherwise the suspicious event is sent to Tier 2 analysts. Tier 2 analysts perform two main tasks. First, they analyze unknown events that are suspicious, and following the result of their investigation, create a new qualified incident if needed. Second, they manage the incidents and the creation of an appropriate response.

Based on our findings, we highlight the current limitations inside a SOC and divide them into two aspects: process and technology. The process issues are:

- *Lack of creativity.* Tier 1 analysts follow written procedures that severely limit creativity and they stay with what they know, resulting in failure to react appropriately to novel operational scenarios.
- *Lack of feedback.* Once their decision is made, Tier 1 analysts lose track of their actions. They do not have the result of the analysis of Tier 2 analysts and therefore will not know if they acted correctly.
- *Repetition of the same task.* Tier 1 analysts perform repetitive tasks following known procedures. This aspect is also true for Tier 2 analysts. Because Tier 1 analysts keep sending the same type of events, Tier 2 analysts have to deal with them. The consequence is a loss of time and a diminished appreciation for the work accomplished by Tier 1 analysts.

The technology issues are:

- *Numerous data, and numerous data sources that are not linked.* Even with only IDSes alerts as main data source, Tier 1 analysts face a huge volume of security events and only have seconds or minutes to accomplish their task. This challenge also exists for Tier 2 analysts, the amount of data given to them being prodigious, in the order of millions of security events. Moreover the data sources are various: antivirus, IDSes alerts, system events, network traffic, etc, and are not necessarily linked one with the others. Thus an expertise in each of these data sources is required, and correlation and pivoting between pieces of data is a difficult task.
- *Progression of threat escalation.* It is particularly important to evaluate if an event is isolated or if it is a part of a bigger scenario. The knowledge of the current context, threats and incidents currently happening help the security analysts to take a decision.
- *Rhythm of networks.* Security analysts learn the rhythm of the network. They recognize frequent events and know which will follow them. The understanding of such events and of the typical amounts of errors in the system is currently insufficiently exploited, even if we should mention that it is a part of the collection strategy required in [3].

3 A new collaboration process

The limitations exhibited persuade us to propose a new collaboration process which introduces the concept of security meta-event and the creation of a feedback loop between Tier 1 and Tier 2 analysts. The purpose of security meta-events is to avoid, for Tier 1 analysts, to have to continuously deal with the same type of events. Instead of repeating the same procedures, events are regrouped in a security meta-event, an identified sequence of similar security events belonging to the same data source. Security meta-events should be easily created by Tier 1 analysts. Tier 2 analysts should have the possibility to refine it and collaborate around it, so we use rules based on signature to describe security meta-events. Rules are designed so that all analysts can quickly grasp their meaning. When creating a rule for a security meta-event, the key point for a Tier 1 analyst are: a name, a comment (used to explain more precisely the rule), a filter (stating which events should match with pattern matching).

When manipulating rules Tier 2 analysts have the possibility to improve them with: a label (the status of meta-events linked to the rule), a person (the Tier 2 analyst in charge of the remediation), an end date if needed, an interval (the minimum time needed between two matched events to create a new security meta-event). The values of the label field can be a suspicious meta-event, qualified incident, or noise (false positive alerts). Suspicious meta-events are those which are composed of security events currently happening in the system. A Tier 2 analyst has not looked at this meta-event and a response has not yet been found. By contrast, after an examination by a Tier 2 analyst, the meta-event can become a qualified incident. The rule describing this security meta-event can now be used to create future qualified incidents, if the analyst estimates that it is important to know when new events matching this rule arrive.

We now present in Figure 1 a new workflow we designed that uses the concept of security meta-events and implements a feedback loop to empower Tier 1 analysts. The differences it exhibits with the current workflow used in SOCs are shown in bold and brown. Tier 1 analysts are now sending suspicious meta-events instead of single events, when faced with unknown suspicious security events. By using meta-events defined by rules, significant time can be saved. After the analysis of the meta-event, Tier 2 analysts have the possibility of modifying the rule if they estimate that it can be improved. Whatever the result, feedback is given to Tier 1 analysts, empowering them. They can now create rules, and improve their knowledge over time with the continuous feedback given by Tier 2 analysts.

At the beginning, there are no rules inside the system. With the constant creation and modification of rules, Tier 1 analysts see the rate of irrelevant events diminish so they can be more efficient in accomplishing their task. This workflow facilitates the work of Tier 1 analysts while still keeping them under the supervision of Tier 2 analysts. The limitations regarding the lack of creativity and feedback for Tier 1 analysts are also addressed since Tier 1 analysts have to think about the creation of relevant rules and understand the changes made by Tier 2 analysts to their rules. We advocate that this improvement helps Tier 1

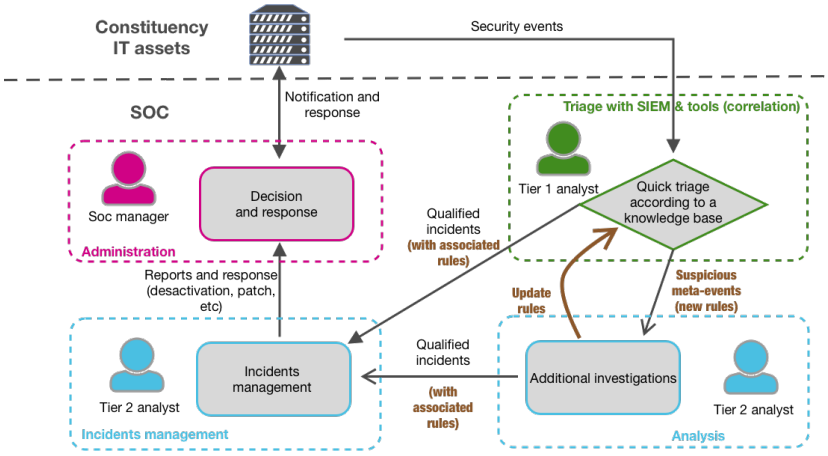

Fig. 1. Proposed workflow for a SOC.

analyst stay motivated, to accomplish their task more easily and results in an improved efficiency of the SOC.

An evaluation was performed in order to validate this new process. Eleven experts out of the twelve performed the job of a Tier 1 analyst with [4] on the VAST 2012 challenge, (50000 IDS alerts over three days of capture). We ask them to judge if this new process is improving the efficiency of a SOC. With an average rating of 4.1 out of 5, the experts answer positively. They judged that meta-events were a good way to keep the volume of irrelevant security events low. The fact that security events were sent in groups, in meta-events, was declared very useful for both Tier 1 and Tier 2 analysts. The introduction of rules to enhance the collaboration between analysts was appreciated. Rules and their comments helped the analysts to quickly understand the context of the security events. Three expert pointed out that the skill of Tier 1 analysts was a limiting factor of our solution. However, we advocate that this was already the case before the introduction of meta-events. Similarly, we believe that Tier 1 analysts will improve their knowledge and so the rules they create thanks to the feedback of Tier 2 analysts. Another point of interrogation for two experts was the evolution of the rules and their growing number over time. The interface presented in the next Section tries to answer this point.

4 Our application design

The results from the evaluation and our study were used to design an interface to exchange rules between analysts. This interface addresses the last two technical challenges described in Section 2, progression of threat escalation and rhythm of networks, by proposing quick situational awareness, visual correlation of incidents, visual reconstruction of attack scenarios. The design of our prototype is made of different views. The objective of the timeline view is to provide

situational awareness, and the scenarios and rules views are dedicated to these types of data. The different views are accessible to all analysts while modifying data is limited to Tier 2 analysts.

Fig. 2. Timeline view.

The timeline shown in Figure 2 is the central view, provides high-level awareness of the rhythm of the network and enables visual correlation of incidents. It is divided into three sections, according to a gradient of gravity. The unclassified alerts are represented on a time chart in zone (A), giving an idea of the volume of security events arriving. The suspicious meta-events are then shown in the zone (B) and qualified incidents in zone (C). The color of the meta-events and the incidents on the timeline are indicators of the related scenarios of attacks, if unknown grey is used. The timeline form enables the analyst to understand the time relation between the security events and redraw the story behind them.

Analysts can access scenarios in the scenarios view. Sparklines are used in small multiples[4] to display the current trend for each scenario over time. For each scenario, analysts have access to the number of rules and events composing it. They can modify its caracteristics or delete it if needed. New scenarios can be added. The rules view is based on the same principle that the scenario view.

5 Related Work

Sundaramurthy et al. [2] performed anthropological studies of SOCs, evaluated the security analyst burnout in SOCs, and tried to find causes. Four factors are cited as the origin for the high burnout rate: lack of skills management, lack of empowerment, insufficient possibility to express creativity and lack of growth. The collaboration inside a security team is also addressed by Rajivan et al. [5]

[4] A series of similar graphs with same scale and axes to compare them easily.

who focus on the team situational awareness. Some observations are relevant to our subject, even if the teams in their study are not working in a SOC. The authors emphasize the need for a better collaboration and cooperation inside security analysts teams. A collaboration tool is proposed with OCEANS [6] with web-based interface, however designed only for Tier 2 analysts.

Timelines are present in [7], a visual system for analyzing, examining and investigating time-series data. In [8] analysts can investigate network flow using timelines with specific glyphes to plot events. NStreamAware [9] leverages timelines with sliding slices and feature selection. L. Franklin et al. propose a design for an alerts management system resulting in an inbox metaphor prototype [10], with mail displayed on a timeline. In our proposition the design integrates the concept of timeline with the different teams and escalation process of SOCs.

6 Conclusion

In this paper, we have presented a description of the workflow currently in place in SOCs. We have emphasized their limitations deriving in a high turn over and detrimental to the efficiency of the SOC. In order to enhance the collaboration between security analysts working inside a SOC, we have proposed a new collaboration process and a design prototype using security meta-events defined by rules, with a feedback loop between Tier 1 an Tier 2 analysts. The evaluation shows that our contribution makes a positive impact with respect to SOC efficiency and experts of the field acknowledge our approach.

References

[1] C. Zimmerman. *Ten Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, Oct. 2014.

[2] S. Sundaramurthy et al. "A Human Capital Model for Mitigating Security Analyst Burnout". In: SOUPS '15. USENIX Association, July 2015.

[3] *Prestataires de détection des incidents de sécurité*. Référentiel d'exigences. ANSSI, 2017.

[4] D. Crémilleux et al. "VEGAS: Visualizing, exploring and grouping alerts". In: *NOMS*. IEEE, 2016, pp. 1097–1100.

[5] P. Rajivan and N. Cooke. "Impact of Team Collaboration on Cybersecurity Situational Awareness". In: Lecture Notes in Computer Science. Springer, 2017.

[6] S. Chen et al. "OCEANS: Online Collaborative Explorative Analysis on Network Security". In: VizSec '14. 2014.

[7] F. Stoffel, F. Fischer, and D. A. Keim. "Finding Anomalies in Time-Series Using Visual Correlation for Interactive Root Cause Analysis". In: VizSec '13. 2013.

[8] D. Phan et al. "Visual Analysis of Network Flow Data with Timelines and Event Plots". In: Mathematics and Visualization. Springer Berlin Heidelberg, 2008.

[9] F. Fischer and D. A. Keim. "NStreamAware: Real-Time Visual Analytics for Data Streams to Enhance Situational Awareness". In: VizSec '14. 2014.

[10] L. Franklin et al. "Toward a Visualization-Supported Workflow for Cyber Alert Management Using Threat Models and Human-Centered Design". In: VizSec '17. 2017.