**Use Cases for Enterprise Cybersecurity**

# Making SIEM efficient with selection and fine-tuning

**Use cases are the essential core of any Security Information and Event Management (SIEM). Use cases are used to identify threats and output them in the SIEM's messages. However, an excessive number of use cases or the selection of the wrong ones for a particular company often lead to false alerts and to actual threats either not being detected or being lost in a mass of alerts. It is therefore important to select use cases and adapt them to the respective company in such a way that they can cover as many threat scenarios as possible with as little effort as possible. In doing so, it makes sense to orient oneself on the known attack vectors and thus on a framework. Tuning, the adaptation of the use cases to the existing IT, is also important.**

A Security Information and Event Management (SIEM) collects messages, events and log files of the systems in companies. This data is used to issue alerts on threats and cyber attacks in real time so that analysts can respond to them as quickly and appropriately as possible. The basis for this is provided by previously defined use cases. The SIEM uses them to identify the relevant events in the large volumes of data: They describe scenarios with suspicious behavior, e.g., unusual logon activities, the addition of new users, or an atypical use of ports. In view of this, the goal must be to select the smallest possible number of use cases, with which one simultaneously achieves the greatest possible coverage of relevant attack scenarios. This can be achieved by focusing on known attack vectors, such as those specified in the MITRE&ATT&CK framework - use cases should map and take into account the most important techniques and tactics from this. The MITRE&ATT&CK framework presents numerous different approaches from a forensic perspective and provides examples. It thus provides the optimal basis for deriving use cases; IT security managers therefore do not have to build hundreds of use cases themselves to cover all possible scenarios, but can select the ones that make the most sense for them. IT security partners like SECUINFRA also ideally have their own use case library. Developed by their cyber defense experts, this ensures maximum effectiveness of use cases at high efficiency for the customer. The use of monetary and time resources is thus kept as low as possible. When selecting the use cases, it is also advisable to coordinate closely with the security and IT risk management departments in order to find out from practical experience which areas the SIEM needs to cover for the company in question.

In parallel, it makes sense to monitor operating systems, servers and clients with user and rights management. They are the central points in the company and are suitable as a starting

point, since most cyber attacks target users, clients and servers. In addition, consideration must be given to how IT systems with in-house developments can be checked so that no security-relevant anomalies occur there either. The larger the company, the more likely it is that such in-house developments will exist outside the framework.

**Tuning the use cases**

The selected use cases must then be implemented taking into account the company's specifics and then adapted to them - they require tuning. In the process, they are primarily cleansed of false positives, i.e., false alarms. As part of this, sets of rules are adapted that evaluate the log messages. In addition, whitelists for standard alarm-triggering events are integrated in the event that these events are not critical. For example, if a data readout takes place, this event may already trigger an alarm and indicate a cyber attack. However, if this is done by an authorized system user in the company, the event is not critical - and the alarm would be a false positive. Another example of this is access to sensitive data in a database, but this is not caused by attackers from outside, but originates from administrators. If it is then determined in the analysis phase that there are too many false positives, optimization adjusts the set of rules with white and black lists.

Even if the first optimization is as effective as possible, a 100% solution cannot be achieved immediately. Tests must be carried out to check whether, in the event of an anomaly, the rules will continue to apply in the future. Experience shows that it takes up to three months before no or very few false positives are caused. In rarer cases, even processes that run only every few months can trigger false positives. Fine-tuning the use cases is therefore an ongoing and quite time-consuming task. This is because each use case must be monitored for its function and false positives over the entire runtime. However, the effort can be minimized by clever preselection.

**Implement tuning as a continuous task**

In addition, a SIEM is a living system. If something changes in the infrastructure, e.g. operating systems of the log sources are updated, this can lead to the fact that originally adapted rules are no longer optimally effective. Changes in the system environment can create new false positives if an old set of rules no longer applies, log messages have changed with an update, or the set of rules that checks the messages logs too much - or not at all. This makes continuous readjustment necessary. The cycle thus extends from analysis, findings, optimization, testing, importing and changes to the use cases back to analysis, so that the process must be continuously re-implemented.

Tuning runs most efficiently when the teams of use case tuning and analysts work together to find the best setup. It therefore requires an interplay of implementation, evaluation and consultation with the business departments.

Targeted tuning as well as optimization therefore contribute significantly to the cost-effectiveness of security monitoring, as it significantly reduces the workload of security analysts and makes correspondingly less personnel effort necessary. A setting that throws up 90% false positives, for example, requires a great deal of manpower, since all cases must be evaluated individually in order to filter out actual threats - after all, a real attack could be behind a report. Tuning, however, makes manual effort of this kind largely obsolete and relieves organizations of the need to manage excessive alert volumes. In addition, suboptimally implemented rule sets require more system resources. They are less performant, which increases the load on the SIEM - in the end, it makes a significant difference whether five or 20 servers have to be operated for the SIEM if the rule sets cause correspondingly high loads.

**Communication is the be-all and end-all**

One group of people is often particularly affected by SIEM use cases or the scenarios depicted: the company's workforce - in other words, individual employees. At the personnel level, this often gives rise to the concern that user-related use cases could represent supposed vehicles for employee monitoring. Although the works council or staff representatives are not involved in the selection of use cases, it makes sense to communicate that the SIEM will not be misused to create evaluations of employee performance or to track them at HR manager level, so to speak. It must be clear that the SIEM only detects security-related anomalies and does not report that an employee is supposedly working too slowly.

**Implement use cases with specialized IT security partners**

The support of external partners is indispensable when selecting SIEM use cases, since the entire process requires know-how and experience that are usually not available in companies and cannot be built up in a short period of time. However, if sufficient staff is available, they often still cannot cope with the amount of tasks that a SIEM entails - they are more than busy with its implementation or building up the SOC (Security Operation Center) and have no time for selecting and implementing use cases.

An experienced IT security partner, on the other hand, can work more efficiently and effectively. This eliminates the tedious search for usually expensive personnel, and the company can also benefit from a transfer of knowledge.

Despite the vast experience that an external partner brings to the table, collaboration with the company's security and IT risk management is essential, as they have an understanding of the organizational context of the use cases. Because one thing is clear: The service provider needs this internal support, for example, to be able to react correctly to the log messages, events and alarms of the SIEM system. That's why it's important to start communicating early. For example, kickoff meetings with specialist departments are a good way to pick up all the parties involved, present the plan and goal, and obtain support. If the teams and decision-

makers involved know each other, collaboration is more harmonious and misunderstandings and problems can be quickly resolved.

On the other hand, it is not very helpful to immediately switch to alarm mode when the first hurdles appear. For example, if the first rules have been written, but the systems have not been connected or log and event generation on systems have not been configured to the required extent, early evaluation is not a good idea. Instead, professional communication should be established that picks up all parties involved and points out possible solutions.

**Conclusion**

In addition to selecting the appropriate use cases, fine-tuning them is essential for an efficiently operating SIEM. Otherwise, the wrong and frequent alarms can quickly lead to an inefficient system that paralyzes the company more than it supports it. This requires know-how and expertise - companies therefore benefit from the support of external partners when selecting and implementing the use cases for the SIEM. After all, they are often unable to handle the task on their own, either in terms of personnel or content. In addition, the selection and fine-tuning of use cases is not a one-time task, because even minor changes to the IT system can make readjustments necessary. Furthermore, new threat scenarios are constantly emerging, which may need to be addressed by adapting existing use cases or developing new ones. The selection of suitable scenarios alone is not enough; the use cases require continuous adaptation and fine-tuning. By understanding the SIEM as a quasi-living system in this way, a cycle of continuous optimization is created.

**Author:** Jan Kilby, Senior Cyber Defense Consultant
SECUINFRA

**Further Information:** https://www.secuinfra.com/en/services/siem-consulting/

**Press contact:** SECUINFRA GmbH
Svenja Koch
Stefan-Heym-Platz 1
10367 Berlin
Deutschland
Tel. +49 (0) 160 921 633 44
svenja.koch@secuinfra.com