# SIEM: this is the mirage of Computer Security

**By Cyrille HERDHUIN,**
Cyber Security professional at SCOR

For those who do not know, a SIEM is: "Called also SEM (security event management) or security event information management (SEIM) or SIEM (security information and event management), They allow the management and correlation of logs. We speak of correlation because these solutions are equipped with correlation engines that make it possible to link several events to the same cause. " Thank you, Wikipedia!

To put it simply: the SIEM can take two innocuous events apart to create a new one. Because nothing beats an example:

**Log 1:** Mrs Michu managed to connect to her post in Paris at 10:01 GMT + 1. Everything is fine.

**Log 2:** Mrs. Michu managed to connect to her post in New York at 10:04 GMT + 1. Everything is fine.

Following the passage in the correlation engine:

**Log 3:** Alert! Mrs. Michu has the gift of ubiquity. Nothing goes well.

You will understand, it is very convenient to realize that there is an anomaly on the SI. This gives another angle of approach, new visibility. This makes it possible to address rather trivial points as points that are much more complex and potentially based on several technologies if the latter generate logs.

Great! We have just found the solution to all our security problems on the IS. The SIEM, like an Oracle, will see everything and tell us everything. Disillusionment.

The nerve center of a SIEM solution is its correlation engine. But this engine to move forward needs to know what to rely on. This is where the added value of SIEM comes in: Rules / Signatures. Without a rule or signature, the SIEM does not know that the fact that Mrs. Michu has the gift of ubiquity, and this is a problem for me.

Let's dwell on these rules and ask the question: where do they come from? In the best case, they come from a risk analysis. Risk analysis, which itself is drawn from feedback and / or incidents that have arrived and / or feared.

This is an existing knowledge. Being the SIEM can be compared to an antivirus or virtual patch. The SIEM will include rules / signatures based on scenarios. The SIEM will bring us back to what we already know. No request exists to query the logs on behavior that we do not know. If we take this vision to the extreme, it is possible to say that if we know what we fear, the SIEM is the downstream means of not solving a known security problem upstream.

The role of the SIEM should be to temporarily highlight certain points or to control known security issues. It allows to be a lever allowing to enter a virtuous circle within the company, in which each point reassembled must be corrected as and when.

But then a solution able to address even what we do not know is possible? Are we helpless in the face of this threat? Well no! We must focus on what is common to all attacks: deviant behavior. An attack, in essence, will create unexpected and abnormal behavior. If a deviation is observed, it can be identified and can be explained / remedied. For that there are tools that are based on statistical / mathematical models. We are no longer on an analysis via signatures but on empirical analysis.

Again, there is no magic solution, and a learning time (important) is to be expected. And the false positives will be daily. However, it ends up being refined and becoming more and more relevant.

In short, we must not confuse the tools. Each has its usefulness.

**So if I had to summarize:**

- If you want to address known issues: you need a SIEM
- If you want to address problems that are currently unknown: you need a behavioral analysis tool.

The two are not incompatible, you just need to target the need.

## And what is your need?