AXEL JOLLIS

Security Architect at ZENDATA

How did I deploy a SIEM-as-Code?

The emergence of the tool known as Security Information and Event Management or SIEM comes from the need of monitoring logs across an organization. The National Institute of Standards and Technology provides the following definition for SIEM: "Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface."

There's no such thing as perfection, and SIEM was no exception. As it stands, one of the main issues was the capacity to monitor and automatize our configuration changes. So, I decided to focus on a specific way of creating a SIEM: SIEM-as-code. The principle of SIEM-as-code is pretty basic: it's about being able to manage different SIEM configurations with continuous integration, testing and delivery. This means incorporating peer reviews, monitoring and alerting to changes, and debugging incident information. SIEM-as-code is an extension of known detection code that focuses solely on alerts, and also includes event logs ingestion management, SIEM architecture configuration and event logs enrichment management.

"As code" provides a wide range of advantages not usually found in traditional SIEMs:

Monitoring & Versioning: it provides an overview of SIEM modifications, making it possible to track problems related to alerts, monitor development time for each part of the infrastructure, and compare versions.

Modularity & Community: it must be reusable, modular and shareable. This means it must be a continuous service, which is a real headache when it comes to processes and compliance with a classic SIEM configuration. I was inspired by what the cyber community shared to improve detection development, security configuration and problem resolution. Thanks to this, I've multiplied our ability to create new detections by importing new rules created by other SOCs.

Standardization & Testing: one of my main challenges has been to guarantee perfect data standardization, as this has an impact on SIEM performance, rule execution, log ingestion, etc....It's difficult today to guarantee the singularity of fields. By adding a test process, I was able to continually test the log model to ensure the best data analysis.

> "That's why the SIEM are the eyes of your security.
>
> Axel JOLLIS
> Cyber SIEM Architect at ZENDATA

Always in movement to protect

our team.