AXEL JOLLIS

Security Architect chez ZENDATA

Comment j'ai déployé un SIEM-as-Code?

L'émergence de l'outil, connu sous le nom de Security Information and Event Management (SIEM), découle de la nécessité de surveiller les logs (journaux) au sein d'une organisation. Le National Institute of Standards and Technology donne la définition suivante du SIEM : "Application permettant de collecter des données de sécurité à partir des composants du système d'information et de présenter ces données sous forme d'informations exploitables via une interface unique."

La perfection n'existant pas, le SIEM ne dérogeait pas à la règle. Tel quel, l'un des principaux problèmes était la capacité de surveiller et d'automatiser les changements de configuration. J'ai donc décidé de me concentrer sur une manière spécifique de créer un SIEM : le SIEM en tant que code (SIEM-as-code). Le principe du SIEM-as-code est assez basique : il s'agit de pouvoir gérer les différentes configurations du SIEM avec une intégration, des tests et une livraison en continu. Cela signifie qu'il est possible d'incorporer des examens par les pairs, de surveiller et d'alerter les changements et de déboguer les informations relatives à un incident. Le SIEM-as-code est une extension du code de détection connu qui est uniquement axé sur les alertes et comprend également la gestion de l'ingestion des journaux d'événements, la configuration de l'architecture SIEM et la gestion de l'enrichissement des journaux d'événements.

Le "as code" offre des avantages que l'on ne trouve pas dans les SIEM classiques :

Surveillance & Versionnement : il permet d'avoir une vue d'ensemble de la modification du SIEM, ce qui donne la possibilité de suivre les problèmes liés aux alertes, de surveiller le temps de développement de chaque partie de l'infrastructure et de comparer les versions.

Modularité & Communauté : il doit être réutilisable, modulaire et partageable. Cela signifie qu'il doit être un service en continu, ce qui est un véritable casse-tête lorsqu'il s'agit de processus et de conformité avec une configuration SIEM classique. J'ai été inspiré par ce que la cybercommunauté a partagé pour améliorer le développement de la détection, la configuration de la sécurité et la résolution des problèmes. Grâce à cela, j'ai multiplié nos capacités à créer de nouvelles détections en important de nouvelles règles créées par d'autres SOC.

Normalisation & Tests : l'un de mes principaux défis a été de garantir une normalisation parfaite des données car cela a un impact sur les performances du SIEM, l'exécution des règles, l'ingestion des logs, etc....Il est difficile aujourd'hui de garantir la singularité des champs. En ajoutant un processus de test, j'ai pu continuellement tester le modèle de log pour assurer la meilleure analyse des données.

> "C'est pourquoi les SIEM sont les yeux de votre sécurité.
>
> Axel JOLLIS
> Cyber SIEM Architect at ZENDATA

Always in movement to protect

notre équipe.