

DÉPLOIEMENT D'UN SIEM-XDR AVEC WAZUH

ACTIVITÉ 1 – INSTALLATION DU SIEM-XDR WAZUH ET DES AGENTS

Fiche 1 : SIEM WAZUH - Architecture

Fiche 2 : SIEM WAZUH - Installation

L'objectif est ici de :

- comprendre les notions de SIEM (*Security Information and Event Management* ou Gestion des Évènements et des Informations) de EXR (*Extended detection and response* ou de Détection et Réponse Etendues).
- se familiariser avec le fonctionnement d'un SIEM-XDR WAZUH.

Nous allons déployer une distribution Ubuntu serveur et rendre accessible le service SSH.

Préconisation pour le serveur Ubuntu : 4 vCPU / 8 GiB / 50 GB

Trois types d'installations sont proposés :

- pas à pas dans une machine virtuelle Ubuntu
- avec un ensemble de conteneurs sous Docker
- par l'utilisation d'un script d'installation unique

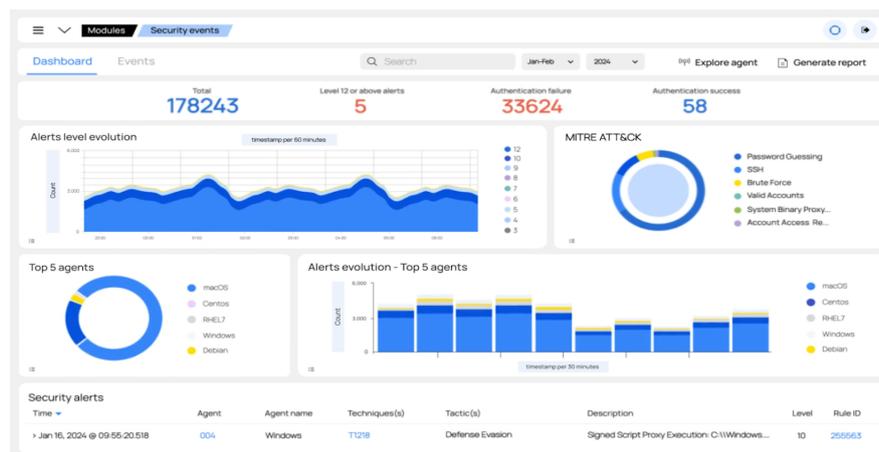


Vous allez découvrir un certain nombre de commandes, il est nécessaire de ne pas se contenter de les saisir, mais de les comprendre.

TRAVAIL À FAIRE :

1. Retrouver les rôles, fonctionnalités, limites, avantages et inconvénients d'un EDR, d'un XDR, d'un SIEM et d'un HIDS en vous appuyant notamment sur le document fourni.
2. Préciser dans un tableau les différents composants compris dans l'architecture de la solution Wazuh en expliquant leur fonction.
3. Installer la solution Wazuh en utilisant la méthode choisie par votre enseignant.
4. Expliquer l'intérêt de l'utilisation de certificats entre les différents composants de Wazuh.
5. Créer un groupe d'agents nommé « serveurs » sur Wazuh pour l'ensemble des serveurs du vlan « Production »
6. Installer un agent Wazuh sur chacun des serveurs du vlan « Production ».
7. Vérifier la remontée des points d'extrémité (CubAD et CubDHCP)
8. Vérifier les versions du serveur Wazuh et des agents et si besoin mettre à jour les versions avec la version la plus récente
9. Expliquer l'utilité de mettre à jour le serveur Wazuh et les agents

DOCUMENT : QU'EST-CE QU'UN SIEM ET UN XDR ?



Au cours des vingt dernières années, les plateformes de gestion de l'information et des événements de sécurité (SIEM) ont été l'une des principales solutions de gestion de cybersécurité, car elles aident les équipes de sécurité à centraliser les activités de détection des attaques et des menaces. L'industrie de la cybersécurité évolue maintenant vers un nouveau type de solution appelée détection et réponse étendues (XDR pour Extended Detection and Response).

Comme les deux technologies sont similaires et ont des capacités communes, beaucoup de gens ne savent toujours pas faire la différence. Cependant, le choix de la bonne solution est essentiel à la construction d'une architecture de sécurité efficace et durable qui répond aux besoins spécifiques des clients des MSP.

Différences entre XDR et SIEM

La différence cruciale entre les deux solutions est que le **SIEM** adopte une approche plus générale qui la rend moins efficace que les plateformes **XDR**. Ces dernières sont hautement spécialisées dans la corrélation des informations de sécurité et sont capables de détecter les attaques et les menaces plus facilement. Les outils SIEM permettent aux entreprises de collecter des logs et des alertes à partir de plusieurs solutions. Cependant, cette technologie n'inclut pas l'analyse ou l'automatisation, contrairement au XDR qui intègre des éléments **EDR** (*Endpoint Detection and Response* ou **Détection et réponse des points d'extrémité**) et **MDR** (*Managed Detection and Response* ou **Détection et réponse gérées**), formant ainsi une solution de bout en bout qui améliore la détection et la réponse. Le XDR utilise les données collectées auprès du système SIEM pour fournir un volume plus digeste d'alertes et de données, ce qui en fait le complément idéal de la technologie SIEM.

Une fois qu'une menace a été détectée, on lui attribue un score critique sur la base duquel une action spécifique est effectuée. Elle peut également être programmée pour être effectuée plus tard ou chaque fois qu'une situation future répondant à ces mêmes critères se produit. En comparaison, un système SIEM est passif et informe les utilisateurs en générant des alertes qui doivent être gérées par du personnel qualifié.

La plupart des solutions SIEM offrent des capacités centralisées de gestion et d'analyse des logs pour une entreprise. Cela implique de générer des alertes, de corréler les données de plusieurs solutions sélectionnées et de mettre en place une **analyse post-événement**. Le SIEM peut également être utilisé pour le monitoring de la conformité, le confinement et la génération de rapports plus complets.

Le XDR se concentre sur l'utilisation des données qu'il collecte pour améliorer la détection et la réponse aux menaces. **Son objectif est d'identifier, d'enquêter et de prendre les mesures appropriées pour résoudre les incidents rapidement et efficacement.**

Comme elles sont plus ouvertes, les solutions SIEM nécessitent souvent un effort de gestion important pour les connecter à des sources de données, corrélérer des événements et configurer des alertes. Compte tenu de la quantité d'informations qu'elles traitent pour une visibilité centralisée, elles produisent un grand nombre d'alertes individuelles qui sont difficiles à classer et à hiérarchiser.

En revanche, les solutions XDR sont conçues pour s'intégrer plus facilement dans l'architecture de sécurité d'une entreprise. L'avantage est qu'elles réduisent le nombre d'alertes pertinentes. En déployant la corrélation automatique des données depuis différentes couches de sécurité, les alertes peuvent être confirmées automatiquement. Cela réduit ainsi le temps dont les analystes de sécurité ont besoin pour évaluer les alertes et les risques afin de décider de ce qui nécessite une attention et une enquête plus approfondie. De plus, la configuration centralisée aide à hiérarchiser les actions nécessaires en générant une pondération des alertes. Le XDR nécessite également moins d'heures de formation et offre une gestion unifiée et un workflow qui s'étend sur plusieurs composants de sécurité.

Le principal défi que le SIEM pose est la désensibilisation aux alertes de sécurité (alert fatigue). Ces solutions génèrent un grand nombre d'alertes, y compris de faux positifs. De ce fait, si le client est doté d'une petite équipe, elle peut se retrouver submergée par toutes ces alertes et avoir des difficultés à les classer et à investiguer. Comme il s'agit d'une solution plus large et plus complexe, les coûts sont plus élevés, ce qui peut être une entrave pour les entreprises de taille moyenne.

Le XDR est idéal pour les petites et moyennes entreprises car il permet d'économiser des ressources, du temps et des coûts. Mais il est important de souligner qu'il s'agit d'une solution plus spécialisée, tandis qu'un SIEM est plus large et peut corrélérer des données plus disparates, dont certaines en provenance d'autres solutions, au-delà du firewall et des endpoints tels que les logs de proxy ou d'application.

Source (extrait d'article) : www.watchguard.com

Auteur : Carlos Arnal

Date de parution : 14 juin 2023