

DÉPLOIEMENT D'UN SIEM-XDR AVEC WAZUH

ACTIVITÉ 2 – ÉVALUATION DES CONFIGURATIONS ET CHASSE AUX MENACES

Fiche 3 : SIEM WAZUH – Évaluation des configurations

Fiche 4 : SIEM WAZUH – Chasse aux menaces

L'objectif est ici de :

- corriger les vulnérabilités des configurations des deux serveurs (CubAD et CubDHCP) de manière proactive ;
- d'analyser des sources de données afin de découvrir les menaces potentielles toujours de manière proactive.

Selon les versions de système que vous utilisez, les résultats peuvent être différents.

TRAVAIL À FAIRE :

A. ÉVALUATION DES CONFIGURATIONS

Dans cette première étape, vous devez repérer le niveau de vulnérabilité des configurations actuelles de vos deux serveurs (CubAD et CubDHCP) puis améliorer de manière proactive les scores de vulnérabilité.

1. Retrouver les scores de vulnérabilité des deux serveurs (CubAD et CubDHCP) en précisant les scores des tests « passés », des tests en « échec » et des tests « non-évalués ».
2. Indiquer le nombre de tests de vulnérabilité réalisé sur un environnement Windows avec celui d'un environnement sous Linux. Pourquoi le nombre de tests n'est pas identique ?
3. Retrouver au moins deux vulnérabilités sur chaque serveur et expliquer les raisons indiquées pour qualifier ces vulnérabilités.
4. Corriger au moins deux vulnérabilités sur chaque serveur en suivant les remédiations proposées par Wazuh.
5. Afficher le nombre de vulnérabilités identifiées par Wazuh sur chacun de vos serveurs.
6. Retrouver une CVE (*Common Vulnerabilities and Exposures* - Vulnérabilités et Expositions Communes) liée à une vulnérabilité identifiée comme « élevée ».

B. CHASSE AUX MENACES

Dans cette deuxième étape vous devez repérer les menaces qui visent vos deux serveurs (CubAD et CubDHCP) puis analyser les tactiques d'attaques pouvant être engagées.

7. Retrouver le nombre d'évènements réalisés sur chacun de vos et identifiés par Wazuh.
8. Retrouver le détail des évènements identifiés.
9. Retrouver dans MITRE ATT-CK les tactiques et techniques pouvant être utilisées pour exploiter les vulnérabilités de vos deux serveurs.