DÉPLOIEMENT D'UNE SOLUTION DE GESTION DES ÉVÈNEMENTS ET DES INFORMATIONS DE SÉCURITÉ (SIEM-XDR) AVEC WAZUH

DESCRIPTION DU THÈME

Propriétés	Description
Intitulé long	Déploiement d'une solution de Gestion des Évènements et des Informations de Sécurité (SIEM-XDR) avec WAZUH
Formation(s) concernée(s)	☐ Classes de première Sciences et technologies du management et de la gestion (STMG) ☐ Terminale STMG Système d'information de gestion (SIG) ☒ BTS Services Informatiques aux Organisations
Matière(s)	☐ Sciences de gestion ☐ SIG ☐ Bloc 1 – Support et mise à disposition de services informatiques ☐ Bloc 2 SISR – Administration des systèmes et des réseaux ☒ Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	L'objectif de ce « Labo » est de comprendre l'intérêt d'un SIEM-XDR et d'en tester les principaux usages (détecter les vulnérabilités des serveurs, répondre aux menaces). La solution Wazuh sera étudiée dans cette proposition mais les fonctionnalités présentées sont disponibles dans d'autres solutions SIEM. Ce « Labo » comporte **3 activités** qui peuvent être réalisées en bloc3 SISR : • **Activité 1** : installation du siem wazuh et des agents • **Activité 2** : évaluation des configurations et chasse aux menaces • **Activité 3** : réponse aux menaces
Savoirs	• Outils de sécurité : prévention et détection des attaques, gestion d'incidents.
Compétences	**3.3 Sécuriser les équipements et les usages des utilisateurs** • Identifier les menaces et mettre en œuvre les défenses appropriées • Vérifier l'efficacité de la protection **3.4 Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques** • Organiser la collecte et la conservation des preuves numériques

Prolongements	D'autres activités (comme la gestion des faux positifs, l'intégration des éléments d'interconnexion sans agents, etc.) seront intégrées ultérieurement.
Prérequis	Commandes de base d'administration d'un système Linux. Notions de virtualisation voire de conteneurisation (si installation via docker-compose).
Outils	Un serveur physique ou virtuel sous une distribution Linux 64 bits (ici Debian 12 – version stable actuelle ou Ubuntu serveur) sur lequel Wazuh sera installé avec un serveur. Un serveur physique ou virtuel sous Linux avec le service DHCP Un serveur physique ou virtuel sous un environnement Windows Serveur avec Active Directory installé. Une machine physique ou virtuelle Kali. Site officiel : https://wazuh.com/
Mots-clés	SIEM, XDR, EDR, HIDS, HIPS Wazuh
Durée	6-8 heures (suivant le type d'installation choisi pour Wazuh)
Auteur·e·s	David BALNY avec Apollonie Raffalli comme testeuse et relectrice.
Version	v1
Date de publication	Avril 2025

DERNIÈRES RÉVISIONS

Ce tableau contient les modifications apportées au document après sa publication uniquement.

Date	Auteur·e	Description

CONTEXTE

Née en décembre 2010, la société CUB est une entreprise spécialisée dans l'incubation de startups partageant les mêmes valeurs de solidarité et de développement durable. Au travers de sa plate-forme web, CUB permet à des professionnels d'accéder à des espaces de travail dédiés : salles de réunion, de formation ou de séminaire.

Le concept novateur de CUB repose sur une démarche collaborative de type « BtoB », en effet CUB propose aux entreprises qui disposent d'espaces inoccupés de les louer à l'heure ou à la journée.

À la différence d'une pépinière d'entreprises classique, CUB s'adresse à des sociétés très jeunes, ou encore en création, pour leur apporter un appui lors des premières étapes de la vie de l'entreprise. Elle met à disposition de ses clients un ensemble de solutions techniques d'accès dans un millier de salles de réunion situées dans une quarantaine de villes différentes. Les ressources et outils du Web 2.0 qui permettent aux entreprises de gérer leurs contenus et leurs connaissances de manière sécurisée sont accessibles indépendamment via des prestataires de type informatique dans les nuages (cloud computing) : partage de fichiers, gestion de projet, réseau social d'entreprise, wiki d'entreprise, etc.

La direction des systèmes d'information (DSI), située au siège à Paris, participe étroitement aux choix stratégiques de CUB, elle a pour mission de définir et mettre en œuvre la politique informatique en accord avec la stratégie générale et ses objectifs de performance.

CUB héberge, dans un Vlan « production » des services réseaux essentiels :

- un Active Directory paramétré sur un **serveur Windows** (RDP activé) ;
- un service DHCP paramétré sur un **serveur debian** (SSH activé).

Deux autres Vlan sont utilisés dans l'infrastructure :

- le Vlan « SIEM » pour héberger l'installation du **serveur Wazuh** et d'une **machine Kali** ;
- le Vlan « client » pour les postes des collaborateurs de la société.

La DSI a décidé :

- **de mettre en place le SIEM Wazuh et les agents sur les serveurs (Activité 1)**
- **de repérer les vulnérabilités sur ses principaux serveurs (CubAD, CubDHCP) (Activité 2).**
- **d'automatiser des réponses à des menaces (Activité 3)**

Voici le schéma de cette architecture :