

## AC33.09 – Surveiller l’activité du système d’information

### Contexte

Dans le cadre de la surveillance d’un **système d’information**, il est primordial de mettre en place des outils permettant de détecter et analyser les événements de sécurité. Cette compétence est appliquée lors de l’implémentation d’un **SIEM** (Security Information and Event Management) pour analyser les logs, surveiller les incidents et automatiser certaines tâches. Le projet de surveillance dans la **SAE CTF** a impliqué la mise en œuvre de **Wazuh** pour la gestion des logs, l’analyse des événements et l’automatisation des tâches de sécurité.

---

### Savoir mis en œuvre

- **Analyse et installation des outils de surveillance** : Mise en place d’un **SIEM**, en l’occurrence **Wazuh**, pour collecter et analyser les logs systèmes en temps réel, détecter les anomalies et répondre aux incidents de sécurité.
  - **Administration de l’outil** : Configuration de **Wazuh** pour interagir avec les sources de logs (serveurs, applications, etc.) et d’autres outils (ELK Stack, par exemple) afin de centraliser l’information et d’obtenir des alertes en cas d’anomalies.
  - **Exploitation des logs** : Utilisation des logs pour détecter les événements de sécurité, les erreurs système et les intrusions potentielles.
  - **Automatisation des tâches** avec des outils comme **Ansible** pour déployer et configurer automatiquement les composants nécessaires à la surveillance du SI.
- 

### Savoir-faire mis en œuvre

- **Mise en place de Wazuh** : Installation et configuration de **Wazuh** pour collecter, analyser et stocker les logs des serveurs et applications dans un but de surveillance continue de l’activité du SI.
  - **Collecte de logs** : Configuration de l’agent Wazuh sur les serveurs et stations de travail pour qu’ils envoient leurs logs vers le serveur Wazuh central.
  - **Configuration des règles d’analyse** : Définition de règles spécifiques pour détecter les événements critiques et générer des alertes en cas d’attaque ou d’incident.



- **Intégration avec ELK (Elasticsearch, Logstash, Kibana)** : Utilisation d'**ELK** pour visualiser et analyser les logs collectés par Wazuh. **Logstash** permet de filtrer et formater les logs, **Elasticsearch** de les indexer, et **Kibana** de les visualiser sous forme de tableaux de bord interactifs.
  - **Surveillance active et métrologie** : Suivi en temps réel de l'état du système via les logs et les alertes générées par Wazuh et ELK. Utilisation des capacités de **métrologie** pour analyser les performances et identifier les zones à risque.
  - **Automatisation avec Ansible** : Automatisation du déploiement et de la configuration de Wazuh, ELK et des autres outils associés via **Ansible**, réduisant ainsi les erreurs humaines et accélérant le processus d'installation.
- 


### **Savoir-être mis en œuvre**


- **Rigueur et précision** dans la configuration des outils de surveillance et d'analyse pour s'assurer de la fiabilité des données recueillies.
  - **Réactivité** face aux alertes et aux événements de sécurité pour minimiser l'impact des incidents.
  - **Capacité d'analyse critique** pour comprendre les logs, identifier les événements importants et exploiter les informations afin d'améliorer la sécurité du système.
  - **Collaboration** avec d'autres équipes (administrateurs systèmes, équipes sécurité, etc.) pour assurer une surveillance cohérente et une réponse rapide aux incidents.
- 


### **Tâches réalisées et résultats**

#### **Tâches effectuées :**

 **Installation de Wazuh** : Déploiement du serveur **Wazuh** sur une machine dédiée, installation des agents sur les serveurs et machines de l'infrastructure. 

**Configuration des règles de sécurité** : Mise en place de règles pour détecter les attaques et les comportements anormaux comme les tentatives de connexion échouées, les accès non autorisés et les modifications suspectes de fichiers. 

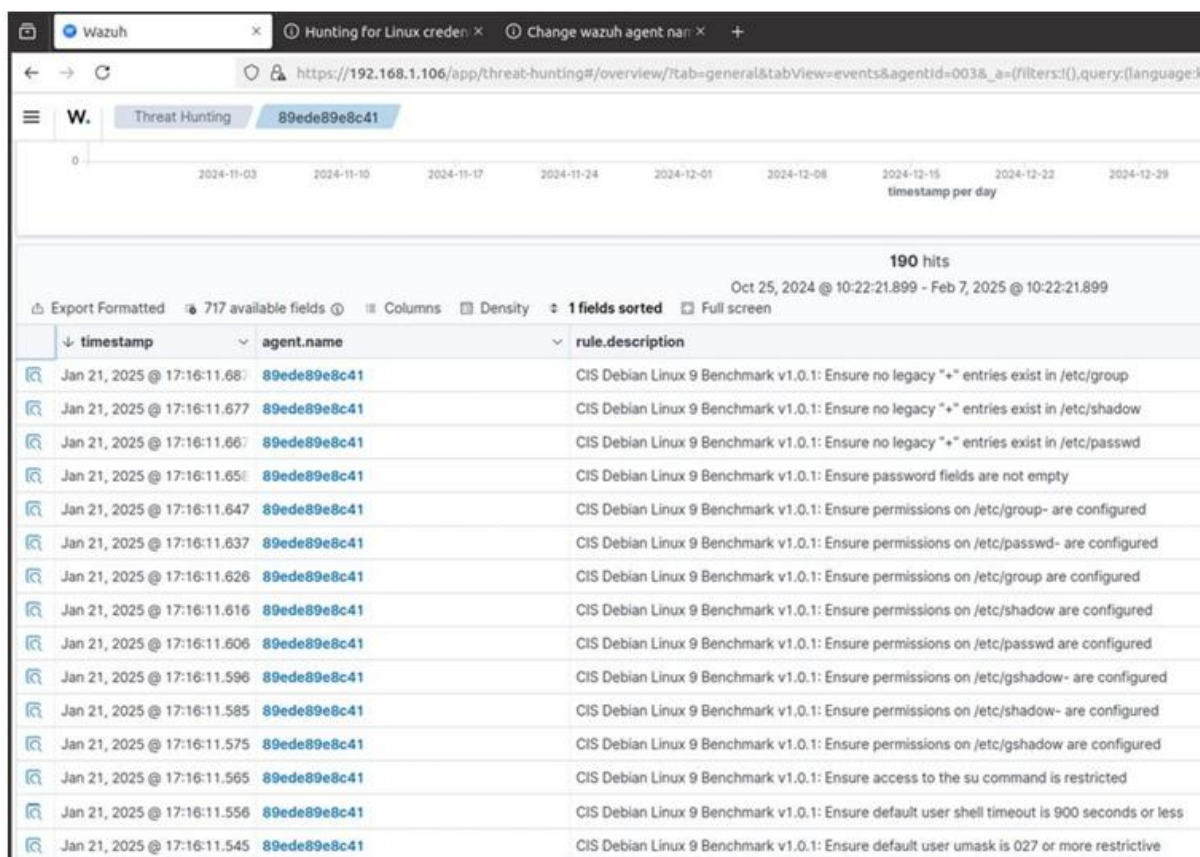
**Intégration avec ELK** : Connexion de Wazuh à **Elasticsearch** pour stocker les logs et à **Kibana** pour visualiser les alertes et tendances en temps réel. 

**Automatisation des tâches avec Ansible** : Déploiement automatique de la solution de surveillance et configuration des agents sur tous les serveurs à l'aide de **playbooks Ansible**. 

**Surveillance et gestion des alertes** : Surveillance des logs collectés et analyse des alertes en temps réel pour détecter et répondre rapidement aux incidents de sécurité.

### Résultats :

- **Centralisation des logs** et des événements de sécurité, permettant une surveillance continue du système d'information.
- **Amélioration de la réactivité** face aux incidents grâce à l'automatisation des alertes et la gestion centralisée des logs.
- **Visibilité accrue** de la sécurité du SI avec des tableaux de bord interactifs permettant une analyse rapide et précise des menaces.
- **Réduction du temps d'intervention** lors de l'identification d'incidents grâce à l'automatisation du processus de surveillance et de déploiement.



Wazuh Threat Hunting interface showing results for agent 89ede89e8c41. The interface displays a timeline and a table of 190 hits. The table columns are timestamp, agent.name, and rule.description. The hits are sorted by timestamp, showing events from Jan 21, 2025 @ 17:16:11.687 to Jan 21, 2025 @ 17:16:11.545. The rules are related to CIS Debian Linux 9 Benchmark v1.0.1, specifically ensuring no legacy "\*" entries exist in /etc/group, /etc/shadow, and /etc/passwd, and ensuring permissions on /etc/group, /etc/passwd, and /etc/shadow are configured.

timestamp	agent.name	rule.description
Jan 21, 2025 @ 17:16:11.687	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure no legacy "*" entries exist in /etc/group
Jan 21, 2025 @ 17:16:11.677	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure no legacy "*" entries exist in /etc/shadow
Jan 21, 2025 @ 17:16:11.667	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure no legacy "*" entries exist in /etc/passwd
Jan 21, 2025 @ 17:16:11.657	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure password fields are not empty
Jan 21, 2025 @ 17:16:11.647	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/group- are configured
Jan 21, 2025 @ 17:16:11.637	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/passwd- are configured
Jan 21, 2025 @ 17:16:11.626	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/group are configured
Jan 21, 2025 @ 17:16:11.616	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/shadow are configured
Jan 21, 2025 @ 17:16:11.606	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/passwd are configured
Jan 21, 2025 @ 17:16:11.596	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/gshadow- are configured
Jan 21, 2025 @ 17:16:11.585	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/shadow- are configured
Jan 21, 2025 @ 17:16:11.575	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure permissions on /etc/gshadow are configured
Jan 21, 2025 @ 17:16:11.565	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure access to the su command is restricted
Jan 21, 2025 @ 17:16:11.556	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure default user shell timeout is 900 seconds or less
Jan 21, 2025 @ 17:16:11.545	89ede89e8c41	CIS Debian Linux 9 Benchmark v1.0.1: Ensure default user umask is 027 or more restrictive