Infrastructure Intégrée pour la Surveillance et la Gestion des Incidents de Sécurité

Introduction :

La cybersécurité est devenue une priorité incontournable pour les organisations face à l'augmentation des menaces numériques. Afin de protéger efficacement les systèmes d'information, il est essentiel de déployer une infrastructure performante capable de détecter, analyser et répondre aux incidents de sécurité. Ce projet consiste à l'installation et la configuration d'un SOC SIEM et SOAR avec l'intégration de plusieurs outils tels que Wazuh, ElasticSearch, DFIR IRIS, Shuffle, MISP et Cortex. Ces solutions permettent de mettre en place une surveillance proactive et une réponse coordonnée aux cybermenaces.

1. **Wazuh**

   - **Objectif :** Surveillance de la sécurité, gestion des journaux et détection d'intrusions.

- **Installation :**
- **Configuration :**
  - Définir les règles de détection et configurer l'agent Wazuh.
  - Activer SSL pour les communications sécurisées.
- **Intégration :**
  - Connecter ElasticSearch et Kibana.
  - Configurer les alertes pour surveiller les journaux du système.

2. **ElasticSearch et Dashboard Kibana**

   - **Objectif** : Stockage et visualisation de grandes quantités de données.

- **Installation :**
- **Configuration :**
  - Modifier le fichier elasticsearch.yml pour définir les paramètres réseau.
  - Configurer Kibana pour pointer vers ElasticSearch.
- Intégration :
  - Connecter ElasticSearch à Wazuh pour stocker les journaux.

3. **DFIR IRIS**

❖ **Objectif** : Gestion des incidents de sécurité et centralisation des alertes.

➢ **Installation :**

➢ **Configuration :**

- Créer la base de données avec les tables nécessaires.
- Configurer les utilisateurs et les rôles d'accès.

➢ **Intégration :**

- Configurer l'importation des alertes provenant de Wazuh.

4. MISP (Malware Information Sharing Platform)

❖ **Objectif** : Partage d'informations sur les menaces.

➢ **Installation :**

➢ **Configuration :**

- Définir les sources de threat intelligence.
- Configurer les utilisateurs et les organisations.

➢ **Intégration :**

- Connecter MISP à DFIR IRIS pour partager les informations sur les incidents.

5. Cortex

❖ **Objectif** : Automatisation des analyses d'incidents.

➢ **Installation :**

➢ **Configuration :**

- Définir les analyzers (modules d'analyse).

➢ **Intégration :**

- Configurer DFIR IRIS pour envoyer les alertes à Cortex.

6. SOAR Shuffle

❖ **Objectif** : Automatisation des workflows de réponse aux incidents.

➢ **Installation :**

➢ **Configuration :**

- Définir les workflows pour répondre automatiquement aux alertes.

➢ **Intégration :**

- Connecter Shuffle à DFIR IRIS, Wazuh, et Cortex pour une automatisation fluide.

Conclusion :

Ce projet consiste à fournir une vue d'ensemble sur l'installation, la configuration et l'intégration des outils Wazuh, ElasticSearch, DFIR IRIS, MISP, Cortex et Shuffle. L'objectif principal est d'obtenir une infrastructure robuste permettant une surveillance et une gestion optimale des incidents de sécurité.