Compte Rendu Détaillé du Projet : Déploiement d’un SIEM (ELK Stack/Splunk)

Date de rendu : 04/04/2025

Durée du projet :

**1. Contexte et Objectifs**

Objectif principal : Déployer une solution SIEM (Security Information and Event Management) pour centraliser, analyser et alerter sur les événements de sécurité du réseau, en utilisant ELK Stack ou Splunk, et former l’équipe SOC (Security Operations Center) à son utilisation.

**Livrables attendus :**

- SIEM opérationnel (ELK ou Splunk) avec collecte de logs centralisée.

- Règles d’alertes personnalisées pour détecter les menaces (ex: attaques brute force, activités suspectes).

- Équipe SOC formée à l’analyse des alertes et à la réponse aux incidents.

- Documentation technique et manuels de formation.

**Contraintes :**

- Intégration avec l’infrastructure existante (serveurs, pare-feux, Active Directory).

- Respect des réglementations de confidentialité (RGPD, ISO 27001).

**2. Méthodologie et Organisation**

2.1. Rôles de l’Équipe

- Chef de Projet : Coordination des ressources et respect des délais.

- Architecte SIEM : Installation et configuration d’ELK/Splunk.

- Analyste SOC : Création des règles d’alertes, tests de détection.

- Formateur Cybersécurité : Conception des modules de formation.

- Administrateur Système : Intégration des sources de logs (pare-feux, AD, serveurs).

2.2. Outils Utilisés

- ELK Stack (Elasticsearch, Logstash, Kibana) ou Splunk Enterprise.

- Wazuh (intégration avec ELK pour la détection d’intrusions).

- Sigma Rules : Bibliothèque de règles de détection standardisées.

- TheHive: Plateforme de gestion des incidents (optionnel).

- Jira/Confluence : Suivi des tâches et documentation.

**3. Phases du Projet**

3.1. Phase 1 : Planification et Choix de la Solution (2h)

Objectif : Sélectionner la solution SIEM et définir l’architecture.

Tâches réalisées :

- Comparatif ELK vs Splunk :

- ELK : Open source, personnalisable, coût réduit.

- Splunk : Interface intuitive, support professionnel, coût élevé.

- Architecture retenue :

- Serveur ELK : Ubuntu 22.04 (4 CPU, 16 Go RAM, 500 Go SSD).

- Sources de logs : pfSense, Active Directory, serveurs Windows/Linux.

3.2. Phase 2 : Installation et Configuration du SIEM (6h)

Objectif : Déployer la solution et configurer la collecte de logs.

Tâches réalisées :

- Installation d’ELK Stack :

```bash

# Installation d’Elasticsearch et Kibana

sudo apt install elasticsearch kibana

# Configuration de Logstash pour les logs pfSense

input { beats { port => 5044 } }

filter { grok { match => { "message" => "%{SYSLOGTIMESTAMP:timestamp} %{SYSLOGHOST:hostname} %{DATA:message}" } } }

```

- Intégration avec Wazuh :

- Déploiement d’agents Wazuh sur les postes clients pour la collecte EDR (Endpoint Detection and Response).

3.3. Phase 3 : Création de Règles d’Alertes Personnalisées (5h)

Objectif : Détecter les activités malveillantes via des règles spécifiques.

Tâches réalisées :

- Exemples de règles :

- Attaque Brute Force SSH :

```yaml (Kibana)

Alert Name: "Multiple SSH Failed Logins"

Conditions:

WHEN count() OVER all documents IS ABOVE 5 FOR THE LAST 5 minutes

WHERE source.ip IS NOT null AND event.action == "ssh\_login\_failed"

```

- Activité suspecte AD :

```spl (Splunk)

index=wineventlog EventCode=4625

| stats count by user

| where count > 3

```

- Intégration de règles Sigma :

- Conversion des règles Sigma en formats compatibles (ex: Elasticsearch Query DSL).

3.4. Phase 4 : Formation de l’Équipe SOC (4h)

Objectif : Former les analystes à l’utilisation du SIEM et à la réponse aux incidents.

Tâches réalisées :

- Ateliers pratiques :

- Analyse d’un faux incident : Investigation d’une alerte "Brute Force" dans Kibana.

- Utilisation de MITRE ATT&CK pour mapper les TTPs (Tactics, Techniques, Procedures).

- Scénarios de simulation :

- Jeu de rôles : Analyste SOC vs Attaquant (utilisation de Caldera pour les simulations).

3.5. Phase 5 : Tests et Documentation (3h)

Objectif : Valider le SIEM et produire les guides.

Tâches réalisées :

- Tests de détection :

- Lancement d’une attaque simulée (ex: scan de ports avec Nmap) et vérification des alertes.

- Mesure du temps de réponse moyen : \*\*15 minutes\*\* pour les incidents critiques.

- Documentation :

- Guide d’administration SIEM : Procédures de maintenance, mise à jour des règles.

- Manuel SOC : Workflow d’investigation, contacts d’urgence.

**4. Résultats et Livrables**

4.1. SIEM Opérationnel

- Logs collectés : 10 sources intégrées (pare-feux, AD, serveurs web).

- Alertes configurées : 20 règles personnalisées, 50 règles Sigma importées.

- Performance : Temps de traitement des logs < 2 secondes.

4.2. Formation SOC

- Équipe certifiée : 100% des analystes capables d’investiguer une alerte de niveau moyen.

- Matériel pédagogique : 5 scénarios de simulation, 10 fiches réflexes.

5. Défis Rencontrés et Solutions

- Problème : Surcharge d’Elasticsearch due au volume de logs.

- Solution : Optimisation des index (rotation quotidienne, suppression des logs obsolètes).

- Problème : Alertes en faux positifs sur les logs AD.

- Solution : Affinement des règles avec filtres supplémentaires (ex: exclusion des comptes de service).

6. Bilan et Améliorations Futures

- Points forts : Détection proactive des menaces, formation pratique efficace.

- Axes d’amélioration :

- Intégration d’une solution SOAR (ex: TheHive) pour automatiser la réponse.

- Mise en place de dashboards temps réel pour la surveillance continue.

**Annexes**

Annexe 1 : Capture d’écran du Dashboard Kibana

Légende : Visualisation des tentatives de connexion SSH et des alertes actives.

Annexe 2 : Exemple de Règle Sigma Convertie pour Elasticsearch

```yaml

title: Suspicious PowerShell Execution

description: Détecte l’exécution de PowerShell avec des arguments masqués.

logsource:

product: windows

service: sysmon

detection:

selection:

EventID: 1

CommandLine: "-enc "

condition: selection

```

Annexe 3 : Programme de Formation SOC

```plaintext

Module 1 : Bases du SIEM

- Navigation dans Kibana/Splunk.

- Interprétation des logs bruts.

Module 2 : Réponse aux Incidents

- Analyse d’une alerte "Phishing".

- Rédaction d’un rapport d’incident (modèle fourni).

```

---

Équipe Projet

Membres : Axel