

Comprendre et Utiliser les Systèmes SIEM et SOAR

Partie Théorique

1.a. Qu'est-ce qu'un SIEM ?

Un SIEM (Security Information and Event Management) est une solution centralisée qui collecte, corrèle et analyse les journaux provenant de différents systèmes informatiques. Son rôle principal est de **détecter les menaces et anomalies en temps réel**, de faciliter l'investigation et de générer des alertes exploitables pour l'équipe de sécurité.

1.b. Qu'est-ce qu'un SOAR ?

Un SOAR (Security Orchestration, Automation, and Response) est une solution qui automatise et orchestre la réponse aux incidents de sécurité. Il complète le SIEM en permettant de réagir automatiquement aux alertes générées par celui-ci.

2.a. Trois fonctionnalités principales d'un SIEM

Collecte centralisée des journaux provenant de multiples sources.
Corrélation d'événements pour détecter des scénarios de compromission.
Alerting et reporting pour informer les analystes et fournir des tableaux de bord.

2.b. Trois fonctionnalités principales d'un SOAR

Automatisation des réponses via des playbooks.
Orchestration des outils (firewall, EDR, annuaire AD, ticketing).
Gestion des workflows d'incident avec suivi et documentation intégrée.

3.a. Intégration SIEM + SOAR

Le SIEM détecte une menace en corrélant des journaux.
Le SOAR reçoit cette alerte et déclenche un playbook automatisé.

Exemple : le SIEM détecte un login suspect → le SOAR isole automatiquement la machine et alerte l'équipe.

3.b. Avantages pour l'entreprise

Réduction du temps de réponse.
Moins de charge manuelle pour les analystes SOC.
Réduction des risques grâce à une réponse rapide et cohérente.
Meilleure traçabilité des incidents (rapports détaillés, conformité).

Scénario Pratique

1.a. Types de journaux à examiner

Journaux de pare-feu (connexions entrantes/sortantes suspectes).

Journaux d'authentification (tentatives de connexion échouées, logins anormaux).

Journaux des systèmes d'exploitation (création de comptes, processus inhabituels).

Journaux d'applications critiques (bases de données, messagerie, VPN).

```

Password:
Added monitor of 'C:\Windows\System32\winevt\Logs\Application.evtx'.
PS C:\Program Files\SplunkUniversalForwarder\bin> ./splunk.exe add monitor "C:\Windows\System32\winevt\Logs\System.evtx"
Added monitor of 'C:\Windows\System32\winevt\Logs\System.evtx'.
PS C:\Program Files\SplunkUniversalForwarder\bin> ./splunk.exe add monitor "C:\Windows\System32\winevt\Logs\Security.evtx"
Added monitor of 'C:\Windows\System32\winevt\Logs\Security.evtx'.
  
```

1.b. Exemple de comportements anormaux

Plusieurs échecs de connexion sur un compte sensible (bruteforce).

The screenshot shows a Splunk search interface with the query `index=_audit action="login attempt" info=failed` and a time range of "Last 24 hours". It displays 13 events. The "Events (13)" tab is active, showing a list of events with columns for Time and Event. The "INTERESTING FIELDS" list on the left includes `action 1`, `index 1`, `info 1`, `# linecount 1`, `method 1`, and `splunk_server 1`.

i	Time	Event
>	9/11/25 1:00:15.399 PM	Audit:[timestamp=09-11-2025 13:00:15.399, user=admin, action=login attempt, info=failed, src=102.3.2.8 method=Splunk] host = ubuntu-focal source = audittrail sourcetype = audittrail
>	9/10/25 2:09:01.781 PM	Audit:[timestamp=09-10-2025 14:09:01.781, user=admin, action=login attempt, info=failed, src=102.3.2.5 method=Splunk] host = ubuntu-focal source = audittrail sourcetype = audittrail
>	9/10/25 2:05:01.437 PM	Audit:[timestamp=09-10-2025 14:05:01.437, user=admin, action=login attempt, info=failed, src=127.0.0.1 method=Splunk] host = ubuntu-focal source = audittrail sourcetype = audittrail
>	9/10/25	Audit:[timestamp=09-10-2025 14:03:43.767, user=admin, action=login attempt, info=failed, src=102.3.2.8 method=Splunk] host = ubuntu-focal source = audittrail sourcetype = audittrail

Connexion réussie depuis une IP géolocalisée inhabituelle (Ex. 98.120.3.4).

Transfert massif de données sortant (exfiltration potentielle).

Tentative d'accès à un serveur critique en dehors des heures normales.

Exemple de playbook SOAR

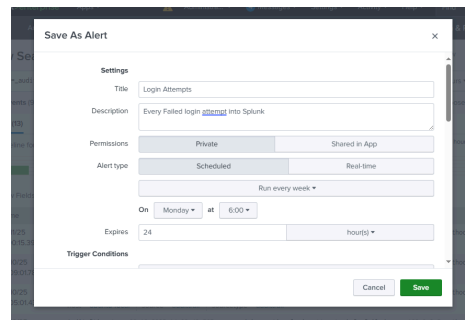
→ Confirmation de la menace

- ◆ Vérifier si l'IP source est connue comme malveillante (threat intelligence).

- ◆ Confirmer les anomalies dans les logs.

→ Action corrective

- ◆ Bloquer l'IP au niveau du firewall.
- ◆ Isoler la machine compromise du réseau.
- ◆ Désactiver temporairement le compte utilisateur suspect.
- ◆ Alerter des tentatives ultérieures de se connecter



→ Notification

- ◆ Envoyer une alerte par e-mail à l'équipe de sécurité.

→ Post-action

- ◆ Forcer une réinitialisation du mot de passe.
- ◆ Lancer un scan antivirus sur la machine.
- ◆ Documenter l'incident et archiver les preuves.

Résultats attendus

- Le SOAR exécute automatiquement le blocage de l'IP.
- Le compte compromis est désactivé.
- L'équipe SOC est notifiée immédiatement.
- L'incident est documenté dans un rapport.