Les technologies SIEM et SOAR

Contexte	https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf
Hypothèses	Le SOAR vient-il remp lacer le SIEM ? | Numeryx
Théorie	SIEM: https://www.microsoft.com/fr-fr/security/business/security-101/what-is-siem Qu'est-ce qu'une solution SIEM ? Définition et explications | Avira https://www.ibm.com/fr-fr/topics/siem SOAR: Qu'est-ce qu'une solution SOAR ? Technologie et solutions | Sécurité Microsoft Le SOAR vient-il remplacer le SIEM ? | Numeryx https://fr.wikipedia.org/wiki/SOAR_(s%C3%A9curit%C3%A9_informatique)
Terrain	Étude de cas Carrefour | Splunk
Réponses aux hypothèses	Comprendre la différence entre SIEM et SOAR - Arsen Cybersécurité https://www.logpoint.com/fr/blog/la-prochaine-evolution-du-siem-et-soar-avec-logpoint-7/ https://www.ibm.com/fr-fr/topics/security-orchestration-automation-response https://www.stormshield.com/fr/actus/detection-and-response-la-question-des-faux-positifs-en-cybersecurite/ https://media.kaspersky.com/fr/business-security/enterprise/Fiche-Kaspersky-Security-Awareness_Facteur-humain.pdf

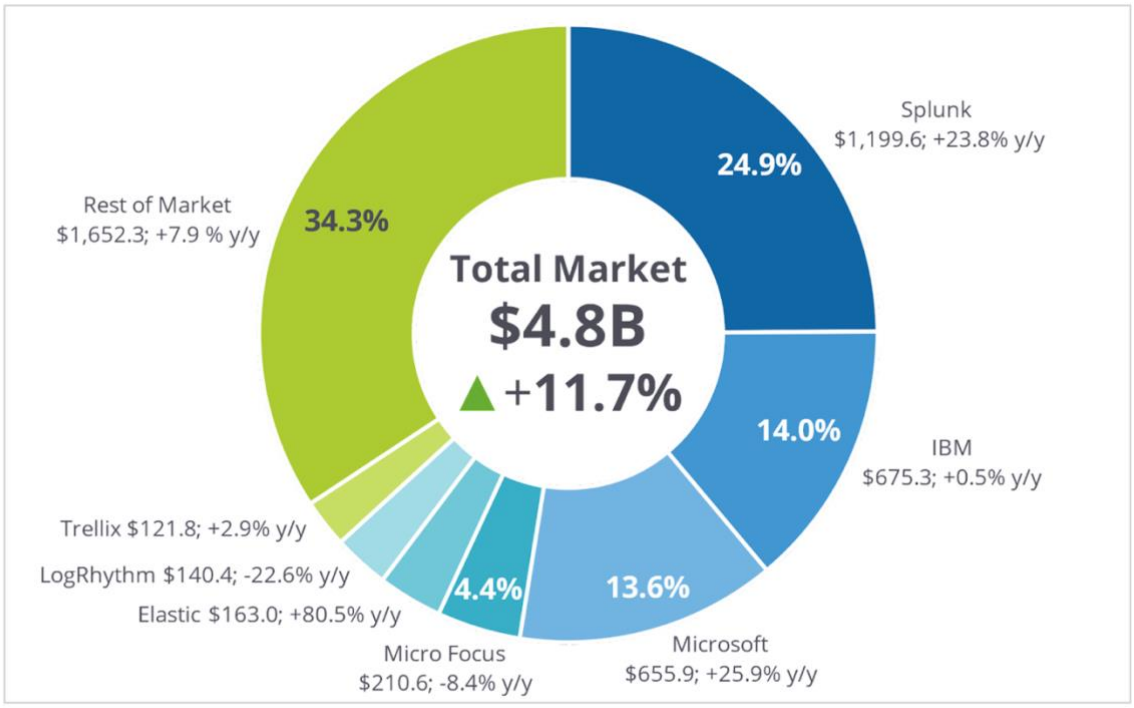
1. Contexte

Aujourd'hui, il est primordial pour les organisations, de protéger les systèmes informatiques contre les menaces.
Par exemple, on peut retrouver le panorama de la cybermenace en 2022 sur le site de l'ANSSI. Les attaquants améliorent leurs capacités à des fins de gain financier, d'espionnage et de déstabilisation.

Ensuite, il y a beaucoup de fournisseurs SIEM leader sur ce marché comme Splunk, IBM ou Microsoft.

Parts de marché par chiffre d'affaires des systèmes SIEM dans le monde en 2021

Rapport IDC Worldwide Security Information and Event Management Market Shares



Source: Worldwide Security Information and Event Management Market Shares, 2021: The Cardinal SIEMs (IDC #US48506522, July 2022)

2) Hypothèses

Pour les hypothèses :

- Est-ce que le SOAR vient remplacer le SIEM ?

C'est une question qui est posée dans le monde de la cybersécurité.

- L'évolution des menaces nécessite une adaptation constante des évolutions SIEM et SOAR.

Comme dans le contexte, les menaces évoluent rapidement et sont de plus en plus sophistiquées. Les deux solutions SIEM et SOAR doivent donc s'adapter.

- L'automatisation des processus de réponse avec le SOAR peut réduire les erreurs humaines dans la gestion des incidents de sécurité.

Les erreurs humaines dans le domaine de la cybersécurité peuvent causer de graves dommages pour l'organisation.

3) Théorie

Le SIEM veut dire Security Information and Event Management.

C’est un logiciel de sécurité qui donne aux organisations, une vue d’ensemble de l’activité de leur réseau pour leur permettre de réagir plus rapidement aux menaces avant que leur activité professionnelle ne soit perturbée.

Le logiciel offre plusieurs fonctionnalités comme gérer les journaux, il centralise de grandes quantités de données qu’il organise avant de déterminer si celles-ci présentent des signes de menace, d’attaque ou de violation.
Ensuite, les données sont triées pour identifier les relations et les schémas afin de détecter rapidement les menaces potentielles et d’y répondre.
Puis, les technologies SIEM surveillent les incidents liés à la sécurité sur le réseau d’une organisation, et fournissent des alertes et des audits pour toutes les activités en lien avec ces incidents.

- **Avantages**

Le principal avantage est la protection contre les menaces virtuelles, chaque utilisateur même les traqueurs ou pirates laissent des traces dans les données de journal. Les systèmes SIEM peuvent donc comparer tous les comportements passés sur le réseau et ils distinguent une utilisation légitime d’une attaque malveillante.
Les solutions SIEM peuvent aussi permettre d’automatiser la mise en conformité avec les réglementations de sécurité des données.
Ensuite, ils réduisent considérablement le délai nécessaire pour identifier les menaces et vulnérabilités potentielles du réseau et y répondre.
La cybersécurité évolue rapidement, les solutions SIEM peuvent détecter et résoudre des menaces inconnues.

Ensuite, je vais définir ce qu’est le SOAR qui veut dire Security Orchestration Automation and Response.
C’est un groupe de technologies qui automatisent la prévention des cyberattaques et la réponse proposée pour contrer celles-ci.

- **Fonctionnalités**

Une solution SOAR recouvre trois fonctions complémentaires qui permettent de détecter et de bloquer les attaques : l’orchestration, l’automatisation et la réponse aux incidents.

L’orchestration intègre des applications personnalisées avec des outils de sécurité intégrés, de manière à ce qu'elles fonctionnent toutes les unes avec les autres. Elle améliore la rapidité et la précision des réponses et réduit le nombre de problèmes de sécurité à résoudre.

L’automatisation programme les tâches pour qu’elles s’exécutent d’elles-mêmes. Par exemple, on peut utiliser l’automatisation pour programmer des tâches, des alertes ou des réponses aux incidents. Cela permet également d’accélérer les processus de sécurité tels que le repérage des menaces et leur correction.

La réponse aux incidents est basée sur l’intelligence artificielle ce qui améliore la rapidité et la précision des réponses et réduit le nombre de problèmes de sécurité à résoudre. Il peut ajouter automatiquement des règles de blocage au niveau du firewall et créer des tickets d’incidents afin de les envoyer aux équipes concernées.

- **Avantages**

Les outils SOAR simplifient les opérations de sécurité et offrent de nombreux avantages. On peut accroître sa productivité car les outils réduisent le nombre de tâches et d'opérations répétitives.
On peut répondre aux incidents beaucoup plus rapidement et plus précisément qu'une équipe humaine.
Toute l'activité est centralisée au même endroit, ce qui permet aux équipes du SOC d'accéder facilement aux informations pour enquêter sur les accidents et y remédier.

4) Terrain

J'ai choisi une étude de cas Carrefour qui utilise la plateforme Splunk Cloud pour répondre aux menaces de sécurité.
Splunk est une plateforme unifiée de sécurité et d'observabilité. Leur objectif est d'aider les équipes de sécurité à garantir le bon fonctionnement de leur organisation.

Aujourd'hui, dans les grandes surfaces, les clients attendent une expérience multicanale et que tout se fasse simplement que ce soit en ligne ou en magasin. Il faut donc que le magasin gère sa sécurité pour protéger les clients.
Grâce à cette plateforme, Carrefour a pu développer de nouvelles fonctionnalités et de nouveaux services.
L'équipe du centre des opérations de sécurité (SOC) réagit désormais trois fois plus rapidement aux incidents. Le cloud Splunk s'occupe des opérations et de l'infrastructure de sécurité donc l'équipe du SOC peut se consacrer à la gestion des applications, à l'analyse des menaces et aux investigations de sécurité.

L'analyste SOC de chez Carrefour précise qu'ils peuvent donc se focaliser sur la tâche la plus importante qui est de garantir aux clients une expérience d'achat toujours sécurisée.

5) Réponses aux hypothèses

La première hypothèse était : **est-ce que le SOAR vient remplacer le SIEM ?**
Il y a plusieurs différences entre le SIEM et le SOAR. D'abord, le SIEM se concentre sur la collecte d'informations des menaces potentielles et l'analyse de données de sécurité, tandis que le SOAR se concentre sur la réponse aux incidents de sécurité. Les solutions SOAR sont souvent intégrées à des solutions SIEM et d'autres outils de sécurité existants. Combiner les deux solutions est intéressant pour les entreprises car cela leur fournit une solution de sécurité complète.

Ensuite, **l'évolution des menaces nécessite une adaptation constante des évolutions SIEM et SOAR.**
Les cybercriminels développent constamment de nouvelles techniques pour contourner la sécurité. Les menaces évoluent et sont de plus en plus complexes et

difficiles à détecter. Les fournisseurs de solutions SIEM et SOAR publient régulièrement des mises à jour pour intégrer de nouvelles fonctionnalités.
Par exemple, grâce à l'intelligence artificielle et à l'apprentissage automatique intégrée dans le SOAR, on peut analyser les données des outils de sécurité et recommander la manière de gérer les menaces à l'avenir.

Enfin, **l'automatisation des processus de réponse avec le SOAR peut réduire les erreurs humaines dans la gestion des incidents de sécurité.**
Selon l'indice relatif à la veille stratégique en matière de sécurité d'IBM, l'erreur humaine est impliquée dans plus de 90 % des incidents de sécurité (clic sur un lien de phishing, consultation d'un site Web suspect, activation de virus ou autres menaces persistantes avancées).
Il peut y avoir de graves conséquences comme la possibilité de ne pas détecter une menace, de ne pas répondre correctement à une attaque, ou de causer des fuites de données.
L'automatisation grâce au SOAR a donc plusieurs avantages, il réduit le nombre de tâches et d'opérations répétitives et réduit les risques d'erreurs humaines.

Conclusion

Les technologies SIEM et SOAR peuvent aider les organisations à se protéger des cyberattaques. Le SIEM et le SOAR peuvent être complémentaires.