

Comment garder une longueur d'avance sur les cybercriminels grâce à SIEM



Table des matières

1.	Le paysage commercial actuel	2
2.	Utiliser le SIEM pour garder une longueur d'avance sur les cybercriminels	2
	Bien surveiller votre environnement	3
	Éviter l'erreur humaine grâce à l'IA et à l'automatisation	4
	Mettre en place un système robuste de chasse aux menaces	4
	Disposer d'un plan de réponse aux incidents	5
3.	Aller plus loin avec Log360	6
	Gestion complète des journaux et audit des changements AD	6
	Renseignements sur les menaces	7
	UEBA optimisé par l'IA	7
	Gestion des incidents complète	8
	Pas une solution SIEM ordinaire	8

Le paysage économique actuel

Voici un constat alarmant : un cybercriminel peut s'introduire dans 93% des réseaux des entreprises. C'est l'une des constatations faites par [Positive Technologies](#) dans le cadre de sa nouvelle étude sur les projets d'intrusion (pentesting). Si l'on ajoute à cela que les organisations sont de plus en plus interconnectées, cela représente de grandes opportunités pour les cybercriminels et des préoccupations majeures pour les organisations.

Chaque organisation contient non seulement ses propres données, mais aussi celles de ses partenaires commerciaux. Ainsi, une organisation victime d'une attaque d'extorsion de données, par exemple, signifie que ses partenaires commerciaux sont également impliqués dans l'attaque. L'année dernière a montré qu'il s'agit d'un réel sujet de préoccupation. C'est pourquoi il n'est pas seulement impératif pour les organisations de sécuriser leurs réseaux, mais essentiel.

Utiliser SIEM pour garder une longueur d'avance sur les cybercriminels

Si le paysage actuel est inquiétant, ce n'est pas une cause perdue. Les solutions de cybersécurité se préparent à faire face aux nouvelles menaces, et la prochaine génération de solutions est prometteuse si elle est mise en œuvre correctement. Si vous cherchez à sécuriser votre réseau, le SIEM est une solution à privilégier.

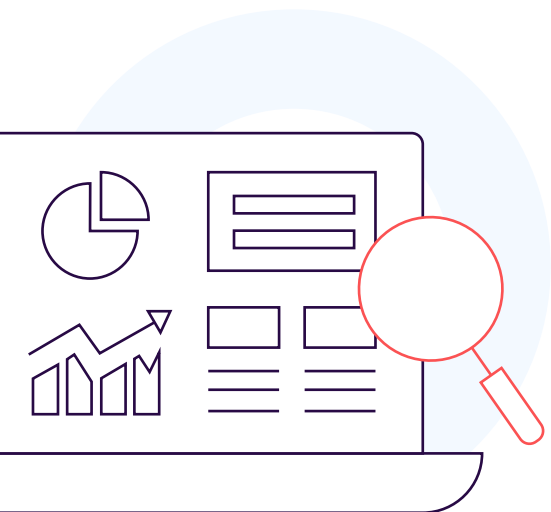
Outre la surveillance des journaux de votre réseau et l'émission d'alertes, les solutions SIEM intégrant l'automatisation et l'intelligence artificielle permettent de réduire considérablement les temps de réponse aux incidents ainsi que les erreurs humaines. Voici quatre façons de garder une longueur d'avance sur les cybercriminels grâce aux solutions SIEM :

- ✓ **Bien surveiller votre environnement**
- ✓ **Éviter l'erreur humaine en utilisant l'IA et l'automatisation**
- ✓ **Mettre en place un système robuste de chasse aux menaces**
- ✓ **Disposer d'un plan de réponse aux incidents**

Bien surveiller votre environnement

La première étape consiste à utiliser une solution SIEM pour surveiller tous les recoins de votre réseau. Les solutions SIEM fonctionnent avec des journaux et vous devez vous assurer que tous les journaux nécessaires sont introduits dans la solution. Une fois qu'une solution SIEM a collecté les journaux nécessaires, elle peut compiler les informations dans des rapports, des graphiques et d'autres formats qui peuvent être utilisés par les analystes de sécurité pour détecter les anomalies, corrélater les événements et identifier tout ce qui est préoccupant.

Voici quelques exemples de sources à partir desquelles les journaux peuvent être récupérés :



Postes de travail et terminaux

- Ordinateurs des utilisateurs
- Imprimantes

Périphériques

- VPNs
- Pare-feu

Réseaux Active Directory

- Serveurs DNS
- Contrôleurs de domaine

Applications cloud

- Amazon Web Server
- Azure AD
- Google Cloud
- Salesforce

Applications métier

- Serveurs Exchange
- Serveurs Web
- Bases de données
- Microsoft 365

Toutes ces sources de données de logs peuvent être compilées pour fournir les informations nécessaires sur votre environnement. Cependant, la quantité de journaux collectés est énorme, et les passer au crible manuellement pour trouver des modèles prend du temps, demande beaucoup de travail et présente un risque d'erreur humaine. L'automatisation peut pallier ces inconvénients.

Éviter l'erreur humaine grâce à l'IA et à l'automatisation



L'utilisation du ML et de l'IA se développe parmi les solutions SIEM, car ces technologies peuvent identifier efficacement les anomalies dans le réseau d'une organisation. Par exemple, ManageEngine Log360 utilise des technologies de ML et d'IA pour détecter les comportements inhabituels des employés. Cela peut aider à détecter les initiés malveillants en utilisant des modèles qui sont souvent manqués lors de la corrélation manuelle des événements.

Un point clé à noter est que l'intervention humaine ne peut pas encore être complètement évitée. Cependant, l'IA et le ML peuvent réduire considérablement les temps de réponse aux incidents, car ils peuvent analyser de grands ensembles de données plus rapidement qu'un examen manuel. Cela réduit également le besoin de travail humain et, par conséquent, l'erreur humaine.

Mettre en place un système robuste de chasse aux menaces



Les cyberattaques évoluent constamment et les pirates informatiques sont de plus en plus compétents pour identifier et exploiter les failles du réseau d'une entreprise. Si les organisations peuvent se défendre contre les types d'attaques qui se sont déjà produites, il est plus difficile d'identifier les modèles d'attaque qui exploitent les vulnérabilités de type "zero-day", par exemple.

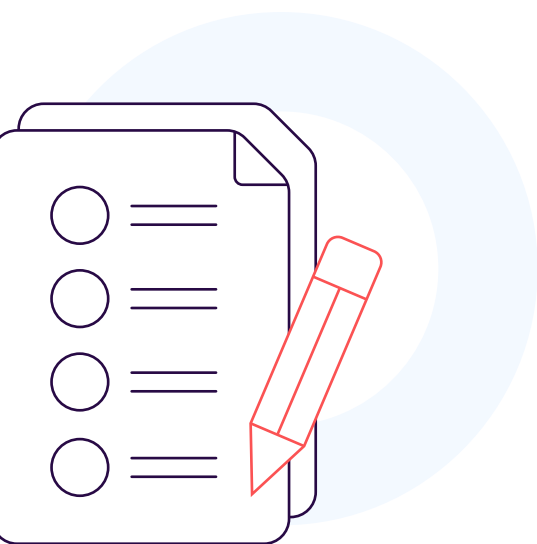
C'est pourquoi les organisations doivent mettre en place un système capable de détecter les acteurs malveillants et les attaques cachées qui ont pu échapper à vos systèmes de défense initiaux. Les solutions SIEM peuvent utiliser des systèmes de réponse aux événements en temps réel qui peuvent vous alerter sur toute menace latente.

Ces solutions peuvent extraire des données d'une liste globale d'adresses IP sur liste noire ou d'autres sources d'informations sur les menaces et corréler ces données avec les journaux de votre réseau pour voir s'il y a eu une violation de la sécurité.

À ce stade, si une alerte a été déclenchée, on peut supposer qu'une attaque est déjà en cours. L'organisation doit donc passer aux mesures d'atténuation pour réduire les dégâts autant que possible. Si la détection précoce des attaques est une excellente chose, elle ne résout que la moitié du problème. Une atténuation pleinement réussie comprend la détection précoce des attaques combinée à une réponse forte aux incidents.

Disposer d'un plan de réponse aux incidents

Un incident de sécurité peut être un incident interne ou externe, et une organisation doit être prête à faire face aux deux. Les solutions SIEM sont capables de fournir des alertes en temps réel sur les incidents de sécurité majeurs. De plus, les solutions SIEM les plus complètes vous permettent également de configurer vos alertes de sorte que, en cas d'activité malveillante dans une base de données critique ou d'accès à un fichier sensible par un employé non autorisé, la solution puisse alerter immédiatement l'équipe de sécurité.



La deuxième partie de la gestion d'un incident est le plan de réponse. L'automatisation peut jouer un rôle crucial à cet égard, car le temps est un facteur essentiel. Que faire si personne n'est immédiatement disponible pour déclencher un plan d'intervention en cas d'incident ? Dans ce cas, la préconfiguration d'un plan de réponse aux incidents pour certains incidents critiques donnera à l'équipe de sécurité un délai pour mettre en œuvre des mesures de sécurité supplémentaires pendant que la solution SIEM se charge des mesures initiales de réponse aux incidents.

Par exemple, le tableau de bord des alertes de Log360 offre la possibilité de configurer des scripts personnalisés pour certaines alertes si l'organisation le juge nécessaire. Ainsi, une réponse immédiate est mise en place pour stopper toute attaque en cours et les équipes informatiques ont le temps de concevoir des contre-mesures pour corriger les failles, supprimer les coquilles web malveillantes, révoquer l'accès aux fichiers et systèmes critiques, etc. afin de réduire les dommages causés.

Aller plus loin avec Log360

Log360 est une solution complète de SIEM et d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR), facile à utiliser grâce à son interface intuitive et offrant de puissantes fonctionnalités. La solution peut prendre en charge toutes les fonctions mentionnées jusqu'à présent et plus encore pour garantir la sécurité de votre organisation. Voici ce que vous pouvez faire avec Log360 :

Gestion complète des journaux et audit des modifications AD

Log360 prend en charge une liste exhaustive de sources pour la collecte des journaux, telles que les plateformes de bases de données, les serveurs Web, les routeurs et les commutateurs, les hyperviseurs, les scanners de vulnérabilité, les systèmes Linux et Unix, les pare-feu, les VPN et les solutions de sécurité des terminaux. Toutes les informations recueillies sont traduites dans un format commun et affichées sous forme de tableaux et de graphiques faciles à lire dans le tableau de bord.

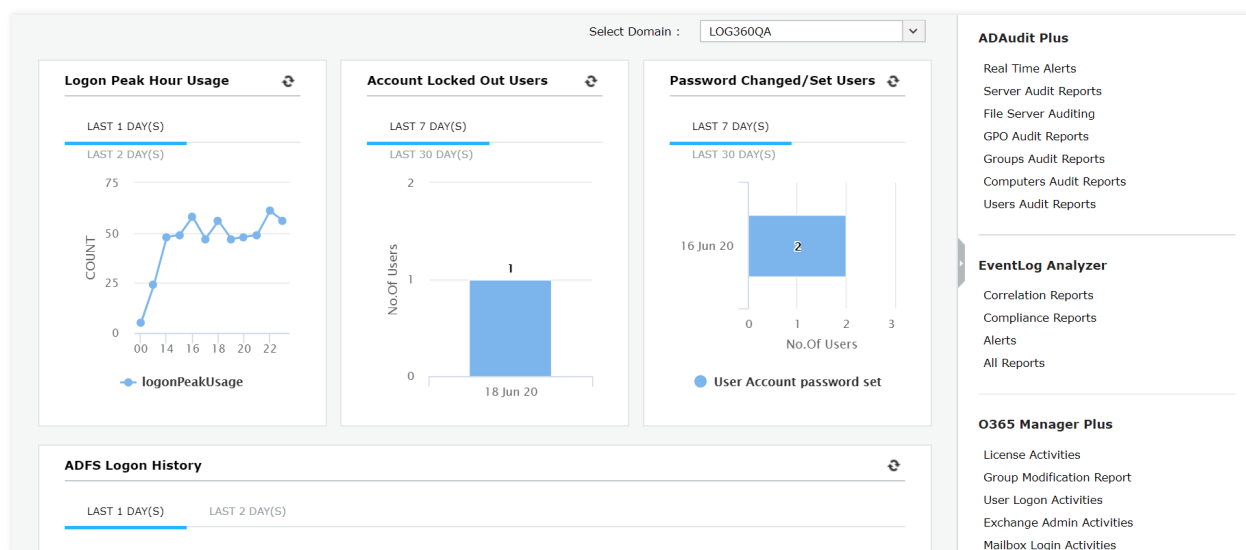


Figure 1 : Le tableau de bord du module d'audit de Log360

Outre l'affichage des données, Log360 stocke les journaux de manière sécurisée pour générer des rapports qui peuvent être utilisés à des fins d'audit et de gestion de la conformité. Il existe des rapports préconfigurés pour les mandats de conformité tels que HIPAA, SOX, le RGPD, et plus encore, qui sont utiles pour répondre aux exigences de conformité. Log360 utilise également les journaux pour générer des alertes en cas d'incidents critiques et déclencher des mécanismes de réponse aux incidents s'ils sont configurés.

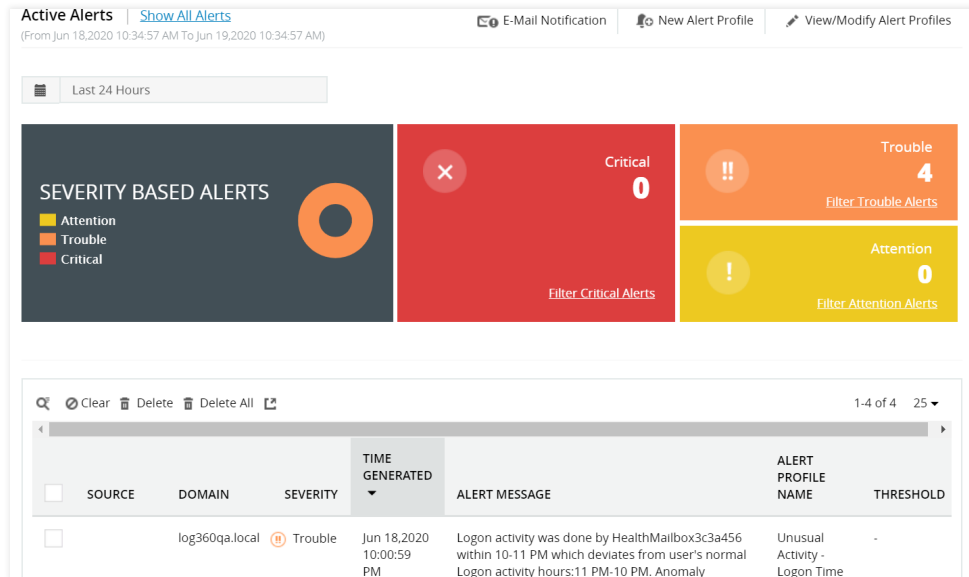


Figure 2 : Le tableau de bord des alertes dans Log360

Renseignements sur les menaces

Log360 est livré avec un ensemble robuste de fonctions de veille sur les menaces qui aident les équipes de sécurité à détecter les menaces internes et externes, et à traquer les attaques cachées potentielles et les acteurs malveillants. Log360 peut :

- Mettre en corrélation une liste noire mondiale d'IP avec les IP qui interagissent avec votre réseau et déclencher des alertes en cas de correspondance.
- Utiliser **STIX**, un langage structuré pour les solutions de renseignement sur les cybermenaces.
- Utilisez **TAXII**, un mécanisme de transport pour le partage des renseignements sur les cybermenaces.
- Utilisez AlienVault **OTX**, le réseau de partage et d'analyse des informations sur les menaces à source ouverte qui fait le plus autorité au monde.

UEBA alimentée par l'IA

L'automatisation fait partie intégrante de Log360. Un pas de plus dans cette direction consiste à utiliser le ML et l'IA. C'est là que l'analyse du comportement des utilisateurs et des entités (UEBA) entre en jeu. L'UEBA est une technique de cybersécurité pour la détection des anomalies qui peut être utilisée pour détecter les signes d'activités anormales des utilisateurs, des hôtes ou d'autres entités au sein de l'organisation.

La solution UEBA apprend à connaître les modèles de comportement des utilisateurs et des entités au sein d'une organisation afin de créer une base de référence pour le comportement normal. La solution utilise ensuite cette ligne de base pour détecter les comportements anormaux et calculer un score de risque, de sorte que les équipes de sécurité peuvent utiliser les scores pour détecter les signes de menaces internes, de compromission de comptes ou d'exfiltration de données bien avant que les dommages ne soient causés.

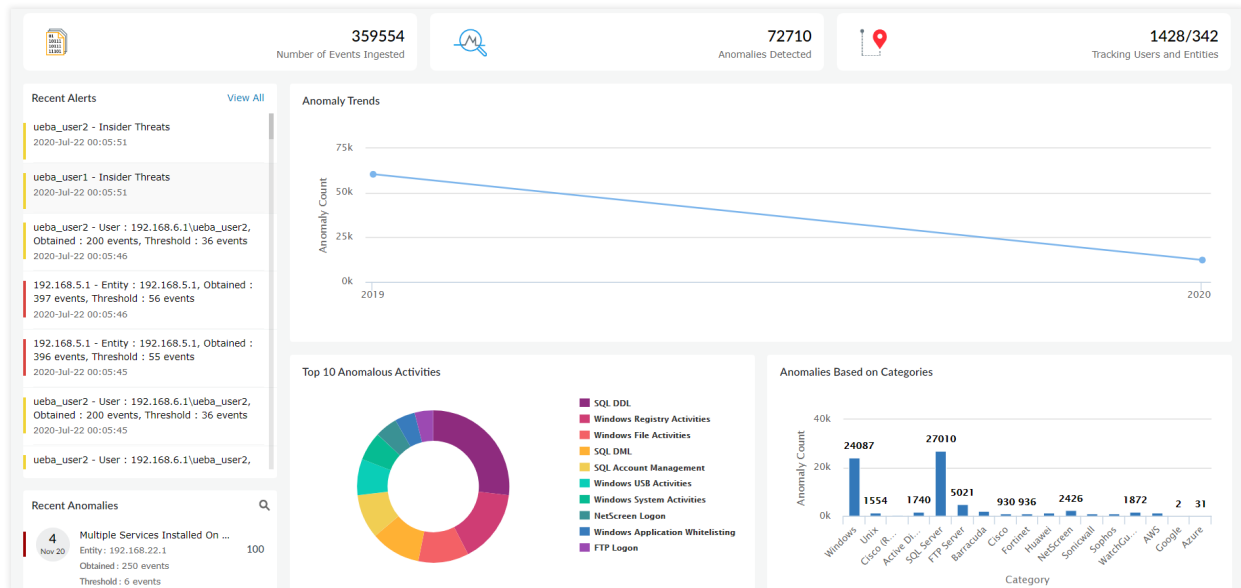


Figure 3 : Le tableau de bord UEBA dans Log360

Gestion des incidents complète

Log360 est doté d'un ensemble de fonctions solides pour aider les organisations à élaborer un plan de gestion des incidents de complet. La plateforme de renseignement sur les menaces de la solution peut efficacement prendre en charge la détection des incidents et les alertes en temps réel, tandis que les flux d'incidents peuvent être utilisés pour mettre en place des mécanismes de réponse aux incidents qui se déclenchent immédiatement. Cela permet de réduire le temps moyen de détection et le temps moyen de résolution d'un incident - deux critères importants sur lesquels repose le succès des mesures d'atténuation.

Select view : All incidents

Name	Created By	Created Time	Assignee	Status	Severity	Due Date
Brute force	admin	2021-08-21 17:59:26	admin	Open	Attention	2021-08-25 00:00:00

Figure 4 : Gestion des incidents dans Log360

Pas une solution SIEM ordinaire

Outre les fonctionnalités mentionnées ci-dessus, Log360 est capable de nombreuses autres fonctions puissantes qui renforcent la sécurité d'une organisation. Log360 est une solution SOAR efficace qui permet d'accélérer la résolution des incidents en hiérarchisant les menaces de sécurité, en automatisant les réponses aux incidents et en accélérant les enquêtes et les réponses aux incidents.

Log360 offre une meilleure visibilité sur vos données en vous permettant de surveiller et de sécuriser spécifiquement les informations d'identification personnelle dans les serveurs de fichiers, de repérer les comportements inhabituels sur ces fichiers et même de bloquer les ports USB pour éviter les fuites de données.

En outre, Log360 prend également en charge la sécurité de l'environnement cloud de votre entreprise et vous permet d'obtenir une visibilité sur vos infrastructures cloud AWS, Azure, Salesforce et Google Cloud Platform. Il vous permet de surveiller en temps réel les modifications apportées à vos utilisateurs, aux groupes de sécurité du réseau, aux clouds privés virtuels, les changements de permission, etc. qui se produisent dans votre environnement de cloud.

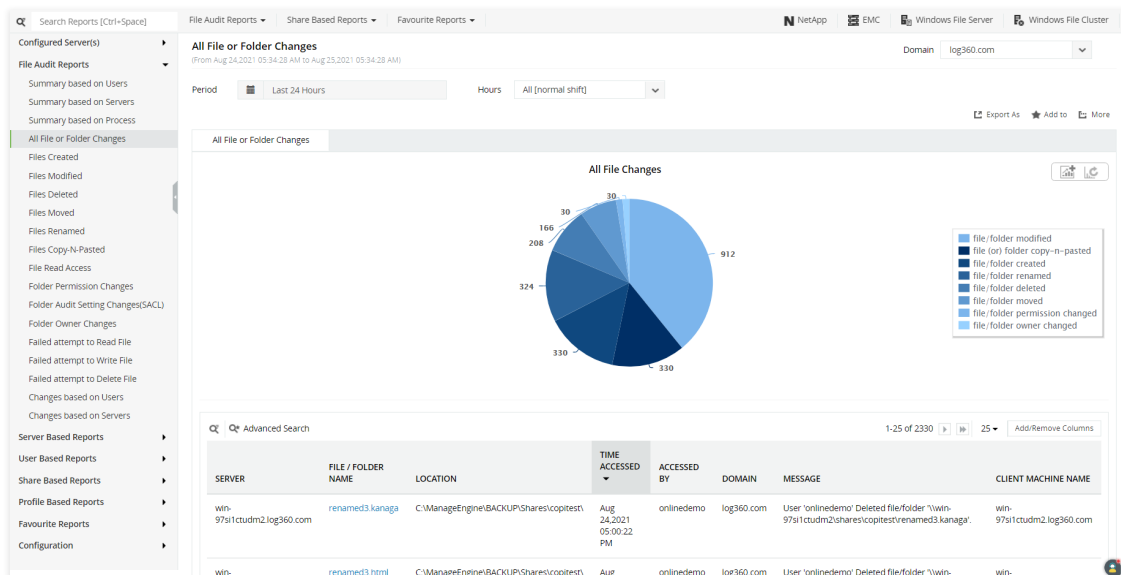


Figure 5 : Surveillance de tous les changements de fichiers dans Log360

Log360 peut donc prendre en charge la sécurité sur site et dans le cloud d'une organisation en allant au-delà de ce que les solutions SIEM traditionnelles peuvent offrir.