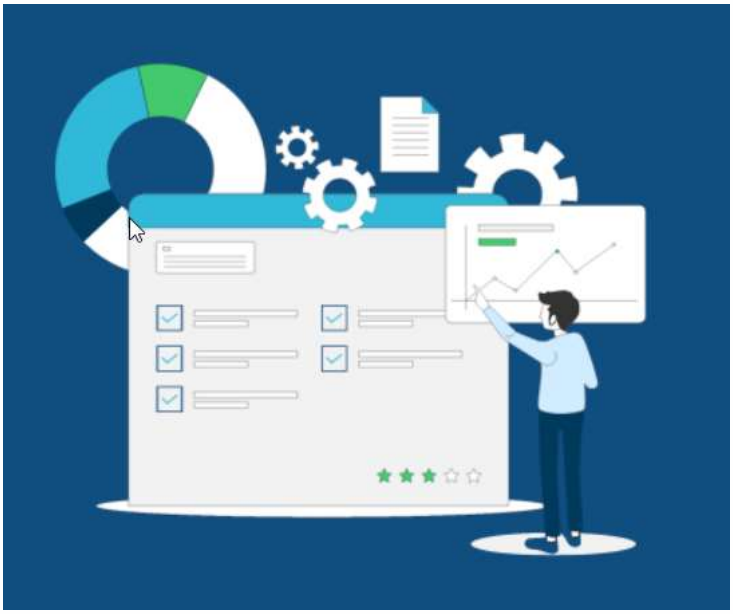

Analyse des évènements 2
1 : Introduction générale
Année académique 2026-2026
Guy Paquet

Table des matières

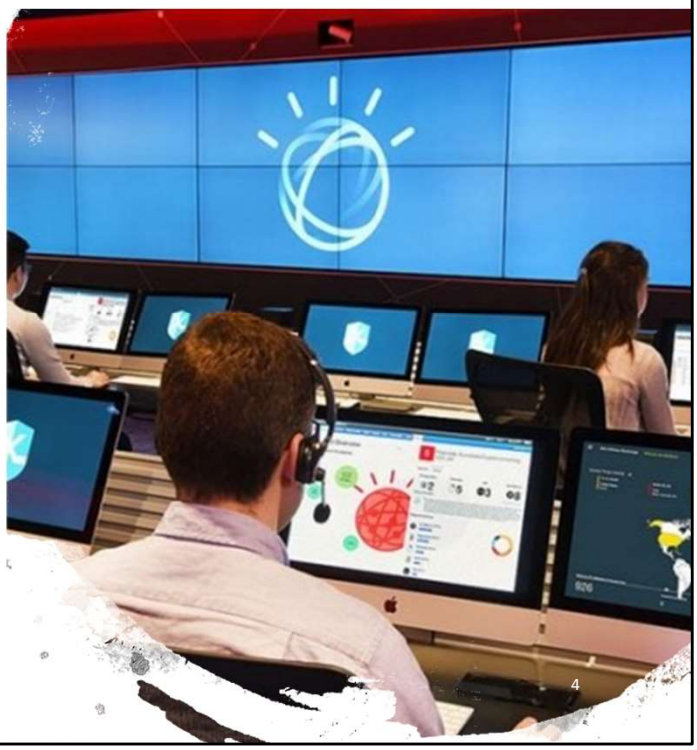


1. Présentation du cours

Analyse des Evénements / Gestion des Logs

Objectifs

- Comprendre l'importance de la gestion des évènements de sécurité dans les réseaux modernes
- Identifier les moyens techniques pour la collecte et la corrélation des données d'une multitude de sources
- Etudier les processus à mettre en place pour que les incidents de sécurité soient correctement identifiés, analysés, défendus, enquêtés et signalés
- Appréhender le fonctionnement d'un SIEM (Security Information & Event Management)



L'analyse d'événements IT est importante car elle permet:
1. De surveiller les systèmes informatiques et les réseaux pour détecter les anomalies et les problèmes potentiels.
2. D'améliorer la sécurité en détectant les tentatives d'intrusion et les menaces informatiques.
3. De faciliter la résolution des problèmes informatiques en fournissant des données détaillées sur les événements qui ont causé les problèmes.
4. D'optimiser les performances en identifiant les goulots d'étranglement et les tendances de rendement.
5. De respecter les réglementations en fournissant une documentation complète des activités informatiques.

Organisation du cours

Théorie : 4 séances de 2h

- Séances 2 et 3 : analyse de base (idem cours de B2)
- Séance 4 : analyse avancée NOUVEAU

Séance 1	• Présentation générale du cours • Introduction à la gestion des logs et des évènements • Rappel : c'est quoi les logs ? • Introduction aux SIEM

Séance 2	• Infrastructure de gestion des logs
	  • Architecture
	  • Fonctions
	  • Syslog

Séance 3	• Processus opérationnels de gestion des logs
	  • Génération des logs
	  • Analyse des logs
	  • Prioritisation

Séance 4	• Gestion avancée des évènements
	  • Gestion des incidents
	  • Analyse des flux réseaux
	  • Gestion des menaces
	  • Orchestration

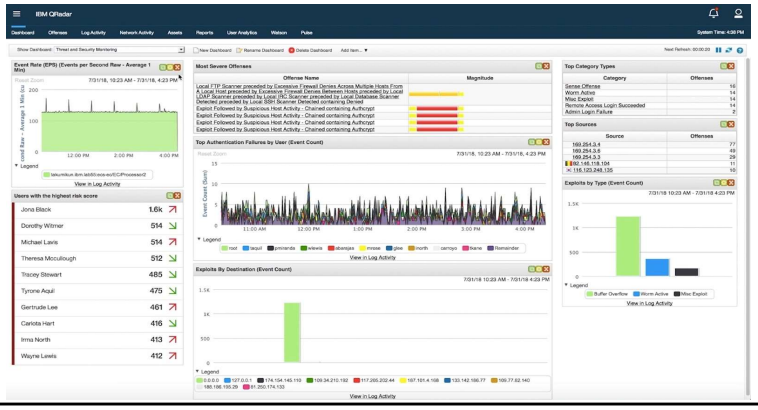
5

Organisation du cours

Labo : 4 séances de 4h

Exercices autour de l'utilisation de Qradar CE

- Installation, configuration
- Découverte de l'interface
- Collecte et analyse de données
- Elaboration de règles de détection
- Use Cases



Evaluation du cours

L'examen théorique est écrit. L'étudiant doit répondre à des questions (QCM, questions ouvertes, …) couvrant la matière vue pendant les séances de théorie.

2 parties :
- Analyse de base (séances 1-2-3)
- Analyse avancée (séance 4)

Pour la partie pratique en laboratoire, l'étudiant utilise une machine virtuelle déjà configurée avec l'outil SIEM utilisé durant les labos et sur laquelle il doit effectuer des manipulations.

	Septembre - Janvier	Deuxième session
Travaux	Travail pratique à réaliser en labo durant la session d'examen pondération : 50%	Travail pratique à réaliser en labo durant la session d'examen pondération : 50%
Interros		
Examens	Examen théorique pondération : 50%	Examen théorique pondération : 50%
Supervision		
Autres		

* Pondération en % par rapport au total de l'activité d'apprentissage

7

La référence : NIST

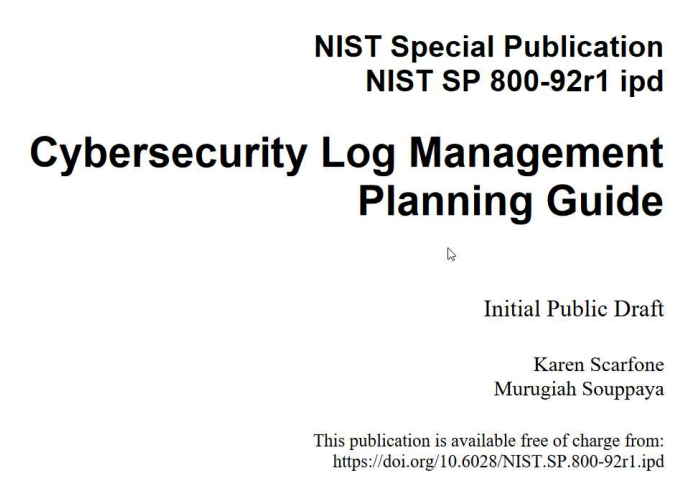
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

Ce document de 2023 est la version revue d'un ancien document de 2006 souvent cité comme la publication de référence concernant la gestion des logs.

Disponible sur

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-92r1.ipd.pdf



NIST Special Publication
NIST SP 800-92r1 ipd

Cybersecurity Log Management Planning Guide

Initial Public Draft

Karen Scarfone
Murugiah Souppaya

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-92r1.ipd

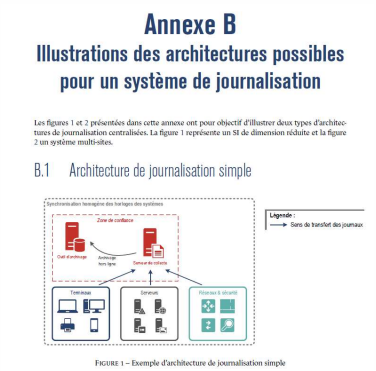
Le « Cybersecurity Log Management Planning Guide" du NIST définit un guide d'action pour aider toute organisation à planifier des améliorations de ses pratiques de gestion des journaux de cybersécurité afin de répondre aux exigences réglementaires et aux pratiques recommandées. Bien que ce guide ne soit pas exhaustif, les actions proposées sont remarquables et généralement bénéfiques pour la planification de la gestion des journaux de cybersécurité par les organisations

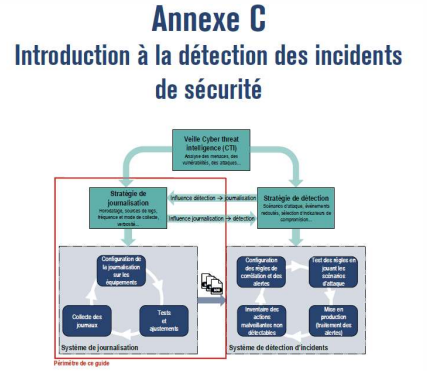
Le document aborde également les aspects juridiques et les exigences réglementaires liées à la gestion des journaux de sécurité informatique. Le but est d'aider les organisations à améliorer la sécurité de leur réseau en fournissant des informations détaillées sur les activités de sécurité informatique, ce qui peut faciliter la détection et la résolution des problèmes de sécurité.

La référence : ANSSI

Recommandations de sécurité pour l'architecture d'un système de journalisation

Cette note technique détaille les prérequis nécessaires à la mise en œuvre d'un système de journalisation efficace et sécurisé et présente les bonnes pratiques permettant de bâtir une architecture de gestion de journaux pérenne, quelle que soit la nature du système d'information (SI bureautique, SI industriel, SI classifié...).





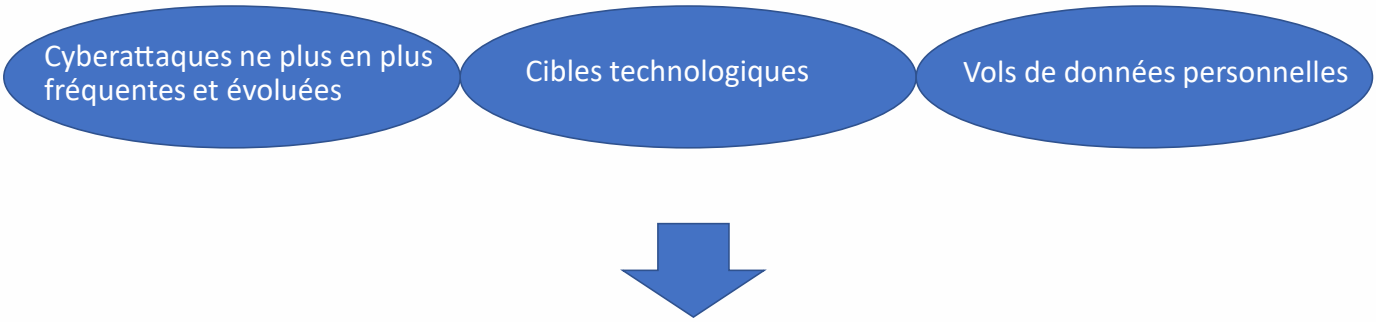
Les journaux d'évènements constituent une brique technique indispensable à la gestion de la sécurité des systèmes d'information, quelles que soient la nature et la taille de ces derniers. Les journaux sont une source d'information riche qui peut être utilisée a priori pour détecter des incidents de sécurité.

Dans ce cas, les évènements constituant les journaux sont consultés et analysés en temps réel. Les journaux peuvent également être employés a posteriori pour retrouver les traces d'un incident de sécurité ; l'analyse des journaux d'un ensemble de composants (postes de travail, équipements réseaux, serveurs, etc.) peut alors permettre de comprendre le cheminement d'une attaque et d'évaluer son impact.

La version en vigueur de ce guide ANSSI est disponible au téléchargement sur https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation

2. Introduction à l'analyse des évènements

Importance des évènements en sécurité



L'analyse des évènements permet de connaitre l'état de la sécurité du système d'information

Les cybermenaces entrent de façon pérenne dans la réalité quotidienne des entreprises. Les cyberattaques sont et seront de plus en plus fréquentes, multiples (c'est-à-dire mettant combinaison de plusieurs cyberattaques), discrètes et évoluées. Elles s'inscrivent dans la durée. Elles ne ciblent plus seulement les systèmes technologiques mais aussi directement les personnes (salariés, prestataires, partenaires, fournisseurs, clients), en leur dérobant des informations primordiales qui accroissent ensuite considérablement leur capacité de nuisance.

[Ref : SUPERVISION DE LA SECURITE DU SYSTEME D'INFORMATION DANS LES SECTEURS BANQUE ET ASSURANCE, Etude ATOS de juin 2016, https://www.forum-des-competences.org/assets/files/v1/Livrables/supervision-de-la-securite-des-si-dans-les-secteurs-banque-et-assurance-soc.pdf]

La gestion des événements/incidents de sécurité de l'information constitue un élément essentiel du cycle de vie de la sécurité de l'information. cette démarche consiste à définir un ensemble de mesures techniques et organisationnelles pour faire face aux différentes menaces qui pèsent sur le patrimoine informationnel d'une organisation.

Risque identifié dans le classement OWASP TO 10

Catégorie A09 - Carence des systèmes de contrôle et de journalisation

12

OWASP Top 10 est un ensemble de 10 des plus grandes vulnérabilités de sécurité Web, publiées par l'Open Web Application Security Project (OWASP).

La dernière classification date de 2021, la prochaine est attendue en 2025.

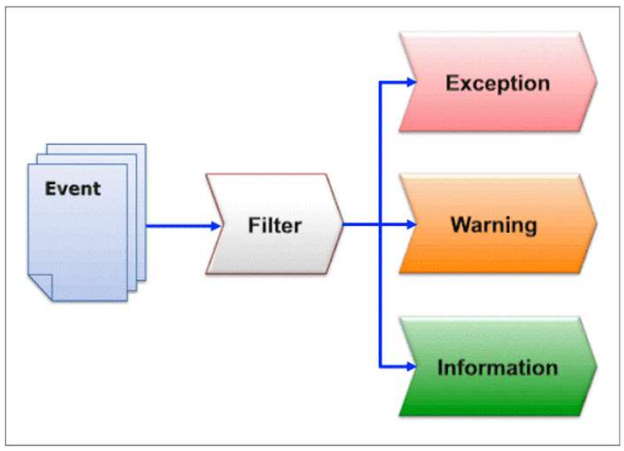
La catégorie A09 a pour but d'aider à la détection, à l'escalade et à la réponse aux brèches actives. Sans journalisation et surveillance, les brèches ne peuvent être détectées. Une journalisation, une détection, une surveillance et une réponse active insuffisantes peuvent survenir à tout moment.

Détails sur https://owasp.org/Top10/fr/A09_2021-Security_Logging_and_Monitoring_Failures/

C’est quoi un évènement informatique ?

Selon le processus ITIL®, un événement est un ***changement d'état significatif d’un élément ou d’un service*** dans l’infrastructure IT

3 niveaux d’évènement



https://wiki.octopus-itsm.com/fr/articles/gestion-des-evenements-processus-itilr

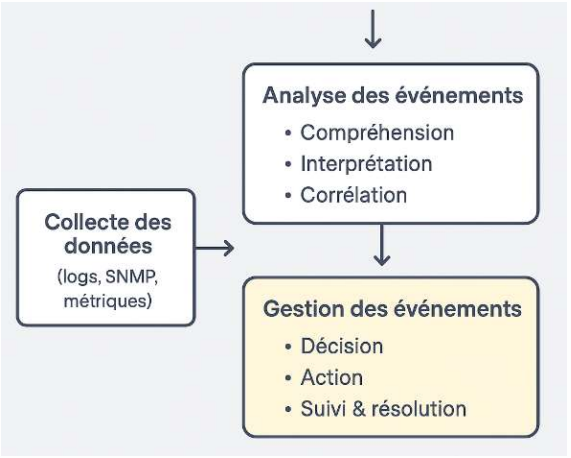
Dans le cadre du processus ITIL, un événement informatique est un indicateur observable d'une situation qui nécessite une attention immédiate pour assurer le fonctionnement optimal des services informatiques. Les événements informatiques peuvent être des alertes logicielles, des messages d'erreur, des pannes matérielles ou tout autre incident qui affecte la disponibilité, la performance ou la qualité des services informatiques.

ITIL (pour « *Information Technology Infrastructure Library* », ou « Bibliothèque pour l'infrastructure des technologies de l'information » en français) est un ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») du management du système d'information.

https://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

Différences entre analyse et gestion des évènements

Gestion des évènements	Analyse des évènements
Processus plus **global et organisé**, qui inclut la détection, la priorisation, la réponse et le suivi des événements. Activité **opérationnelle** et **organisationnelle**.	Processus d'**examen et d'interprétation** des événements collectés (logs, traps SNMP, métriques). Activité **technique** et **diagnostique**
Objectif : décider **quoi faire** et **qui agit** suite à un événement.	**Objectif :** comprendre **ce qui s'est passé** et pourquoi.
Exemple : Des Logs montrent une intrusion → déclenchement d'une alerte sécurité et escalade à l'équipe de support.	**Exemple :** Lecture d'un log système : "Erreur d'authentification multiple sur un serveur".

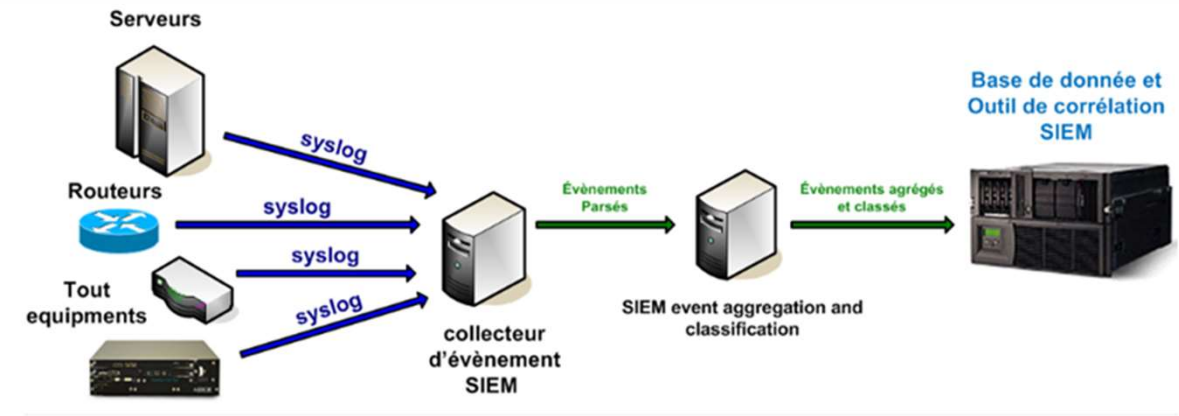


L'**analyse des événements** consiste à interpréter les données collectées (logs, traps SNMP, métriques) pour comprendre ce qui s'est passé et en identifier la cause.
La **gestion des événements**, elle, va plus loin : elle organise la réponse, priorise les incidents, assigne les actions et assure le suivi jusqu'à leur résolution.
En résumé, l'analyse produit une compréhension technique, tandis que la gestion transforme cette compréhension en décisions et en actions concrètes.
Les deux sont complémentaires pour assurer la disponibilité, la sécurité et la résilience d'une infrastructure IT

Analyse des évènements

La mise en place d'un outil d'analyse des évènements nécessite de transférer les logs vers un serveur central qui permettra de mesurer le niveau de sécurité, de détecter d'éventuelles menaces et d'enclencher les éventuelles actions à entreprendre, le tout en temps réel ou pas.

Exemple de système : le SIEM (Security Information & Event Management).

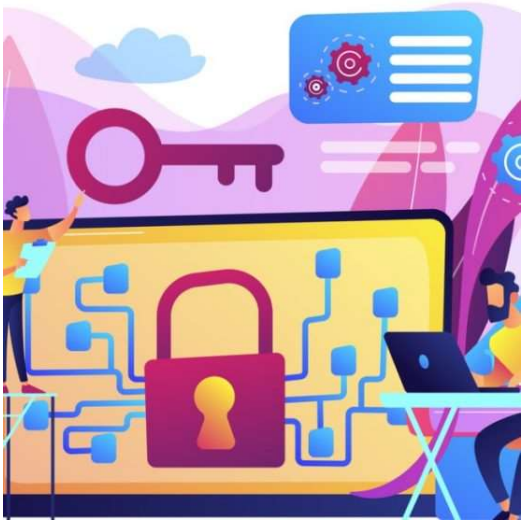


https://www.orange-business.com/fr/blogs/securite/securite-du-poste-de-travail/du-bon-usage-des-logs-de-securite

Le transfert des logs vers un serveur central est important pour plusieurs raisons :
1. Centralisation des données : En centralisant les logs, il est possible d'avoir une vue complète de l'ensemble des événements se produisant sur les différents équipements de l'infrastructure informatique.
2. Facilitation de l'analyse : La centralisation des logs permet une analyse plus rapide et plus efficace des données, ce qui peut aider à résoudre les problèmes plus rapidement.
3. Archivage à long terme : Les logs centralisés peuvent être archivés à long terme pour une utilisation future, par exemple pour répondre aux exigences réglementaires ou pour effectuer des analyses postérieures.
4. Amélioration de la sécurité : Le transfert des logs vers un serveur central permet une meilleure protection des informations sensibles, en empêchant les attaques de suppression de logs ou de falsification de données.
5. Réduction de la complexité : La centralisation des logs peut aider à simplifier la gestion des journaux, en réduisant la quantité de données à gérer sur chaque équipement individuel.

Quelques cas d’usage (Use Case) importants

- Détection d’exfiltration de données
- Détection des identifiants utilisateur compromis
- Détection des comportements inhabituels sur les comptes privilégiés
- Détection des attaques de phishing
- Surveillance des charges et des disponibilités (uptimes)
- Chasse aux menaces



16

https://www.logpoint.com/en/understand/top-10-use-cases-implement/

Les "use cases" en analyse d'événements sont des scénarios d'utilisation décrivant comment les événements sont utilisés pour résoudre des problèmes spécifiques ou détecter des comportements indésirables. Ils décrivent les besoins en matière de surveillance, les données d'entrée nécessaires et les étapes pour résoudre le problème ou détecter l'anomalie. Les use cases peuvent aider à définir les règles de corrélation et les critères d'alerte pour la surveillance des événements.

3. Rappel : c’est quoi des logs ?

Log(s) = enregistrement(s) relatif à un événement ayant eu lieu sur un système informatique au sens large

→ sur un pc, un serveur, un périphérique réseau, une imprimante, …

→ évènements de nature fort diverse : système, hardware, sécurité, audit, network, …

5 grands types :

- logs de système
- Logs d'application
- Logs de sécurité
- Logs de réseau
- Logs de base de données

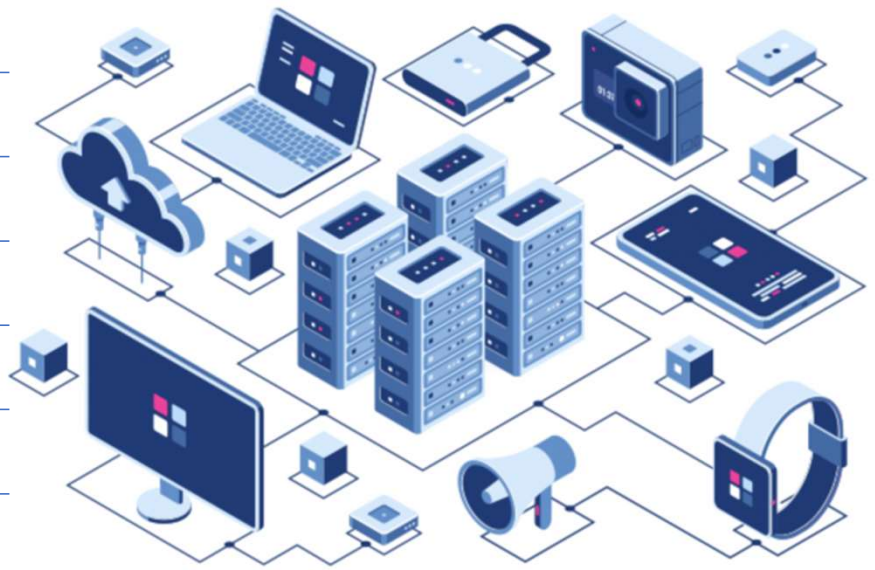
18

Rappel : un **log** est **un fichier qui enregistre des événements qui se produisent sur un système d'exploitation** ou tout autre équipement informatique, routeur, switch, serveur.
Les logs sont aussi appelés des *fichiers journaux*.

Les principaux types de logs sont :
1. Logs de système : Ceux-ci incluent des informations sur l'état du système, les erreurs du noyau et les événements liés à la sécurité.
2. Logs d'application : Ceux-ci incluent des informations sur les erreurs dans les applications, les transactions et les comportements d'utilisateurs.
3. Logs de sécurité : Ceux-ci incluent des informations sur les tentatives d'intrusion, les violations de sécurité et les alertes de sécurité.
4. Logs de réseau : Ceux-ci incluent des informations sur les erreurs de réseau, les activités de liaison et les activités liées à la sécurité du réseau.
5. Logs de base de données : Ceux-ci incluent des informations sur les erreurs de base de données, les requêtes et les transactions de base de données.

Logs générés par les principaux composants

- Antimalwares
- IDS & IPS
- VPN
- Routeurs
- Proxy WEB
- Serveurs d'authentification
- Firewalls
- Scanners de vulnérabilités



19

Connaître les principales sources de logs et quels composants les génèrent est crucial pour une surveillance efficace des systèmes et de la sécurité informatique.

Cela permet aux organisations de :

Assurer une couverture complète : En identifiant tous les composants clés, aucun événement critique n'est manqué.

Simplifier l'analyse : Comprendre l'origine des logs aide à corréler les événements et à détecter plus efficacement les anomalies.

Améliorer la réponse aux incidents : L'identification rapide des composants affectés permet une enquête et une mitigation plus rapides.

Soutenir la conformité et l'audit : Savoir d'où proviennent les logs pertinents permet de répondre aux exigences réglementaires.

Optimiser la gestion des logs : Cela aide à prioriser, stocker et conserver les logs de manière efficace.

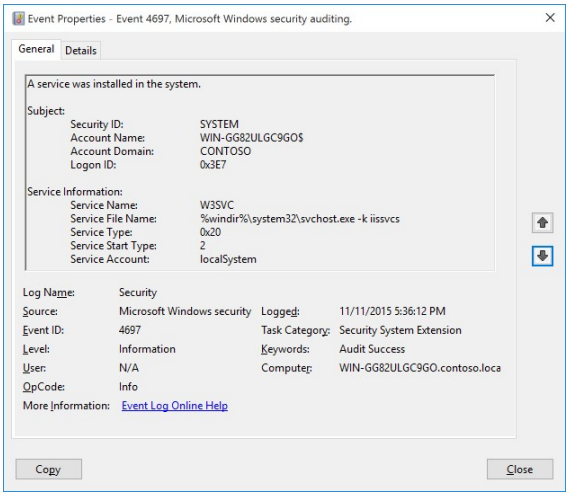
Evénement de niveau Information

Type d'événement qui ne demande aucune action.

Typiquement utilisé pour confirmer le statut d'un équipement ou d'un service, pour le succès d'une transaction ou d'une activité, ou pour générer des statistiques d'analyse.

Exemples :

- Une tâche en traitement différé (batch job)a été exécutée avec succès
- Un service est installé sous Windows10 avec succès



Un événement de type information est un événement qui n'a pas de conséquences immédiates pour les services informatiques et ne nécessite pas d'action immédiate. Il peut s'agir d'une notification d'un logiciel ou d'un message d'alerte qui peut être utile pour comprendre les tendances ou pour surveiller les activités sur les systèmes informatiques, mais qui n'affecte pas le fonctionnement des services informatiques.

Les événements de type information sont généralement enregistrés et analysés pour aider à déterminer s'ils peuvent potentiellement devenir des incidents graves à l'avenir.

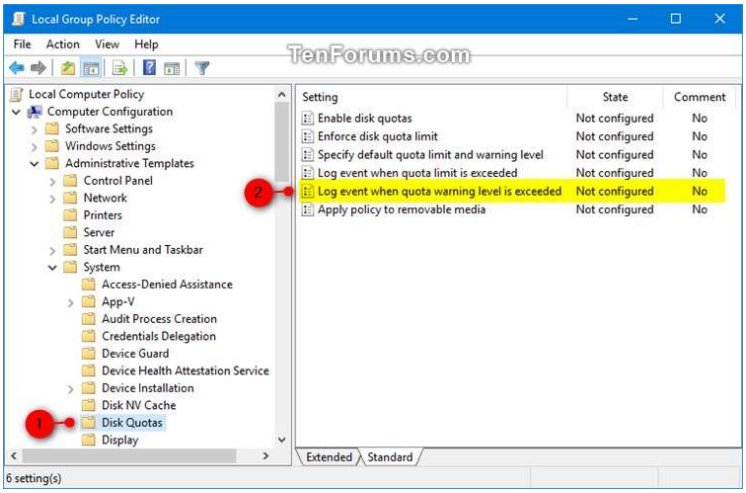
— Evénement de niveau Avertissement (Warning)

Type d'événement signalant l'approche d'un seuil.

Informe que la situation doit être vérifiée et que les actions appropriées doivent être posées pour éviter une exception (panne). L'avertissement signifie une activité inhabituelle.

Exemples :

- L'espace disque d'un serveur est à 65 % et augmente; s'il atteint 75 %, le temps réponse devient inacceptable.
- Le temps d'exécution d'une transaction est plus long de 10 %.
- Le taux de transmission de données par paquet a augmenté de 15 % la dernière heure.



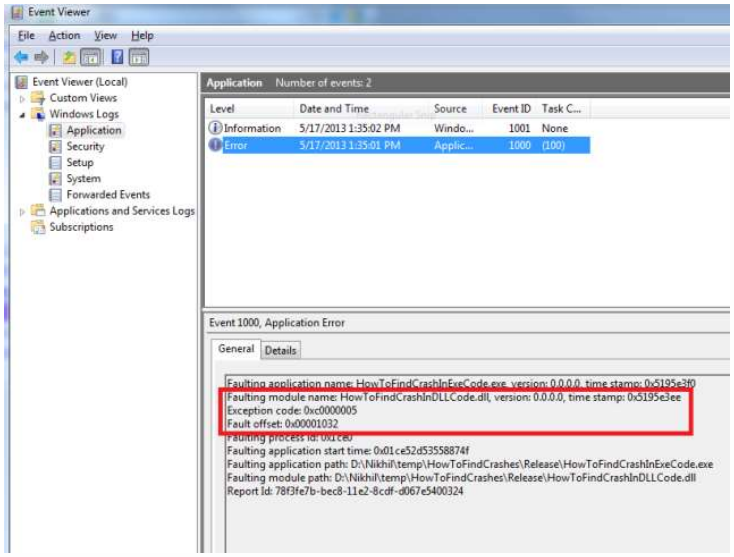
Un événement de type "warning" est un événement qui signale un problème potentiel qui peut affecter les services informatiques, mais qui n'a pas encore causé de perturbation significative. Les événements de type "warning" peuvent inclure des alertes logicielles, des messages d'erreur ou des indicateurs de performance qui peuvent prédire un incident futur.

— Evénement de niveau Exception

Type d'événement signalant qu'un équipement fonctionne de façon anormale qui provoque ou risque de provoquer un impact négatif sur les activités d'affaires.

Exemples :

- Un serveur est en panne.
- Plus de 150 utilisateurs se sont authentifiés en même temps sur une application.
- Une application a crashé sous Windows



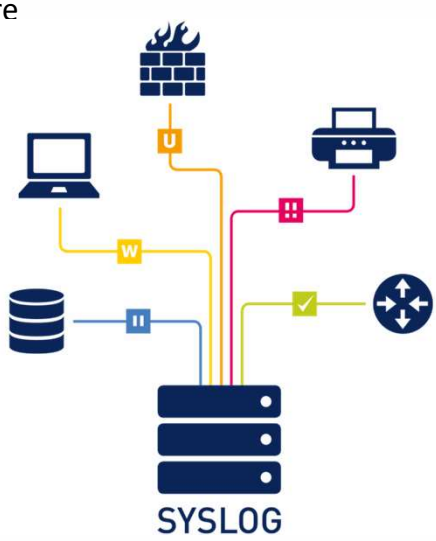
Un événement de type "exception" est un événement qui signale une situation anormale qui affecte la disponibilité, la performance ou la qualité des services informatiques. Les événements de type "exception" peuvent inclure des alertes logicielles, des erreurs de système, des pannes matérielles ou tout autre incident qui peut affecter les services informatiques.

Les événements de type "exception" sont généralement surveillés en temps réel et des actions immédiates peuvent être nécessaires pour corriger la situation et minimiser les impacts sur les utilisateurs finaux et les services informatiques.

Transfer des événements

Pour permettre de repérer plus rapidement et efficacement les défaillances d'ordinateurs présents sur un réseau, les journaux d'évènements doivent être centralisés.

Les échanges de ces journaux se font au travers du protocole **syslog**.



Contenu d'un log au format syslog:

- la date à laquelle a été émis le log,
- le nom de l'équipement ayant généré le log (hostname),
- une information sur le processus qui a déclenché cette émission,
- le niveau de priorité du log,
- un identifiant du processus ayant généré le log et enfin un corps de message.

exemple :

```
Sep 14 14:09:09 machine_de_test dhcp service[warning] 110 corps du message
```

https://fr.wikipedia.org/wiki/Syslog

Syslog est un protocole standard utilisé pour la centralisation des journaux d'événements informatiques. Il permet aux différents équipements informatiques, tels que les serveurs, les périphériques réseau, les pare-feu, etc., de transmettre des informations de journaux d'événements à un serveur central de collecte. Le serveur central peut collecter des informations de journaux d'événements provenant de plusieurs sources différentes et les stocker pour une analyse ultérieure.

Gravité des événements

En normalisant la représentation de la catégorie et de la gravité d'un log, SYSLOG a rendu possible l'**interopérabilité** entre équipements de collecte de journaux et équipements de génération d'alertes.

Syslog fournit des informations de journalisation à différents niveaux. Il existe 8 niveaux de Syslog.

SYSLOG LEVELS
seq no:timestamp: %facility-severity-MNEMONIC:description

LEVEL	NUM.	DESCRIPTION	DEFINITION
Emergency	0	System unstable	LOG_EMERG
Alert	1	Immediate action needed	LOG_ALERT
Critical	2	Critical conditions	LOG_CRIT
Error	3	Error conditions	LOG_ERR
Warning	4	Warning conditions	LOG_WARNING
Notification	5	Normal but significant conditions	LOG_NOTICE
Informational	6	Informational message only	LOG_INFO
Debugging	7	Debugging messages	LOG_DEBUG

https://ipcisco.com/lesson/syslog-server/

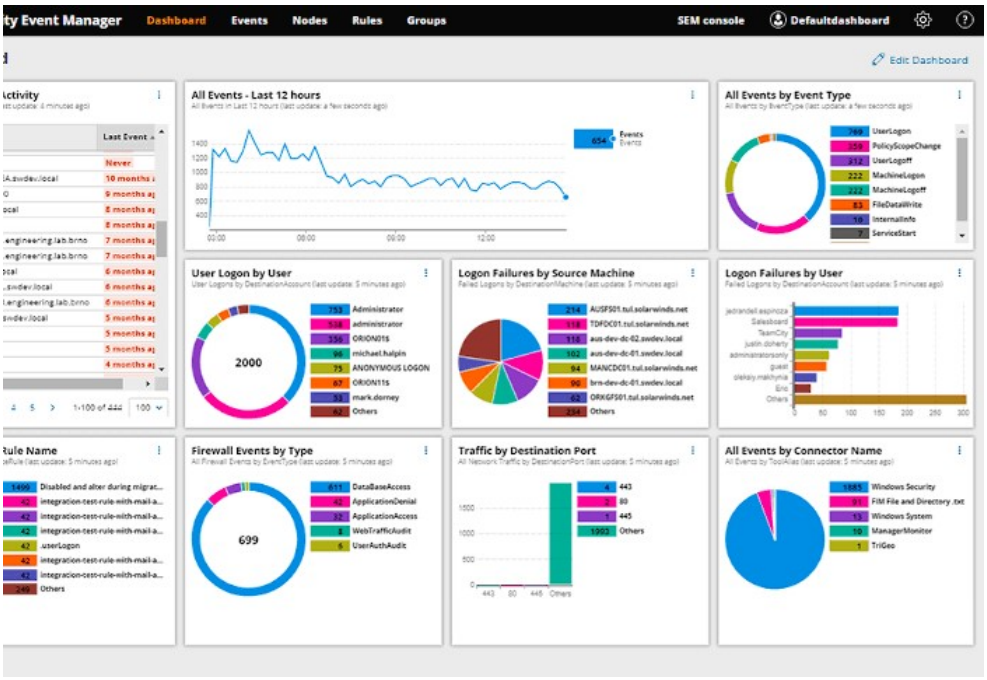
Le format standard syslog utilise une syntaxe définie pour la transmission de ces informations de journaux d'événements. Les différentes implémentations de syslog peuvent inclure des informations supplémentaires en fonction des besoins de l'application ou du systèm

Ces niveaux permettent d'indiquer tous les messages critiques pour le système, en plus des messages système normaux. L'importance de ces logs est numérotée à partir de 0. Le niveau 0 correspond au log le plus important : **Emergency**. Après le niveau Emergency, les sept autres niveaux suivent un ordre décroissant d'importance. Le log le moins important est **Debug**, correspondant au niveau 7.e.

4. Introduction aux SIEM

Objectifs d'un SIEM ?

- détecter les menaces le plus rapidement possible
- fournir des rapports sur les incidents et événements liés à la sécurité, tels que les connexions réussies ou non, et les activités malveillantes
- envoyer des alertes si l'analyse montre qu'une activité va à l'encontre des règles prédéterminées -et indique donc un problème de sécurité potentiel.



26

Les acronymes SEM, SIM et SIEM ont parfois été utilisés de manière interchangeable. SEM, gestion des évènements de sécurité, s'occupe de la surveillance en temps réél, de la corrélation des événements, des notifications et des vues de la console. SIM, gestion des informations de sécurité, assure le stockage à long terme ainsi que l'analyse, la manipulation et la communication des données des logs et des enregistrements de sécurité du type rassemblé par le logiciel SEM.

Les entreprises se tournent vers les grandes plates-formes de données, comme Apache Hadoop, pour compléter les capacités SIEM en étendant la capacité de stockage de données et la flexibilité analytique. La nécessité d'une visibilité centrée sur la voix ou vSIEM (information de sécurité vocale et gestion d'événements) fournit un exemple récent de cette évolution.

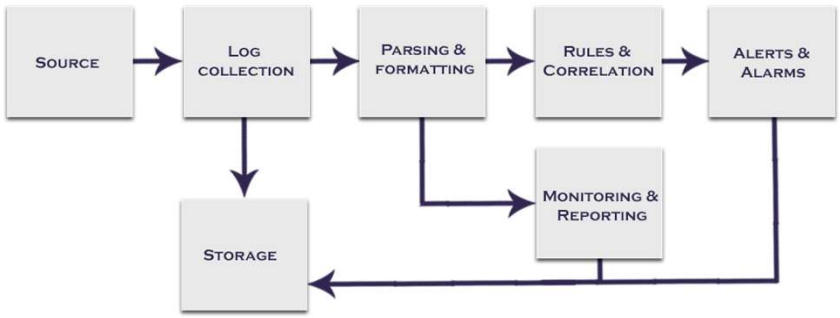
Depuis l'invention du terme SIEM en 2005 par Mark Nicolett et Amrit Williams de Gartner, il désigne :

- les capacités de collecte, d'analyse et de présentation de l'information provenant du réseau et des dispositifs de sécurité.
- les applications de gestion des identités et des accès
- les outils de gestion des vulnérabilités et de conformité aux politiques
- le système d'exploitation, la base de données et les journaux d'application
- les données sur les menaces externes

Processus de gestion des événements

Principales fonctions de traitement :

- La collecte et l'agrégation des données d'une multitude de sources
- La corrélation des évènements
- Le reporting des évènements
- La rétention des données



27

L'agrégation de données est un processus de regroupement de données provenant de différentes sources pour former une vue cohérente et globale. Cela permet de combiner les données pour en faire une analyse plus complète et plus précise. Les données peuvent être agrégées à différents niveaux de détail, en fonction des objectifs de l'analyse.

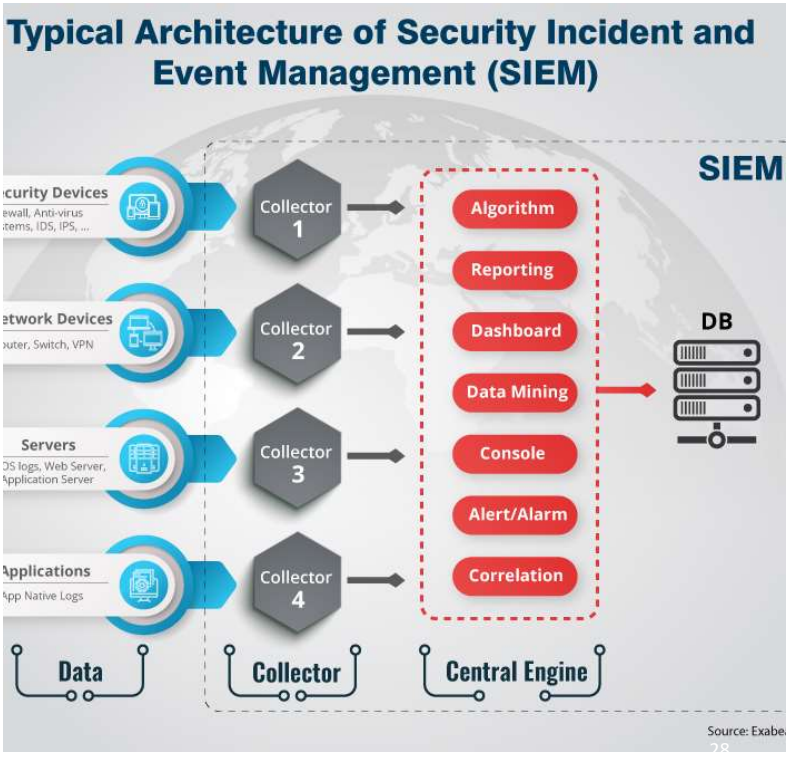
La corrélation d'événements est un processus qui consiste à analyser les relations entre plusieurs événements enregistrés afin d'identifier des modèles, des tendances et des anomalies qui pourraient ne pas être visibles en examinant chaque événement individuellement. En comparant les événements entre eux, il est possible de déterminer les relations causales entre eux et de déterminer les événements qui se produisent en réponse à d'autres événements.

Le reporting d'événements consiste à produire des rapports décrivant les événements enregistrés par un système de surveillance ou de gestion de la sécurité. Les rapports peuvent inclure des informations sur la nature, la fréquence et la gravité des événements, ainsi que des données démographiques, géographiques et temporelles.

La rétention des données est le processus de conservation des données pour une période spécifiée de temps. Cela permet de conserver les données pour une analyse ultérieure, pour une utilisation en cas de litige ou pour respecter les obligations réglementaires et juridiques.

Architecture typique d'un SIEM

- Données collectées par des agents depuis les composants du système
- Envoi des données (syslog) vers un serveur d'analyse et de corrélation
- Stockage des données dans un BD
- Reporting et tableaux de bord au travers d'un interface web



Une architecture SIEM typique comporte les composants suivants:

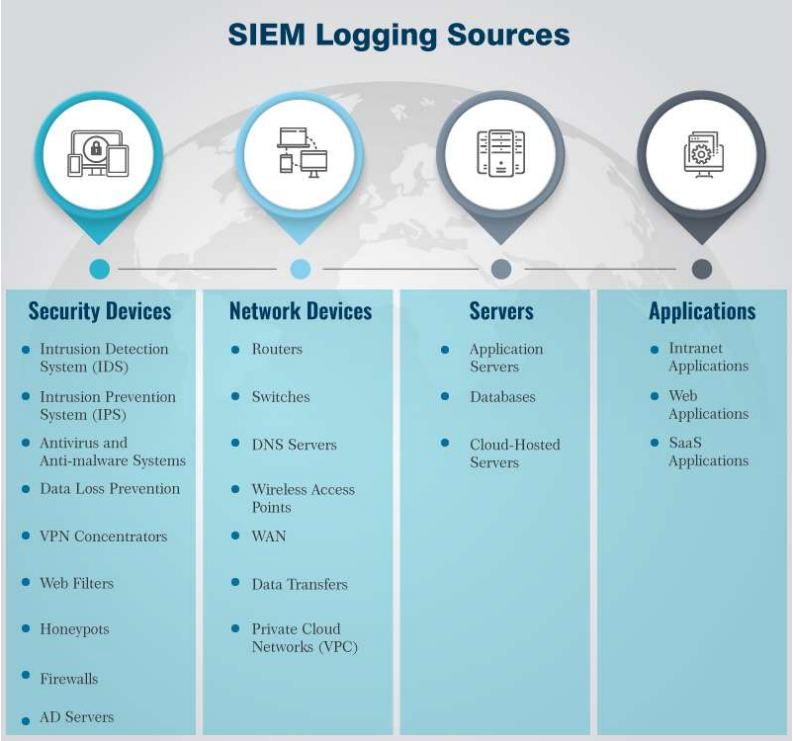
• Collecteur de données: pour la réception, l'enregistrement et l'agrégation des événements provenant de différentes sources.
• Corrélateur: pour l'analyse des événements et la détermination des alertes en fonction des règles de corrélation définies.
• Console d'administration: pour la gestion et la configuration du système.
• Module de rapport: pour la production de rapports sur les événements et les alertes.
• Stockage de données: pour la conservation des événements et des données de rapport.

Inventaire des Sources de données

Categories des sources de données :

- Security devices
- Network devices
- Servers
- Applications

https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/



L'inventaire est une liste complète de tous les systèmes, équipements et applications qui génèrent des journaux ou des événements pour la collecte et l'analyse dans un SIEM.

La première étape consiste à lister l'ensemble des équipements qui constitue les sources des évènements ou logs. Sources qui seront de plus en plus nombreuses, car selon le SANS Institute, une nouvelle génération de SIEM, appelés « SIEM v2 » se concentre sur la collecte la plus vaste possible d'informations, ne se basant plus uniquement sur des informations issues des syslogs, mais aussi netflow ou SNMP par exemple.
Cette volonté d'étendre à l'infini la collecte d'informations est sans doute tout autant liée à la baisse des coûts de stockage et de temps-machine (CPU) qu'à l'optimisation du fonctionnement des bases de données et autres moteurs internes des SIEM.

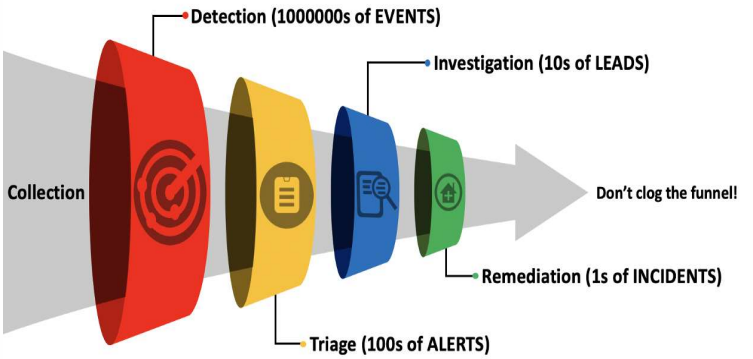
Il est donc nécessaire de mettre tout d'abord en œuvre une méthode d'analyse structurée, de la définition des informations à collecter jusqu'à l'élaboration des tableaux de bord finaux.

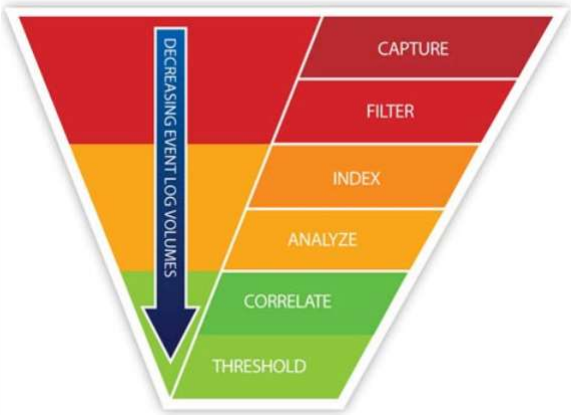
À titre d'exemple encore, pour un routeur Cisco dont la fonction est de simplement aiguiller le trafic, il y aura peu d'événements à collecter. À l'inverse, une passerelle Internet, proposant de multiples fonctions comme un pare-feu, un composant de filtrage d'URL ou un antivirus, produira en comparaison une multitude de fichiers de journalisation et donc d'évènements à collecter.
De plus, les équipements évoluent constamment ainsi que les logs générés. Il est donc nécessaire d'analyser cette évolution des logs afin d'accroitre les évènements considérés comme pertinents pour la sécurité (cas de journaux Windows ou de sondes IDS).

Etapes de traitement des données

Traversée des données dans un « entonnoir » (Logs Funnel) :

des milliers de logs collectés sont triés, analysés, comparés, regroupés pour identifier (peut-être) quelques « vrais » incidents.





https://posts.specterops.io/introducing-the-funnel-of-fidelity-b1bb59b04036

L'approche en « Tunnel » décrit le processus d'application de différentes procédures analytiques pour gérer des millions d'événements contextuels et appliquer des ressources d'enquête limitées aux événements ou situations les plus susceptibles d'être malveillants. Le tunnel comporte 5 étapes : la collecte, la détection, le triage, l'investigation et la remédiation.

Chaque étape prend en entrée ce qui a été généré à l'étape précédente, effectue une sorte de filtrage ou de réduction de bruit et produit une sortie pour l'étape suivante. Idéalement, chaque étape permet une analyse plus profonde ou plus manuelle de l'événement en question car les événements non pertinents ont été filtrés.

Corrélation des événements

La corrélation permet de

- relier différents évènements entre eux, provenant de différentes sources de données

afin

- d'identifier un comportement dangereux ou une faille de sécurité dans le système,
- de déclencher une alerte pour stopper l'attaque et implementer une correction.

en suivant des règles prédéfinies.

Important : pour développer des règles de corrélation qui vont déclencher des alertes, il faut avoir la connaissance du comportement indésirable que l'on essaie de découvrir.

https://digitalguardian.com/blog/what-event-correlation-examples-benefits-and-more

Les règles de corrélation sont des algorithmes ou des conditions qui permettent de relier ou de lier des événements informatiques entre eux. Elles sont utilisées pour identifier les anomalies, les comportements suspects ou les incidents de sécurité à partir de logs, d'alertes ou d'autres sources de données d'événements. Les règles de corrélation peuvent être basées sur des critères tels que la source, la destination, le temps, la fréquence, etc. et peuvent être utilisées pour déterminer la gravité d'un événement et pour prendre des mesures en conséquence.

Le développement efficace de règles de corrélation nécessite une compréhension approfondie des comportements indésirables que l'on cherche à détecter. Si la connaissance du comportement indésirable est insuffisante ou incorrecte, les règles de corrélation peuvent ne pas détecter correctement les incidents ou générer des alertes faussement positives. De plus, sans une compréhension complète du comportement indésirable, il peut être difficile de déterminer les critères corrects pour définir les règles de corrélation et de s'assurer de leur efficacité.

Exemple de règle de corrélation

Cas d'usage (Use Case) d'une détection d'exfiltration de données (Data Exfiltration Detection)

Un utilisateur se connecte avec un compte administrateur sur un serveur protégé et transfère une grande quantité de données (via un fichier zip) sur une clé USB.

1. Quels événements et données avons-nous besoin pour détecter cet incident ?

- Evénement/log 1 → Données 1
- Evénement/log 2 → Données 2
- …

2. Quels tests pourrait-on effectuer pour confirmer l'incident ?

- Test 1
- Test 2
- Test 3
- …

3. Quelles règles pourrions-nous créer sur base de ces éléments pour signaler une alarme ?

- Déclencher l'alarme quand <condition 1> et <condition 2> et < …> sont réunies

Use case : Un utilisateur disposant de privilèges élevés (compte administrateur) accède à un serveur sensible. Il copie un grand volume de données en les compressant dans une archive (ex. fichier .zip), puis les transfère vers un support amovible (clé USB).

Objectif du Use Case

Détecter en temps réel un comportement anormal pouvant indiquer une tentative d'exfiltration de données et fournir des alertes exploitables pour investigation et réaction rapide.

Principaux SIEM selon Gartner

Rapport « Magic Quadrant » 2024 sur les différents SIEM disponibles

QRadar SIEM
by IBM

Azure Sentinel
by Microsoft

Splunk Enterprise
by Splunk

Exabeam Security Management Platform
by Exabeam

Securonix Next-Gen SIEM
by Securonix

https://www.gartner.com/doc/reprints?id=1-2F6JB0XP&ct=231002&st=sb

https://fr.wikipedia.org/wiki/Gartner

Gartner Inc. est une entreprise américaine de conseil et de recherche dans le domaine des techniques avancées.

Gartner publie des résultats comparatifs de sociétés, solutions ou de produits sous la forme de nuage de points dans un « quadrant magique » (« magic quadrant »), se présentant comme un graphe à deux dimensions. L'axe horizontal mesure la « complétude de la vision », et l'axe vertical mesure la « capacité à exécuter », ce qui répartit les points dans quatre quadrants : acteurs de niche (« niche players »), « visionnaires », « challengers » et « leaders ».

En 2024, plusieurs fusions ont été annoncées : Splunk a été racheté par CISCO et Exabeam a fusionné avec LogRhythm.

— IBM Qradar

Version gratuite pour l'apprentissage : Qradar Community Edition

Une version gratuite d'IBM QRadar SIEM est disponible. Cette édition, appelée "Community" contient toutes les caractéristiques de QRadar SIEM et nécessite peu de mémoire (fonctionne avec seulement 8 ou 10 Go) par rapport à l'au moins 24G requis pour un environnement de version commerciale minimum.

Il comprend également une licence qui n'expire pas et vous permet d'installer toutes sortes de plugins et d'applications. L'objectif est son utilisation privée pour l'apprentissage, les démos, les tests et fondamentalement, le développement d'applications compatibles avec QRadar. C'est pourquoi ses capacités sont limitées à la gestion de 50 événements (journaux) par seconde et de 5 000 paquets réseau par minute.

Cette version sera utilisée dans les labos. A télécharger sur https://developer.ibm.com/qradar/ce/.

Note : en 2025, Qradar va intégrer l'offre d'automatisation des événements de sécurité pour SOC de Palo Alto Networks.

— Importance du SIEM dans un SOC

Le SIEM est l'outil principal du SOC, en lien avec toutes les équipes contrôlant la sécurité de l'organisation

https://pei.com/siem-soc-security-benefits/

https://fr.wikipedia.org/wiki/Security_Operations_Center

Le SOC est le centre d'opérations et de sécurité de l'information. C'est une plateforme où les systèmes d'information de l'entreprise sont surveillés, évalués et défendus.

Le SIEM (Security Information Event Management) est l'outil principal du SOC, mais le SOC a un périmètre beaucoup plus large : le SOC est lié aux personnes, aux processus et aux technologies utilisées pour s'assurer de la connaissance de la situation grâce à la détection, au confinement et à l'assainissement des menaces informatiques.

Petit quizz

1. Quel est le type d'événement qui signale une situation anormale qui affecte la disponibilité, la performance ou la qualité des services informatiques?

   a) événement de type "information"
   b) événement de type "warning"
   c) événement de type "exception »
   d) aucun de ces choix

2. Quels sont les avantages de centraliser les logs?

   a) Archivage à long terme
   b) Meilleure protection des informations sensibles
   c) Réduction de la quantité de données à gérer sur chaque équipement individuel
   d) Toutes les réponses ci-dessus

MERCI