

Technologies de l'information

Cours:

**Sécurité des systèmes
informatiques**

Séance # 10

Préparé par: Blaise Arbouet



DESS

Contenu de la séance

Surveillance et
journalisation de la
sécurité

Opérations de sécurité
et réponse aux
incidents

Qu'est-ce que la journalisation et la surveillance de la sécurité ?

La journalisation et la surveillance des événements de sécurité font partie intégrante d'un processus unique, essentiel au maintien d'une infrastructure sécurisée.

Chaque activité sur votre environnement, des e-mails aux connexions en passant par les mises à jour du pare-feu, est considérée comme un événement de sécurité. Tous ces événements sont (ou devraient être) journalisés afin de garder un œil sur tout ce qui se passe dans votre environnement technologique.

Pour surveiller ces journaux, les organisations examinent les fichiers journaux d'audit contenant des informations confidentielles à la recherche de signes d'activités malveillantes ou non autorisées.

Événement vs alerte vs incident



Événement : un événement désigne tout changement ou événement observable au sein d'un système, qu'il soit routinier, informatif ou révélateur de problèmes. Tous les appareils technologiques créent des événements sous forme d'entrées de journal et de mises à jour d'état régulières, enregistrées comme données d'événement dans diverses bases de données et autres fichiers.



Alerte : une alerte est une notification déclenchée par un événement et conçue pour informer les parties prenantes d'une situation nécessitant leur attention.



Incident : un incident est un type spécifique d'événement négatif qui perturbe les opérations ou les services normaux et nécessite une intervention.

Importance de la journalisation

Les journaux dans un environnement réseau sont générés et mis à jour en permanence. Il est essentiel de consulter et d'analyser régulièrement ces journaux pour rester au courant de vos opérations, de votre sécurité et de votre conformité. Un examen et une analyse réguliers des journaux peuvent aider à identifier les problèmes au plus tôt, à comprendre les tendances et à prendre des décisions éclairées.



Bonnes pratiques de journalisation

- Centralisation des logs
- Protection contre la falsification
- Définition de la politique de rétention
- Format standardisé (JSON, CEF, LEEF)
- Timestamp synchronisé (NTP)

Surveillance des journaux

La surveillance des journaux est le processus de collecte, d'analyse et d'exploitation des données de journaux provenant de diverses sources. Cela peut inclure les applications et l'infrastructure (calcul, réseau et stockage). Lorsque les développeurs et les équipes opérationnelles surveillent les journaux, ils le font pour détecter les anomalies et les problèmes au sein d'un système afin de pouvoir les résoudre aussi efficacement que possible.

Cloud Monitoring Use Cases





Importance de la surveillance

- Alertes pour une détection plus rapide des menaces
 - Reconstruction d'événements
 - Identification rapide des problèmes système ou applicatif
 - Récupération plus rapide après un événement
 - Données essentielles pour la conformité
 - Détection des menaces 24h/24 et 7j/7
 - Etc
-

Types de journaux (logs)



Journaux du serveur Web



Journaux du réseau



Journaux des applications



Journaux des conteneurs



Journaux système



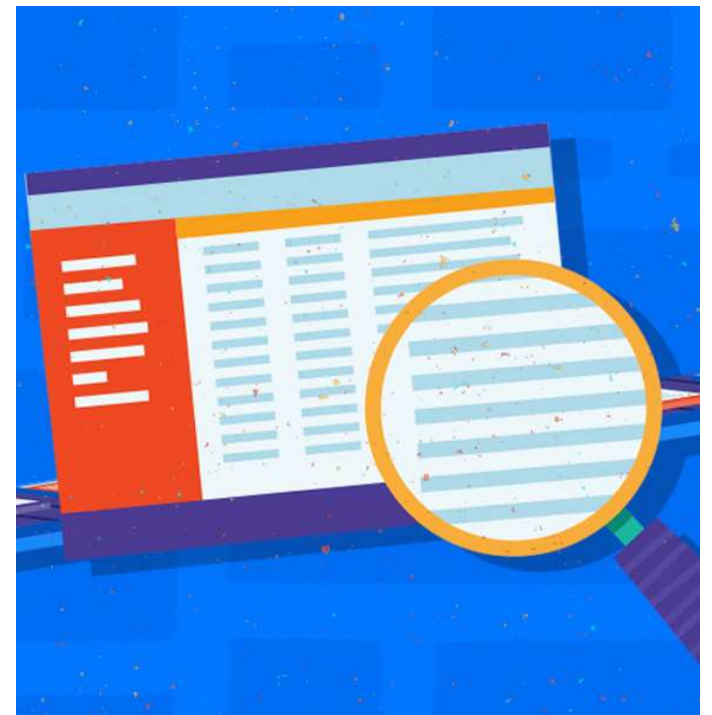
Journaux de sécurité



etc..

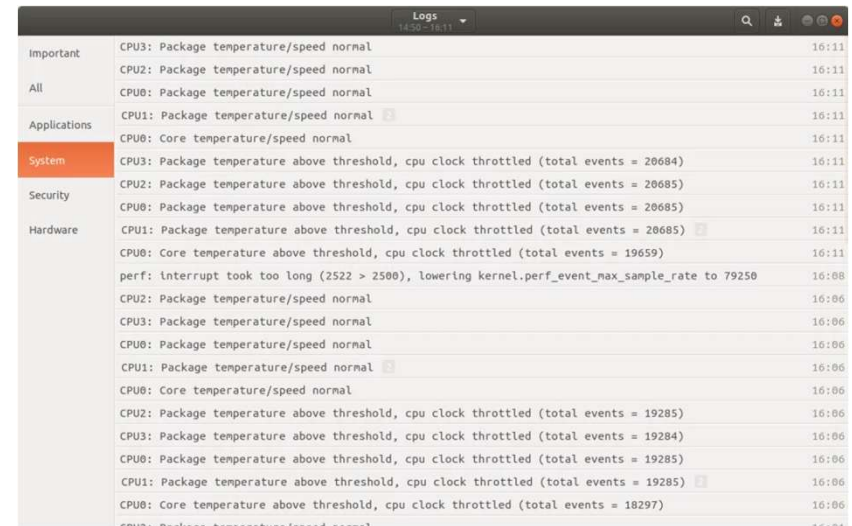
Journaux d'application

Les fichiers journaux d'application sont des enregistrements des activités enregistrées par les applications logicielles. Vous pouvez les utiliser pour le dépannage, le diagnostic et l'audit. Ils vous fournissent une multitude d'informations sur les performances d'une application, par exemple les avertissements relatifs à l'espace disque, les opérations terminées, les problèmes qui empêchent l'application de démarrer, l'audit des connexions réussies et l'audit des échecs de connexion.



Journaux système

Les fichiers journaux système, également appelés « journaux du serveur », incluent des journaux d'informations détaillés sur le système d'exploitation, le système de fichiers, les applications en cours d'exécution et les identifiants de connexion. Ils permettent aux administrateurs de déterminer si les processus système se chargent correctement ou s'il existe des problèmes, tels que des erreurs système, des avertissements, des messages de démarrage, des modifications du système, des arrêts inattendus, etc.



Logs		
Important	CPU3: Package temperature/speed normal	16:11
	CPU2: Package temperature/speed normal	16:11
All	CPU0: Package temperature/speed normal	16:11
Applications	CPU1: Package temperature/speed normal	16:11
	CPU0: Core temperature/speed normal	16:11
System	CPU3: Package temperature above threshold, cpu clock throttled (total events = 20684)	16:11
	CPU2: Package temperature above threshold, cpu clock throttled (total events = 20685)	16:11
Security	CPU0: Package temperature above threshold, cpu clock throttled (total events = 20685)	16:11
	CPU1: Package temperature above threshold, cpu clock throttled (total events = 20685)	16:11
Hardware	CPU0: Core temperature above threshold, cpu clock throttled (total events = 19659)	16:11
	perf: interrupt took too long (2522 > 2500), lowering kernel.perf_event_max_sample_rate to 79250	16:08
	CPU2: Package temperature/speed normal	16:06
	CPU3: Package temperature/speed normal	16:06
	CPU0: Package temperature/speed normal	16:06
	CPU1: Package temperature/speed normal	16:06
	CPU0: Core temperature/speed normal	16:06
	CPU2: Package temperature above threshold, cpu clock throttled (total events = 19285)	16:06
	CPU3: Package temperature above threshold, cpu clock throttled (total events = 19284)	16:06
	CPU0: Package temperature above threshold, cpu clock throttled (total events = 19285)	16:06
	CPU1: Package temperature above threshold, cpu clock throttled (total events = 19285)	16:06
	CPU0: Core temperature above threshold, cpu clock throttled (total events = 18297)	16:06
	CPU3: Package temperature/speed normal	16:06

Journaux de sécurité



De nombreux appareils conservent des données de journal de sécurité qui vous permettent de voir quels types de trafic réseau sont autorisés ou refusés sur votre réseau. Par exemple, les journaux d'audit et les contrôles d'accès peuvent aider à identifier les utilisateurs suspects qui abusent de leurs privilèges d'accès. Et éventuellement à prévenir une attaque par force brute potentielle.



Un autre exemple est celui des fichiers journaux d'authentification qui capturent les tentatives des utilisateurs d'accéder à une ressource réseau. Cela permet de déboguer les problèmes d'accès et de modifier les politiques d'authentification. Il enregistre également les événements de sécurité de haut niveau à des fins d'audit.



Les journaux de sécurité sont souvent un sous-ensemble de journaux système enregistrant des événements spécifiques à la sécurité et à la sûreté de votre infrastructure informatique.

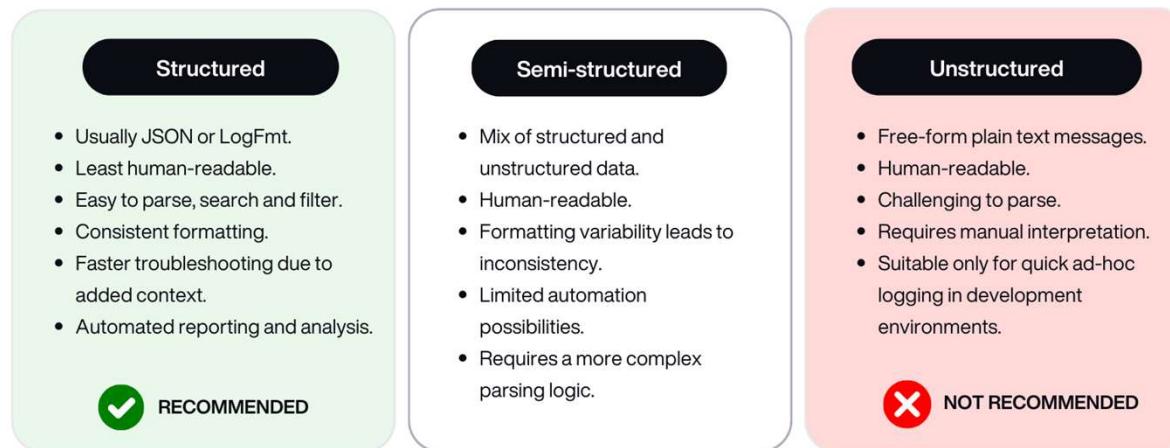
Formatage de journaux

Le formatage des journaux joue un rôle important dans la capture et l'organisation de divers détails d'événements d'application. Il englobe des préoccupations telles que :

- Structurer chaque entrée de journal pour plus de clarté et de cohérence,
- Choisir la méthode de codage des journaux,
- Inclure et organiser de manière stratégique les champs contextuels dans les journaux,
- Définir la manière dont les enregistrements de journal individuels sont séparés ou délimités.

Ex de formatage de journaux

Log Formats Explained



Que préferiez-vous?

```
1687927940843: Starting application on port 3000  
Encountered an unexpected error while backing up the database  
[2023-06-28T04:49:48.113Z]: Device XYZ123 went offline
```

```
2023-06-28 19:09:48.801818 I [969609:60] MyApp -- Starting application on port  
3000  
2023-06-28 19:09:48.801844 I [969609:60] MyApp -- Device XYZ123 went offline  
2023-06-28 19:09:48.801851 E [969609:60 main.rb:13] MyApp -- Service "ABCDE"  
stopped unexpectedly. Restarting the service
```

```
{  
  "host": "fedora",  
  "application": "Semantic Logger",  
  "timestamp": "2023-06-28T17:20:19.409882Z",  
  "level": "info",  
  "level_index": 2,  
  "pid": 982617,  
  "thread": "60",  
  "name": "MyApp",  
  "message": "Starting application on port 3000"  
}
```

Outil de journalisation et de surveillance (SIEM)

La gestion des informations et des événements de sécurité (SIEM) est une solution qui aide les organisations à détecter, analyser et contrer les menaces de sécurité avant qu'elles ne nuisent à leurs opérations.

Le SIEM, prononcé « sim », combine la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM) au sein d'un seul système de gestion de la sécurité. La technologie SIEM collecte les données des journaux d'événements provenant de diverses sources, identifie les activités anormales grâce à une analyse en temps réel et prend les mesures appropriées (correlation).

Cas d'utilisation d'un SIEM

Escalade de
privilèges

Tentatives de
connexion par
brute force

Suppression de
journaux

Exfiltration de
données

Utilisation
inhabituelle des
droits
administrateurs










Courriel
d'hameçonnage

Téléchargement
de maliciels

Etc..

10 Best Free and Open-Source SIEM Tools

What You Need to Know

OSSIM		Offers both server-agent and serverless modes, with log analysis for mail servers, databases, and more.
Sagan		Real-time log analysis and correlation tool that's compatible with graphic consoles like Snorby and EveBox.
Splunk Free		Free version of Splunk tool that lets you index up to 500 MB daily for real-time data indexing and alerts.
Snort		Analyzes network traffic in real time, but features make it best-suited for experienced IT professionals.
Elasticsearch		Combine log search types and easily scan through large volumes of logs with this basic tool.
MozDef		A microservices-based tool that can integrate with third-party platforms for straightforward security insights.
ELK Stack		Combines Elasticsearch with tools like Kibana, Beats, and Logstash, for a fuller SIEM solution.
Wazuh		An on-premises tool that offers threat detection, incident response, and compliance support.
Apache Metron		Combines security operations center functions into one centralized, dynamic tool for catching threats.

2024 GARTNER® MAGIC QUADRANT SIEM



Pratiquer Splunk

<https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchTutorial/Systemrequirements>

Voir aussi vidéo d'installation



Réponse aux incidents

La réponse aux incidents (parfois appelée réponse aux incidents de cybersécurité) désigne les processus et technologies d'une organisation permettant de détecter et de répondre aux cybermenaces, aux failles de sécurité ou aux cyberattaques. Un plan formel de réponse aux incidents permet aux équipes de cybersécurité de limiter ou de prévenir les dommages.

L'objectif de la réponse aux incidents est de prévenir les cyberattaques avant qu'elles ne se produisent et de minimiser les coûts et les perturbations opérationnelles qui en résultent. La réponse aux incidents est la partie technique de la gestion des incidents, qui comprend également la gestion des incidents graves (crise) par la direction, les RH et le service juridique.

Qu'est-ce qu'un incident de sécurité ?

Un incident de sécurité, ou événement de sécurité, désigne toute violation numérique ou physique menaçant la confidentialité, l'intégrité ou la disponibilité des systèmes d'information ou des données sensibles d'une organisation. Les incidents de sécurité peuvent aller des cyberattaques intentionnelles par des pirates informatiques ou des utilisateurs non autorisés aux violations involontaires de la politique de sécurité informatique par des utilisateurs légitimes et autorisés.

Incidents de sécurité les plus courants

Rançongiciels

Phishing et ingénierie sociale

Attaques DDoS

Attaques de la chaîne
d'approvisionnement

Menaces internes

Attaques par élévation de privilèges

Attaques de l'homme du milieu

Etc...



Les référentiels en réponse aux incidents les plus connus



CSA Cloud Incident Response (CIR) Framework



NIST Computer Security Incident Handling Guide (NIST SP800-61 Rev. 2)



CSA incident response research hub



ISO/IEC 27035



ENISA Strategies for incident response and cyber crisis cooperation

Cycle de vie de réponse aux incidents (NIST 800-61 rev 2)



Based on NIST 800-61rev2 (Post Incident Analysis replaces Post Mortem)

Figure 29: Phases of IR Life Cycle in Cloud Security

Étape 1: Préparation

- Établir un processus de réponse aux incidents
- Constituer une équipe et attribuer des rôles et des responsabilités
- Former l'équipe et exécuter des exercices
- Établir un plan et des installations de communication
- Accès des intervenants aux environnements
- Accès des intervenants aux outils : services d'analyse des incidents, matériel et logiciel
- Documentation interne (par exemple, listes de ports, listes d'actifs, base de référence du trafic réseau)
- Évaluer l'infrastructure : analyse et surveillance proactives, évaluation de la vulnérabilité et des risques
- S'abonner à des services de renseignement sur les menaces tiers
- Évaluer les CSP et leurs capacités à contribuer à la réponse aux incidents concernant les services/ressources consommés
- Effectuer régulièrement des tests de restauration de sauvegarde et des tests de reprise après sinistre (DR) au moins une fois par an pour garantir que les plans de réponse aux incidents sont à jour et efficaces

Étape 2: Détection & Analyse

- Ingénierie de détection
- Alertes : cela inclut la gestion de la posture de sécurité du cloud (CSPM), la gestion des informations et des événements de sécurité (SIEM), la protection de la charge de travail et la surveillance de la sécurité du réseau.
- Valider les alertes (réduire les faux positifs), avec escalade.
- Estimer la portée de l'incident.
- Affecter un responsable des incidents pour coordonner les actions.
- Établir une chronologie de l'attaque.
- Déterminer l'étendue de la perte de données ou de l'impact potentiel.
- Notifier et coordonner les activités.
- Communiquer l'état de confinement et de récupération de l'incident à la haute direction.

Etape 3: Confinement, éradication et rétablissement



Confinement : isoler les identités et les charges de travail, mettre les systèmes ou les services hors ligne et tenir compte des compromis entre la perte de données et la disponibilité des services.



Éradication et récupération : nettoyer les actifs compromis et restaurer les systèmes et les services à leur fonctionnement normal. Déployer des contrôles pour éviter des incidents similaires.




Documenter l'incident et rassembler des preuves médico-légales (par exemple, la chaîne de traçabilité).

Étape 4: Analyse post-incident

Leçons apprises :

- Quelles détections ont fonctionné et quelles alertes se sont déclenchées correctement ?
- Quelles détections et protections doivent être créées en fonction de l'événement ?
- Quelles améliorations le processus de réponse aux incidents doit-il apporter ?
- Quels indicateurs de compromission (IOC) ont été découverts et ont-ils été partagés avec la communauté ?

De nombreux incidents peuvent concerner les infrastructures et les appareils cloud et traditionnels, ce qui oblige les intervenants à s'assurer qu'ils ne développent pas une vision tunnel et ne s'intéressent qu'à une seule facette d'un incident.



Tester votre processus de réponse aux incidents

TableTop Exercise

L'exercice TableTop est une réunion pour discuter d'une situation d'urgence simulée. Le personnel de l'organisation examine et discute des mesures qu'il prendrait dans une situation d'urgence particulière, testant leur plan d'urgence dans un environnement informel et peu stressant. Les exercices TableTop sont utilisés pour clarifier les rôles et les responsabilités et pour identifier les besoins supplémentaires d'atténuation et de préparation. L'exercice devrait aboutir à des plans d'action pour une amélioration continue du plan d'urgence.

Scénarios de TableTop

Exemple de scénario n°1 : un employé découvre un faux lecteur attaché à une carte d'accès lors d'une inspection matinale.

Exemple de scénario n°2 : une analyse des journaux montre une augmentation inhabituelle du trafic réseau.

Exemple de scénario n°3 : votre banque acquéreuse vous appelle pour vous informer d'une violation présumée.

Exemple de scénario n°4 : les employés reçoivent un e-mail de phishing ciblé qui compromet leurs identifiants de connexion.

Exemple de scénario n°5 : un employé mécontent sabote les systèmes de l'entreprise ou divulgue des informations confidentielles.

Outils pour le DFIR

Memoire: <https://github.com/digitalisx/awesome-memory-forensics?tab=readme-ov-file> (Belkasoft RAM Capturer)

Disque: <https://www.easeus.com/backup-recovery/forensic-imaging-tool.html> (EaseUS)

<https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81>(FTK Imager)

Autres outils: <https://github.com/Cugu/awesome-forensics>

Analyse d'image de disque: Autopsy
(<https://www.autopsy.com/download/>)

Pratique d'analyse d'image disque

Se référer au lien:

<https://www.hackercoolmagazine.com/digital-forensics-with-autopsy-part-1/>



Pratique de scénario TableTop

Le site web de votre compagnie s'est fait défiguré par un acteur malveillant. Comment allez-vous répondre à cet incident:

Etapas recommandées:

Questions à se poser:

- Processus testé(s):
- Acteur de la menace:
- Actif impacté:
- Contrôle à mettre en place:

Références

- <https://www.vaadata.com/blog/logging-monitoring-definitions-and-best-practices/>
- <https://middleware.io/blog/what-is-log-monitoring/>
- <https://www.bigpanda.io/blog/decode-events-alerts-incidents/>
- <https://www.microsoft.com/en-ca/security/business/security-101/what-is-siem>
- <https://iritt.medium.com/setting-up-splunk-universal-forwarder-on-windows-10-for-your-cybersecurity-home-lab-1094e375ebf1>
- https://mihaillazarov.com/blog/splunk_vb_image/
- https://medium.com/@black_Diamond/splunk-a-comprehensive-siem-tool-d3352b9c4888