Top 16

Cyberattaques détectées par SIEM Solutions

https://www.linkedin.com/in/harunseker/

TOP 16 des Cyberattaques détectées par SIEM Solutions

1. Attaques de phishing

2. Requêtes DNS suspectes/malveillantes

3. Détections de logiciels malveillants/fichiers malveillants (AV, EPP, EDR, XDR)

4. Attaques d'applications Web (OWASP Top 10, SQLi, File Upload)

5. Communications suspectes avec des adresses IP et URL externes (commande et contrôle, réseaux Botnet/Zombie)

6. Activités Powershell suspectes

7. Alarmes de force brute

8. Détections d'activités suspectes/malveillantes depuis l'intranet (Enterprise Network)

9. Transferts de fichiers suspects (contenu sensible, grande taille, etc.)

10. Activités de connexion suspectes (activité de voyage impossible, heures non travaillées, etc.)

11. Rançongiciel

12. Réseaux de zombies

13. Menace persistante avancée

14. Comptes compromis

15. Exfiltration de données

16. DoS / DDoS – Déni de service

https://www.linkedin.com/in/harunseker/

1- Ingénierie sociale / Attaques de phishing

Ce que c'est	Le phishing est un type d'ingénierie sociale dans lequel un attaquant envoie un message frauduleux conçu pour inciter une personne à révéler des informations sensibles à l'attaquant ou à déployer des logiciels malveillants sur l'infrastructure de la victime comme un ransomware.
Indicateurs de menace	● Artefacts d'e-mails suspects tels que l'expéditeur, l'objet et le message suspects. ● Lien URL suspect ● Attachement suspect
Où enquêter	Journaux proxy, journaux DNS, journaux EDR/XDR
Actions possibles	Bloquer les adresses IP et les URL Bloquer l'adresse e-mail de l'expéditeur Mettre régulièrement à jour les logiciels, mettre en œuvre une authentification forte, former les employés

2- Requêtes DNS suspectes/malveillantes

Ce que c'est	Les requêtes DNS suspectes ou malveillantes sont des requêtes adressées au système de noms de domaine (DNS) destinées à se connecter à des domaines associés à des activités malveillantes, tels que des serveurs de commande et de contrôle de logiciels malveillants, des sites de phishing ou des domaines impliqués dans les données. exfiltration. Ces requêtes peuvent indiquer un système compromis au sein d'un réseau ou tentatives de violer la sécurité d'un réseau
Indicateurs de menace	● Volume élevé de requêtes ● Requêtes pour les domaines malveillants connus ● Modèles de requêtes inhabituels (requêtes à des moments impairs)
Où enquêter	Journaux DNS Outils de sécurité des points finaux Analyse du trafic réseau Plateformes de renseignements sur les menaces
Actions possibles	Surveillez et analysez le trafic DNS, mettez en œuvre le filtrage DNS, mettez régulièrement à jour les logiciels de sécurité, utilisez les renseignements sur les menaces, la segmentation du réseau et éduquez les utilisateurs.

3- Malwares / Détections de fichiers malveillants (AV, EDR, XDR)

Ce que c'est	Les logiciels malveillants, ou logiciels malveillants, font référence à tout programme ou fichier nuisible à un utilisateur d'ordinateur. La détection de fichiers malveillants est le processus d'identification et de neutralisation des logiciels malveillants à l'aide de divers outils de sécurité, tels que l'antivirus (AV), la détection des points de terminaison et Systèmes de réponse (EDR) et de détection et réponse étendues (XDR). Ces outils analysent pour détecter, détecter et répondre aux menaces en analysant les signatures, les comportements et les modèles de fichiers.
Indicateurs de menace	● Alertes de sécurité ● Comportement inattendu du système ● Activité de fichiers suspects ● Anomalies du réseau ● Accès utilisateur non autorisé
Où enquêter	Journaux des outils de sécurité EDR/XDR, journaux système et réseau, périphériques de point de terminaison et plates-formes de renseignement sur les menaces
Actions possibles	Mises à jour régulières, utilisation de solutions de sécurité complètes, formation des utilisateurs, mise en œuvre de contrôles d'accès, sauvegardes régulières et segmentation du réseau

https://www.linkedin.com/in/harunseker/

4 - Attaques d'applications Web

Ce que c'est	Une attaque d'application Web est une tentative d'acteurs malveillants d'exploiter les vulnérabilités et les faiblesses des applications Web ou des applications mobiles. Ces vulnérabilités peuvent survenir au cours du processus de développement en raison d'un codage incorrect, de serveurs Web mal configurés, d'applications défauts de conception ou échec de validation des formulaires. Les attaquants peuvent chercher à obtenir un accès non autorisé, obtenir des informations confidentielles, introduire du contenu malveillant ou modifier le contenu du site Web
Indicateurs de menace	● Comportement inattendu du système tel qu'un ralentissement des performances ou un crash ● Trafic réseau suspect ou connexions à des adresses IP malveillantes connues ● Modifications non autorisées des fichiers ou création de fichiers inconnus ● Alertes de sécurité des pare-feu d'applications Web (**WAF**s), systèmes de détection d'intrusion (IDS) ou autres solutions de sécurité indiquant les menaces détectées
Où enquêter	● Journaux des outils de sécurité**WAF**s, IDS et antivirus pour les alertes ● Journaux système et réseau ● Périphériques de point de terminaison ● Plateformes de renseignement sur les menaces
Actions possibles	Mises à jour régulières, utilisation de solutions de sécurité complètes, formation des utilisateurs, mise en œuvre de contrôles d'accès, sauvegardes régulières et segmentation du réseau

https://www.linkedin.com/in/harunseker/

5 - Communications suspectes avec des adresses IP et URL externes

(Commandement et contrôle, réseaux Botnet / Zombie)

Ce que c'est	Les communications suspectes avec des adresses IP et URL externes font référence à des activités réseau sur lesquelles les appareils au sein du réseau d'une organisation, initier ou recevoir des connexions inattendues ou non autorisées à ou à partir d'adresses IP et d'URL externes. Ces activités peuvent indiquer des menaces potentielles pour la sécurité, telles que les infections par des logiciels malveillants, les tentatives d'exfiltration de données, les communications de commande et de contrôle (C2) ou les attaques de phishing. La surveillance de ces communications est cruciale pour identifier et atténuer les menaces de cybersécurité
Indicateurs de menace	● Des volumes de trafic inhabituels ● Connexions à des adresses IP/URL malveillantes connues ● Irrégularités géographiques ● Des moments inhabituels ● Échecs répétés
Où enquêter	**Pare-feu et réseau**Journaux, systèmes de détection/prévention des intrusions (IDS/IPS), outils de détection et de réponse des points finaux (EDR) et de détection et de réponse étendues (XDR) et**Journaux de requêtes DNS**
Actions possibles	Mettre en œuvre la segmentation du réseau, utiliser les renseignements sur les menaces, déployer des solutions IDS/IPS et EDR/XDR,**Configurer le filtrage DNS**, appliquez des règles de pare-feu, mettez régulièrement à jour les solutions de sécurité, éduquez les utilisateurs et surveillez et analysez le trafic réseau.

https://www.linkedin.com/in/harunseker/

6 - Activités Powershell suspectes

Ce que c'est	Les activités PowerShell suspectes font référence à l'utilisation de PowerShell, un puissant langage de script et shell de ligne de commande fourni par Microsoft, d'une manière qui indique une intention malveillante. PowerShell est largement utilisé par les administrateurs système pour l'automatisation et tâches de gestion. Cependant, ses puissantes capacités en font également un outil attrayant pour attaquants pour exécuter des commandes, échapper à la détection, masquer les activités malveillantes, télécharger et exécuter des charges utiles et effectuer une reconnaissance au sein d'un système compromis
Indicateurs de menace	● Utilisation de commandes codées ● Contournement de la politique d'exécution ● Exécution de script inhabituelle ● Comportement anormal du processus PowerShell
Où enquêter	● Journaux PowerShell ● Journaux d'événements ● Systèmes de détection et de réponse des points finaux (EDR) et de gestion des informations et des événements de sécurité (SIEM) ● Solutions antivirus et antimalware
Actions possibles	Activez et configurez la journalisation PowerShell, implémentez les restrictions de politique d'exécution, utilisez la liste blanche des applications, formez les utilisateurs et les administrateurs, mettez régulièrement à jour et corrigez les systèmes et surveillez et analysez l'activité PowerShell.

7. Alarmes de force brute

Brute Forcing

What It Is	An attacker trying to guess a password by attempting several different passwords
Threat Indicators	Multiple login failures in a short period of time
Where to Investigate	Active Directory logs; Application logs; Operational System logs; Contact User
Possible Actions	If not legit action, disable the account and investigate/block attacker

8. Détections d'activités suspectes/malveillantes depuis l'intranet (Enterprise Network)

Ce que c'est	La détection d'activités suspectes ou malveillantes fait référence au processus d'identification et de réponse actions susceptibles de compromettre la sécurité et l'intégrité d'un réseau ou d'un système. Ceci comprend détecter les infections par des logiciels malveillants, les accès non autorisés, les violations de données et autres incidents de sécurité cela pourrait conduire à un préjudice potentiel ou à une exploitation.
Indicateurs de menace	● Modèles ou volumes de trafic réseau inhabituels ● Comportement inattendu du système, tel que des pannes ou des problèmes de performances ● Tentatives d'accès non autorisées ou changements de comportement des utilisateurs ● Alertes de sécurité provenant de solutions IDS, IPS ou antivirus
Où enquêter	● Journaux système et réseau pour identifier des modèles ou des activités inhabituelles ● Alertes et rapports des outils de sécurité sur les signes de menaces potentielles ● Appareils de point de terminaison pour preuve de compromission ou de malware ● Activités du compte utilisateur, y compris les connexions et les modèles d'accès
Actions possibles	Mettre en œuvre des contrôles d'accès et des politiques de mot de passe stricts, Mettre à jour et corriger régulièrement les systèmes et les logiciels, Déployer et configurer des solutions IDS, IPS et antivirus, Éduquer les utilisateurs sur les meilleures pratiques de sécurité et les menaces potentielles, Surveiller le trafic réseau et les journaux système pour détecter les anomalies, Utiliser les renseignements sur les menaces et analyse du comportement pour détecter et réagir aux activités inhabituelles

9. Transferts de fichiers suspects (contenu sensible, grande taille, etc.)

Ce que c'est	Les transferts de fichiers suspects font référence au déplacement de fichiers pouvant contenir du contenu sensible, d'une taille inhabituellement grande ou se produisant dans des circonstances atypiques, ce qui pourrait indiquer une menace à la sécurité telle qu'une comme une violation de données, un vol de propriété intellectuelle ou une exfiltration de données non autorisée.
Indicateurs de menace	● Transferts de gros volumes de données, surtout si la taille dépasse les seuils opérationnels typiques ● Fichiers contenant des informations sensibles ou confidentielles déplacés ou consultés de manière non autorisée ● Transferts survenant à des moments inhabituels ou à une fréquence plus élevée que la normale ● Fichiers envoyés ou reçus de sources externes inconnues ou non fiables
Où enquêter	● Journaux de trafic réseau pour identifier les modèles de mouvement de données inhabituels ● Journaux du système et des accès pour prouver l'accès ou les transferts non autorisés aux fichiers ● Systèmes de détection et de réponse des points finaux (EDR) pour les alertes liées au mouvement de fichiers ● Outils de prévention contre la perte de données (DLP) capables de suivre et de contrôler le transfert de données sensibles
Actions possibles	● Mettez en œuvre des contrôles d'accès stricts et surveillez les activités des utilisateurs pour garantir que seul le personnel autorisé peut déplacer ou accéder aux fichiers sensibles. ● Utiliser le cryptage des données en transit afin de protéger le contenu des fichiers en cours de transfert ● Utiliser des solutions DLP pour détecter et bloquer le transfert non autorisé d'informations sensibles ● Organiser régulièrement des formations de sensibilisation à la sécurité pour les employés afin de reconnaître et de signaler les menaces potentielles ● Établir des politiques claires pour le traitement et le transfert des données et les appliquer avec des contrôles techniques ● Utiliser des outils avancés de détection et de réponse aux menaces pour identifier et répondre aux activités suspectes

10. Activités de connexion suspectes

(Activité de déplacement impossible, heures non travaillées, etc.)

Ce que c'est	Les activités de connexion suspectes sont des tentatives d'accès au compte d'un utilisateur qui s'écartent de leurs comportements normaux. Il peut s'agir de connexions à des moments inhabituels, de nouveaux ou plusieurs emplacements ou des tentatives de connexion infructueuses répétées, ce qui peut indiquer qu'un compte est compromis ou attaqué
Indicateurs de menace	● Voyage impossible ● Heures non travaillées ● Échecs de connexion répétés
Où enquêter	● Journaux de sécurité et d'audit : vérifiez les journaux pour les tentatives de connexion échouées, les emplacements de connexion et les heures. ● Paramètres du compte utilisateur : vérifiez toute modification récente apportée aux paramètres du compte ou aux configurations de sécurité. ● Outils de sécurité des appareils et des réseaux : utilisez des outils tels que SIEM, EDR et IDS/IPS pour analyser et corréler les événements de sécurité
Actions possibles	Surveillez les connexions des utilisateurs, limitez les tentatives de connexion, mettez en œuvre une authentification forte et éduquez les utilisateurs

Ransomware

What It Is	A type of malware that encrypts files and requests a ransom (money payment) from the user to decrypt the traffic
Threat Indicators	User contacting; Burst of “file update” logs; Anti-virus alerts; Connection to suspicious IPs;
Where to Investigate	AV Logs; OS logs; Account logs; Network traffic; etc.
Possible Actions	Request AV checks; Isolate the machine; Turn off the machine*

https://www.linkedin.com/in/harunseker/

Botnets

What It Is	When attackers are using the victim server to perform DDoS attacks or other malicious activities
Threat Indicators	Connection to suspicious IPs; Abnormal high volume of network traffic;
Where to Investigate	Network traffic; OS logs (new processes); Contact server owner; Contact support teams;
Possible Actions	If confirmed: Isolate the server; Remove malicious processes; Patch the vulnerability utilized for infection;

Advanced Persistent Threats (APTs)

What It Is	When attackers get access to the system and create backdoors for further exploitation. Usually hard to detect.
Threat Indicators	Connection to suspicious IPs; Abnormal high volume of network traffic; Off-hours access logs; New admin account creations;
Where to Investigate	Network traffic; Access logs; OS logs (new processes, new connections, abnormal users); Contact server owner/support teams;
Possible Actions	If confirmed: Isolate the machine; Start formal forensics process; Start escalation/communication plan

https://www.linkedin.com/in/harunseker/

Compromised Accounts

What It Is	When attackers get access to one account (via social engineering or any other method)
Threat Indicators	Off-hours account logins; Account group changes; Abnormal high network traffic;
Where to Investigate	Active directory logs; OS logs; Network traffic; Contact user for clarifications
Possible Actions	If confirmed: Disable account; Password changes; Forensic investigations

Data Exfiltration

What It Is	When an attacker (or rogue employee) exfiltrate data to external sources
Threat Indicators	Abnormal high network traffic; Connection to cloud-storage solutions (Dropbox, Google Cloud, etc); Unusual USB sticks;
Where to Investigate	Network traffic; Proxy logs; OS logs
Possible Actions	If rogue employee: contact manager, perform full forensics If external threat: isolate the machine, disconnect from network

Denial of Service (DoS / DDoS)

What It Is	When an attacker is able to cause interference in a system by exploiting DoS vulnerabilities or by generating a high volume of traffic
Threat Indicators	Abnormal high network traffic in public facing servers;
Where to Investigate	Network traffic; Firewall logs; OS logs;
Possible Actions	If DoS due to vulnerabilities: Contact patching team for remediation If DDoS due to network traffic: Contact network support or ISP