Alerte 1 : **Outil Nmap détecté sur le serveur FR-01-86139**

Caractéristiques de l'alerte

Listez ici les éléments importants à savoir pour pouvoir traiter l'alerte. Ajoutez ou enlevez des points au besoin.

- ***Serveur affecté :*** *FR-01-86139 (Serveur Web hébergeant le site vitrine de Banco)*
- ***Outil détecté :*** *Nmap*
- ***Utilisateur :*** *Omer Berthelot de l'équipe Core*

Omer a confirmé que l'outil Nmap a été installé pour effectuer des tests de réseau temporaires.

Détails d'investigation

Reportez ici les éléments pertinents relevant de l'investigation. Ajoutez ou enlevez des points au besoin.

- ***Le hash de l'outil correspond bien à Nmap.***
- ***Nmap a été utilisé de manière légitime par un membre de l'équipe Core pour des tests de réseau. Cet usage était temporaire et ne devrait plus se reproduire.***

Plan d'action

Détaillez ici les points d'action que vous envisagez pour la résolution de chaque alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

- ***Désinstallation de Nmap :*** *Confirmer avec Omer Berthelot que Nmap a bien été désinstallé du serveur FR-01-86139.*
- ***Vérification de la configuration du serveur :*** *Assurer que les tests n'ont pas laissé de configurations potentiellement vulnérables ou d'accès non sécurisé.*
- ***Surveillance continue :*** *Activer une surveillance spécifique pour détecter toute utilisation future de Nmap ou d'autres outils similaires sur ce serveur.*
- ***Rapport:*** *Documenter et informer, renforcer la culture de la sécurité au sein de l'entreprise.*

Alerte 2 : **Windows Defender ATP a détecté Lockbit Mutex XO1XADpO01**

Caractéristiques de l'alerte

Listez ici les éléments importants à savoir pour pouvoir traiter l'alerte. Ajoutez ou enlevez des points au besoin.

- Machines affectées : *Plusieurs postes de travail du site de Bordeaux (WRK-BO-5789, WRK-BO-5797, etc.)*
- Mutex : *XO1XADpO01*
- Hash du processus : *a72e18efa33f1e3438dbb4451c335d487cbd4082*
- Exécutable : *B6kDLnDpHBYpjlGVLWwnZEX.exe*
- Adresse IP : *52.158.209.219*
- Nature de l'alerte : *Détection d'un ransomware Lockbit qui communique avec une adresse IP malveillante.*

Détails d'investigation

Reportez ici les éléments pertinents relevant de l'investigation. Ajoutez ou enlevez des points au besoin.

- VirusTotal : *La recherche du hash confirme le caractère malveillant de l'exécutable.*
- Mutex : *Le nom du Mutex confirme qu'il s'agit d'un ransomware Lockbit.*
- Communication IP *: L'exécutable communique avec l'adresse IP 52.158.209.219.*
- Impact : *Aucun poste de travail n'a encore affiché de message de rançon, ce qui signifie que le ransomware est détecté avant de se déployer complètement.*

Plan d'action

Détaillez ici les points d'action que vous envisagez pour la résolution de chaque alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

-Isolation immédiate des machines affectées : *Déconnecter les postes de travail WRK-BO-5789, WRK-BO-5797, WRK-BO-5792, WRK-BO-5807, WRK-BO-5798, et WRK-BO-5804 du réseau pour prévenir la propagation du ransomware.*
- Bloquer hash du procesus *a72e18efa33f1e3438dbb4451c335d487cbd4082 , ajouter à l'antivirus*
- Blocage de l'adresse IP : *Configurer le pare-feu pour bloquer toute communication entre les machines internes et l'adresse IP 52.158.209.219.*
- Analyse et suppression : *Effectuer une analyse complète des machines pour identifier et supprimer l'exécutable malveillant (B6kDLnDpHBYpjlGVLWwnZEX.exe).*
- Réinitialisation des systèmes : *Si nécessaire, réinitialiser les machines affectées pour assurer l'élimination complète du ransomware.*
- Surveillance accrue : *Mettre en place une surveillance spécifique des machines affectées et des logs réseau pour détecter toute autre tentative de communication malveillante.*
- Documentation et rapport : *Documenter les actions prises et rédiger un rapport pour la direction, expliquant l'incident et les mesures d'atténuation.*

Alerte 3 : **2058 requêtes malveillantes bloquées sur le WAF**
(Alerte la plus importante à traiter : Un script de blocage pour ces IP est plus pertinent car ils attaquent le serveur WAF)

Caractéristiques de l'alerte

Listez ici les éléments importants à savoir pour pouvoir traiter l'alerte. Ajoutez ou enlevez des points au besoin.

- Requête malveillante (tentative d'injection SQL) : *[url] : hxxps://api-endpoint[.]banco[.]com?product=-1+union+select+1,2,3,4,5,6,7,8,9,(SELECT+group_concat(table_name)+from+information_schema[.]tables+where+table_schema=database()) <script\x0Ctype="text/javascript">javascript (document[.]cookie);</script>*

- IPs malveillantes (IOCs) : *118.71.95.25, 115.89.119.166, 193.174.167.74, 7.227.7.145, 48.108.146.81, 87.129.91.47, 46.123.183.243, 170.169.43.40, 77.159.91.107, 219.253.23.64, 204.8.93.157, 238.105.95.237, 223.230.60.83, 102.66.3.221, 10.203.234.137, 95.84.125.255, 209.224.20.64, 147.65.131.19, 113.191.0.101, 23.11.96.242, 191.203.101.233, 127.238.70.112, 236.143.151.139, 43.235.240.197, 101.115.94.82, 200.154.55.33, 248.10.203.170, 226.134.226.229, 174.181.123.25, 238.237.9.63*

- Nombre d'adresses IP impliquées : *241 adresses IP à l'origine des requêtes.*

- Nature des requêtes : *Provenant d'un outil de scan de vulnérabilité non déterminé.*

- Adresse IP suspecte : *104.238.46.241, associée à un fournisseur de VPN, utilisée par un client Banco.*

Reportez ici les éléments pertinents relevant de l'investigation. Ajoutez ou enlevez des points au besoin.

- Logs du WAF : *Les logs ont révélé 241 IPs responsables des requêtes malveillantes.*

- Client Banco suspect : *L'adresse IP 104.238.46.241, utilisée par un client avec une balance nulle, fait partie des IPs suspectes.*

- Suspicion d'utilisation de VPN *: Cette IP semble appartenir à un fournisseur de VPN, ce qui complique l'identification précise de l'origine.*

Plan d'action

Détaillez ici les points d'action que vous envisagez pour la résolution de chaque alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

- Blocage des IPs : *30 adresses IP ont été identifiées dans les observables et bloquées pour empêcher d'autres requêtes malveillantes.*

- Blocage de l'URL : *L'URL malveillante hxxps://api-endpoint[.]banco[.]com?product=-1+union+select+... a également été bloquée à l'aide du script Python pour prévenir toute tentative d'exploitation via cette URL.*

- Investigation sur 104.238.46.241 : *Vérifier l'usage légitime ou compromis de cette IP par le client Banco et le contacter si nécessaire.*

- Analyse des logs : *Analyser les logs pour détecter d'autres comportements suspects liés aux IPs bloquées.*

- Surveillance accrue : *Mettre en place une surveillance continue et activer des alertes pour les IPs suspectes, notamment celles associées à des VPN.*

- Documentation : *Documenter les actions et rédiger un rapport pour la direction.*

Alerte 4 : **Nombre d'échecs d'authentification dépasse 300 par heure**

Caractéristiques de l'alerte

- Serveur affecté : *Console Azure*
- Nature de l'attaque : *Tentative de bruteforce sur plusieurs comptes utilisateurs*
- Utilisateurs ciblés : *Gilberte Batteux, Samantha Aparicio, Octavia Carballar, Santiago Franco, Emilio Villa*
- Adresses IP suspectes : *5.31.3.31, 54.24.3.85, 55.64.4.15*
- Résultat : *Tentative réussie sur le compte d'Emilio Villa, sans double authentification activée*

Détails d'investigation

Reportez ici les éléments pertinents relevant de l'investigation. Ajoutez ou enlevez des points au besoin.

- Les tentatives de bruteforce proviennent des adresses IP suivantes : *5.31.3.31, 54.24.3.85, 55.64.4.15.*

Ces adresses IP ont ciblé les comptes des utilisateurs mentionnés ci-dessus.
Une tentative de bruteforce a réussi sur le compte d'Emilio Villa, qui n'avait pas activé la double authentification sur son compte Azure.

Plan d'action

Détaillez ici les points d'action que vous envisagez pour la résolution de chaque alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

- Blocage IP : *Bloquer les trois adresses IP identifiées pour prévenir de nouvelles tentatives.*
- Sécurisation : *Activer la double authentification pour Emilio Villa et lui faire changer son mot de passe.*
- Audit : *Analyser les journaux Azure pour d'autres tentatives suspectes.*
- Communication : *Informer les utilisateurs concernés et leur donner des recommandations de sécurité.*
- Surveillance : *Activer une surveillance continue avec des alertes spécifiques.*
- Documentation : *Documenter les actions et soumettre un rapport à la direction.*

Alerte 5 : **Alerte Windows Defender ATP: Opération de type Kerberoasting détecté sur FR-DC-01**

Caractéristiques de l'alerte

Listez ici les éléments importants à savoir pour pouvoir traiter l'alerte. Ajoutez ou enlevez des points au besoin.

- Machine affectée : *FR-DC-01 (Serveur de domaine).*
- Processus suspect : *yolokatz.exe.*
- Hash du processus : *d007f64dae6bc5fdfe4ff30fe7be9b7d62238012.*
- Compte de service compromis : *srv_database_app01.*
- Adresse IP source : *10.80.43.10.*
- Type d'attaque : *Kerberoasting visant à extraire des MDP hachés à partir de l'Active Directory.*

Reportez ici les éléments pertinents relevant de l'investigation. Ajoutez ou enlevez des points au besoin.

- VirusTotal : *Confirme que le hash appartient à un outil portant la signature de Mimikatz, utilisé pour des attaques de type Kerberoasting.*
- Comportement observé : *L'adresse IP 10.80.43.10 a récupéré le mot de passe haché du compte de service srv_database_app01, qui dispose de privilèges d'administration sur les serveurs de base de données SWIFT.*
- Utilisateur associé : *L'adresse IP est attribuée au poste de travail de Simonne Girard.*

Plan d'action

Détaillez ici les points d'action que vous envisagez pour la résolution de chaque alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

- Isolation de la machine FR-DC-01 : *Déconnecter la machine du réseau pour éviter toute propagation.*
- Blocage de l'adresse IP 10.80.43.10 : *Configurer le pare-feu pour bloquer toute communication avec cette adresse IP.*
- Bloquer hash du procesus *d007f64dae6bc5fdfe4ff30fe7be9b7d62238012 ajouter à l'antivirus*
- Réinitialisation des mots de passe : *Modifier le mot de passe du compte srv_database_app01 sur tous les systèmes où il est utilisé.*
- Surveillance accrue : *Activer une surveillance des journaux de sécurité pour détecter toute autre activité suspecte liée à cette attaque.*
- Évaluation des accès du compte compromis : *Réaliser une évaluation des accès du compte srv_database_app01 pour identifier d'éventuelles activités suspectes antérieures à l'attaque.*
- Neutralisation du processus Yolokatz : *Supprimer ou neutraliser le processus yolokatz.exe s'il est encore actif sur la machine, et analyser les autres processus pour détecter d'éventuelles menaces supplémentaires.*
- Notification des parties concernées : *Informer les utilisateurs administratifs ou les propriétaires des serveurs SWIFT de l'incident, en raison des privilèges élevés du compte compromis.*
- Évaluation de l'impact et criticité de l'attaque : *L'attaque Kerberoasting vise spécifiquement à obtenir des tickets de service Kerberos, ce qui pourrait compromettre davantage de comptes si elle n'est pas contrôlée.*
- Rapport : *Documenter les actions et informer la direction.*