INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

5ème année INSA Centre Val de Loire

Spécialité sécurité et technologies informatiques

Rapport 5ème année

Module SOC

Documentation sur les règles de détection Splunk

Membres de l'équipe	*Encadré par*
BENDAHMANE Rayane	*M. Quentin Arnould*
VIRGOS Antoine	*M. Alexandre Le Clanche*
MERZOUQI Ayet	*M. Thomas Benet*
ST-JEAN Philémon	
MAKALOU Shérif	

Stratégie de détection

Connectix est une petite entreprise. Elle a plus de chance d'être attaquée par les eCrime qui sont des opportunistes ciblant des petites boîtes et cherchant à faire du profit. Ce sont des pirates qui aiment attaquer à l'aide de malwares afin de pénétrer les systèmes, chiffrer ou exfiltrer les données et demander des rançons en retour. Donc faudra s'attendre à des techniques de brute force, d'usurpation de compte, d'infiltration réseaux, d'escalade de privilèges etc
On doit donc élaborer notre stratégie en détectant des comportements suspects qui rentreraient dans ce cadre.

Alertes

1. Intrusion sur le système

Détection d'Élévation de Privilèges via OpenVPN

Description :
Cette alerte détecte l'utilisation de la commande OpenVPN avec des paramètres spécifiques permettant une élévation de privilèges.

Classification MITRE ATT&CK :

Tactic	Technique/Sub-technique	Description
Privilege Escalation	T1068 - Exploitation for Privilege Escalation	utilisée par les attaquants pour exploiter une faiblesse dans une application ou un service.

Scénario d'Attaque

Élévation de Privilèges : En utilisant OpenVPN avec des options spécifiques (--dev, --script-security, --up, et sudo), l'attaquant cherche à exécuter des scripts ou des commandes avec des privilèges élevés.

Persistance et Mouvement Latéral : Une fois les privilèges élevés obtenus, l'attaquant peut installer des backdoors, exécuter des logiciels malveillants ou se déplacer latéralement dans le réseau pour compromettre davantage de systèmes.

Évasion des Défenses : En utilisant OpenVPN, un logiciel souvent considéré comme légitime, l'attaquant peut réduire les risques de détection.

Technique de Détection :

- **Type de Log :** Sysmon pour Linux, EventID 1

Cette détection est configurée pour surveiller les événements où OpenVPN est exécuté avec des arguments suspects dans la ligne de commande, signalant une potentielle tentative d'élévation de privilèges.

Priorité et Niveau de Sévérité :

- **Sévérité :** High
- **Justification :** La compromission des privilèges administratifs via OpenVPN peut permettre une prise de contrôle totale de l'hôte et faciliter d'autres mouvements latéraux et actions malveillantes.

Actions de Remédiation :

Blocage Immédiat : Déconnectez la machine compromise du réseau pour empêcher toute activité supplémentaire.

Examen des Logs : Analysez les journaux d'activité des processus pour identifier la source de la tentative et retracez les actions entreprises par l'attaquant.

Réinitialisation des Privilèges : Examinez et révoquez les privilèges sur les comptes affectés, et modifiez les configurations d'OpenVPN pour restreindre l'utilisation de paramètres sensibles.

Faux Positifs :

- **Légitimes Cas d'Utilisation :** Certaines configurations d'OpenVPN peuvent nécessiter ces paramètres pour un usage technique spécifique.
- **Tests et Maintenance :** Des administrateurs peuvent utiliser ces paramètres lors de tests ou de maintenance.

Création/Suppression fréquentes de comptes utilisateurs

Description

Identifier des tentatives malveillantes d'ajout ou de suppression de comptes pour maintenir un accès persistant ou se dissimuler dans l'infrastructure.

Classification MITRE ATT&CK

Cette règle de détection de la création ou suppression récurrente de comptes est classée sous la matrice MITRE ATT&CK dans la catégorie *Création de comptes* (Technique T1136) et *Destruction d'informations* (Technique T1485). Elle permet d'identifier des activités suspectes liées à la manipulation de comptes utilisateurs, potentiellement pour faciliter une attaque en renforçant ou en compromettant les accès.

Scénario d'attaque

Dans ce scénario, un acteur malveillant pourrait créer de nouveaux comptes pour établir un accès persistant au réseau ou supprimer des comptes pour masquer ses traces et entraver la réponse aux incidents. La création et la suppression répétées de comptes utilisateurs sur les serveurs critiques

peuvent indiquer une tentative de dissimulation, de maintien de contrôle ou d'altération des capacités d'authentification.

Technique de détection

La règle est basée sur les événements de sécurité Windows ayant les *EventCodes* 4720 (création d'un compte) et 4726 (suppression d'un compte). Elle agrège les événements en fonction des utilisateurs et des heures de création/suppression (_time) et déclenche une alerte si un même compte effectue au moins trois actions de ce type dans un court laps de temps. Cette règle cible spécifiquement les adresses IP de serveurs sensibles.

Priorité et niveau de sévérité

Le niveau de sévérité est élevé pour cette alerte, car des changements récurrents de comptes sur des serveurs sensibles peuvent indiquer une compromission ou un accès non autorisé. La priorité est donnée à cette détection pour éviter que l'attaquant puisse obtenir des privilèges prolongés ou perturber les opérations de l'organisation.

Actions de remédiation

En cas d'alerte, il est essentiel de vérifier si la création ou suppression des comptes est légitime, en consultant les responsables des comptes ou les politiques internes. Si une activité malveillante est confirmée, il est recommandé de suspendre les comptes créés récemment et d'effectuer un audit approfondi des permissions et privilèges des comptes utilisateurs. En outre, il peut être pertinent de renforcer les contrôles d'accès sur les serveurs critiques pour limiter la création de comptes sans authentification préalable.

Faux-positifs

Des faux-positifs peuvent se produire si des administrateurs effectuent des mises à jour ou des configurations légitimes des comptes utilisateurs, surtout dans le cadre de déploiements ou de tâches de maintenance. Il est important de consulter les équipes en charge des comptes et de maintenir une documentation des modifications prévues pour différencier les activités normales des activités potentiellement malveillantes.

Connexion avec privilèges pour des comptes à droits restreints

Description

Cette règle permet de détecter une connexion avec de hauts privilèges de comptes n'ayant initialement aucun droit de super-utilisateur.

Classification MITRE ATT&CK

Cette règle de détection est classée sous la matrice MITRE ATT&CK dans la catégorie *Élévation de privilèges* (Technique T1078.003 : Valid Accounts – Windows Admin). Elle vise à détecter des tentatives d'accès avec des privilèges élevés, un comportement souvent associé à des escalades de privilèges ou à un accès non autorisé par des comptes disposant habituellement de droits restreints.

Scénario d'attaque

Dans ce scénario, des comptes d'utilisateurs spécifiques ayant des droits limités se connectent soudainement avec des privilèges élevés (via EventCode 4672), ce qui pourrait indiquer une

compromission de compte. Un acteur malveillant pourrait utiliser un compte légitime pour obtenir des droits administratifs et étendre ses capacités d'accès, ce qui pourrait permettre des actions malveillantes étendues sur le système, telles que la modification de fichiers ou la suppression de journaux d'audit.

Technique de détection

La règle repose sur l'analyse des événements de sécurité Windows identifiés par *EventCode* 4672, qui signale les connexions avec privilèges spéciaux. Elle suit les comptes spécifiés (Zane, Ethan, Scott, Willa, Victor, Lee, Taylor, Samuel, Noah) qui sont tous des comptes non-admins, en les associant aux privilèges, au nom de l'ordinateur (ComputerName) et au moment de la connexion (_time). Cette règle s'applique à tous les serveurs de l'infrastructure.

Priorité et niveau de sévérité

Le niveau de sévérité est critique pour cette alerte, car des accès avec privilèges élevés par des comptes restreints constituent un signe important de possible compromission.

Actions de remédiation

En cas d'alerte, il est recommandé de désactiver immédiatement le compte suspect et d'effectuer une révision des activités de l'utilisateur pour identifier d'autres signes de compromission. Il est également pertinent de mettre en place une surveillance renforcée pour détecter des activités similaires sur d'autres comptes, ainsi que de s'assurer que des contrôles d'accès stricts limitent les droits d'élévation de privilèges.

Faux-positifs

Des faux-positifs peuvent se produire si un administrateur attribue temporairement des privilèges élevés à un compte pour une tâche spécifique, ou si des accès privilégiés sont nécessaires dans le cadre de mises à jour. Une documentation claire des procédures de maintenance est essentielle pour réduire les faux-positifs et pour faciliter l'identification d'accès suspects sans interférer avec les activités légitimes.

Mimikatz Credential Dumper

Description

Cette règle détecte l'exécution d'outils de type Mimikatz (permet de récupérer des informations d'identification stockées, comme les mots de passe en clair ou les hash) qui extraient les informations d'identification, y compris les techniques de vol de hash NTLM (protocole d'authentification développé par Microsoft) et l'extraction de mots de passe en clair depuis le processus LSASS (responsable de l'application des politiques de sécurité, de la gestion des sessions de connexion et de l'authentification des utilisateurs).

Classification MITRE ATT&CK

La règle "Mimikatz Credential Dumper" est classée sous la matrice MITRE ATT&CK dans la catégorie Accès aux informations d'identification (Credential Access). Elle correspond à la technique T1003.001 (OS Credential Dumping: LSASS Memory), ciblant l'extraction d'informations d'identification en accédant à la mémoire LSASS.

Scénario d’attaque

Dans ce scénario, un attaquant ayant compromis un système utilise Mimikatz ou des outils similaires pour extraire des informations d'identification critiques de la mémoire LSASS. Ces informations peuvent ensuite être utilisées pour se déplacer latéralement dans l'environnement, escalader les privilèges, ou encore accéder à des ressources sensibles. L'extraction des informations d'identification constitue souvent une phase initiale de priorité majeur pour un attaquant.

Technique de détection

La règle repose sur la détection de l'Event Code 4697, associé à la création de services qui exécutent des scripts ou des binaires liés à l'extraction de mots de passe. Des noms de services ou fichiers connus tels que mimidrv, pwdump, ou gsecdump sont surveillés pour indiquer une potentielle activité malveillante. La surveillance de ces indicateurs servira de vecteur de détection compte à l'usage de Mimikatz avant que l'attaquant ne puisse compromettre davantage le système.

Priorité et niveau de sévérité

Le niveau de sévérité est critique, car l'extraction d'informations d'identification à partir de LSASS peut compromettre l'ensemble de l'environnement. Un attaquant ayant accès à ces informations peut aisément escalader les privilèges ou réaliser des attaques de mouvement latéral, nécessitant une réponse immédiate.

Actions de remédiation

En cas d’alerte, il est impératif de :

1. Isoler immédiatement la machine compromise pour empêcher toute exfiltration de données ou mouvement latéral.
2. Examiner les processus en cours pour confirmer la présence d'outils de type Mimikatz et les supprimer.
3. Analyser les logs pour identifier d'autres machines potentiellement compromises ou d'autres signes d'activité malveillante.
4. Réinitialiser les mots de passe des comptes affectés et des comptes administratifs pour limiter l'impact de l'attaque.
5. Mettre en œuvre des protections supplémentaires, telles que Windows Defender Credential Guard, pour sécuriser les informations d'identification en mémoire.

Faux-positifs

Des faux-positifs peuvent survenir si des outils de sécurité légitimes ou des scripts d'administration utilisent des techniques similaires pour tester ou auditer les systèmes. Une vérification manuelle de l'origine des événements est nécessaire.

Tentative de Dump LSASS

Description

Cette règle détecte les tentatives de dump du processus LSASS, une technique utilisée pour extraire les mots de passe stockés en mémoire et accéder aux informations d'identification des utilisateurs.

Classification MITRE ATT&CK

La règle "Tentative de Dump LSASS" est classée sous la matrice MITRE ATT&CK dans la catégorie Accès aux informations d'identification (Credential Access). Elle correspond à la technique T1003.001 (OS Credential Dumping: LSASS Memory), car elle cible l'extraction d'informations d'identification à partir de la mémoire du processus LSASS, souvent utilisée par des outils comme Mimikatz.

Scénario d'attaque

Un attaquant ayant obtenu un accès privilégié à un système tente de dumper la mémoire de LSASS pour récupérer des mots de passe en clair, des hashes NTLM, ou d'autres secrets.

Technique de détection

La règle repose sur l'analyse de l'Event Code 4656, qui enregistre les tentatives d'accès à des objets sensibles. Elle surveille les accès à *lsass.exe* avec des masques d'accès spécifiques tels que 0x705, associés à des tentatives de lecture de la mémoire du processus. L'utilisation de cette technique permet de repérer les tentatives d'extraction d'informations d'identification, même si les outils d'attaque sont déguisés ou modifiés.

Priorité et niveau de sévérité

Le niveau de sévérité est critique, car l'extraction réussie de données de LSASS peut compromettre rapidement l'intégrité de l'environnement et permettre à un attaquant de réaliser des attaques de grande envergure.

Actions de remédiation

En cas d'alerte, il est impératif de :

1. Isoler la machine affectée pour empêcher toute exfiltration de données ou propagation de l'attaque.
2. Vérifier les processus en cours, notamment ceux qui interagissent avec LSASS, et les terminer si nécessaire.
3. Analyser les logs pour identifier la source de l'attaque et vérifier s'il y a d'autres machines compromises.
4. Renforcer les mesures de sécurité pour protéger LSASS, comme l'utilisation de Windows Defender Credential Guard.
5. Réinitialiser les mots de passe des comptes d'administrateurs compromis et surveiller l'activité ultérieure.

Faux-positifs

Des faux-positifs peuvent survenir si des outils de sécurité légitimes, comme des antivirus ou des solutions de monitoring, accèdent à LSASS pour des analyses. Une vérification manuelle est nécessaire.

Attaque PetitPotam sur le Partage Réseau

Description

Cette règle détecte l'attaque PetitPotam, qui utilise des requêtes sur des partages réseau pour exfiltrer des informations sensibles ou escalader les privilèges dans un domaine Windows.

Classification MITRE ATT&CK

La règle "Attaque PetitPotam sur le partage réseau" est classée sous la matrice MITRE ATT&CK dans la catégorie Mouvement Latéral (Lateral Movement). Elle correspond à la technique T1550.002 (Use Alternate Authentication Material - Pass the Hash), car cette attaque exploite des fonctionnalités d'authentification pour s'introduire latéralement et potentiellement compromettre des contrôleurs de domaine.

Scénario d'attaque

Dans ce scénario, un attaquant ayant accès à un réseau interne exploite l'attaque PetitPotam pour forcer un serveur ou un contrôleur de domaine à s'authentifier sur un serveur malveillant contrôlé par l'attaquant (notion de relay / spoofing). Cela permet de capturer des informations d'authentification précieuses ou d'exploiter des protocoles pour escalader les privilèges. L'attaque cible des partages comme \\IPC$ et utilise des comptes anonymes pour masquer l'origine de l'activité malveillante.

Technique de détection

La règle repose sur la détection des événements Windows spécifiques au partage réseau. Elle surveille l'Event Code 5145, qui indique les *tentatives d'accès à un partage*, en se concentrant sur le **partage \\IPC$** et les comptes *ANONYMOUS LOGON*. La règle génère une alerte pour toute tentative d'accès suspecte, particulièrement si elle vise à exécuter des requêtes non autorisées vers des ressources sensibles.

Priorité et niveau de sévérité

Le niveau de sévérité est élevé, car une exploitation réussie de l'attaque PetitPotam peut permettre à un attaquant de compromettre des serveurs critiques ou des contrôleurs de domaine (notions de compromission étendue dans l'environnement).

Actions de remédiation

En cas d'alerte, il est conseillé de :

1. Bloquer immédiatement l'accès au serveur ou à la ressource partagée ciblée par l'attaque.
2. Analyser les journaux pour identifier l'origine de la tentative et vérifier si d'autres actions suspectes ont été effectuées.
3. Renforcer les configurations de sécurité des contrôleurs de domaine, en limitant les communications SMB inutiles.

4. Appliquer des correctifs de sécurité et configurer des protections telles que l'authentification Kerberos pour limiter les attaques de relais NTLM.
5. Surveiller de près l'activité réseau pour détecter d'autres tentatives de ce type.

Faux-positifs

Des faux-positifs peuvent survenir lors d'activités légitimes d'administration ou de surveillance réseau. Une validation manuelle avec les équipes responsables des serveurs et de l'infrastructure est nécessaire pour évaluer si l'activité est suspecte ou attendue.

Sysmon | Suspicious Process Creation in Temp or AppData

Description

Détecte la création de processus dans des répertoires temporaires : Temp ou AppData. Cette règle de détection permet d'Identifier toute exécution suspecte de processus dans des répertoires temporaires, ce qui pourrait indiquer une tentative d'intrusion ou l'exécution de logiciels malveillants sur le système.

Classification MITRE ATT&CK

- **T1059 : Command and Scripting Interpreter** - Exécuter des commandes, des scripts et des binaires sur des systèmes. Les interprètes de commandes PowerShell sur Windows ou les shells Unix sont les plus souvent utilisés.
- **T1203 : Exploitation for Client Execution** - Exploitation de vulnérabilités dans des applications côté client pour exécuter du code malveillant.

Scénario d'attaque

Après avoir obtenu un accès initial au système, l'attaquant dépose un fichier exécutable malveillant dans le répertoire Temp ou AppData de l'utilisateur. Il exécute ensuite ce fichier pour :

- établir une persistance
- effectuer une reconnaissance du système
- lancer d'autres activités malveillantes.

Technique de détection

Événement ciblé : EventID 1 (Création de Processus) et voir si le chemin du processus créé contient '\Temp' ou '\AppData'. Utilisation de Sysmon.

Priorité et niveau de sévérité

Priorité : Élevée | La création de processus dans des répertoires temporaires tels que Temp ou AppData est souvent associée à des comportements malveillants.

Niveau de sévérité : High | Représente un risque significatif concernant l'exécution de processus non autorisés dans les emplacements sensibles Temp et AppData.

Actions de remédiation

- Isoler immédiatement le système concerné du réseau
- Examiner les logs système pour identifier d'autres activités suspectes
- Analyse antivirus complète du système

- Si confirmé malveillant, supprimer le fichier exécutable et tout autre artefact associé

Faux-positifs

Microsoft Windows Defender : **MpSigStub.exe** et **MpCmdRun.exe**.

Sysmon | Executable File Creation in Sensitive Directories

Description

Détecte la création de fichiers exécutables (.exe) dans des répertoires sensibles tels que System32 et SysWOW64. Cette règle de détection permet d'identifier toute création suspecte de fichiers exécutables dans des répertoires sensibles, ce qui pourrait signaler une compromission du système ou une tentative d'injection de logiciels malveillants.

Classification MITRE ATT&CK

- **T1203 : Exploitation of Client-Side Applications** - Exploitation de vulnérabilités dans des applications côté client pour exécuter du code malveillant.
- **T1059 : Command-Line Interface Usage for Executing Commands** - Cette technique permet aux attaquants d'exécuter des commandes et des scripts via des interprètes de commandes, souvent utilisés pour automatiser des tâches malveillantes.

Scénario d'attaque

Après avoir obtenu un accès initial au système, l'attaquant peut créer un fichier exécutable dans un répertoire sensible comme System32 et SysWOW64, ce qui lui permet de masquer son activité et de maintenir une présence sur le système.

Technique de détection

Événement ciblé : EventID 11 (Création/Modification de fichier) et voir si TargetFilename contient '\System32\.exe' ou '\SysWOW64\.exe'. Utilisation de Sysmon.

Priorité et niveau de sévérité

Priorité : Élevée | La création de fichiers exécutables dans des répertoires sensibles comme System32 et SysWOW64 est souvent un indicateur d'activités malveillantes.

Niveau de sévérité : High | Représente un risque significatif associé à la création de fichiers exécutables dans les emplacements sensibles System32 et SysWOW64.

Actions de remédiation

- Isoler immédiatement le système concerné du réseau
- Examiner les logs système pour identifier d'autres activités suspectes
- Analyse antivirus complète du système
- Si confirmé malveillant, supprimer le fichier exécutable et tout autre artefact associé
- Renforcer les contrôles d'accès et appliquer des mises à jour de sécurité pour prévenir les futures compromissions

Faux-positifs

Des applications légitimes, comme les mises à jour de Windows ou d'autres logiciels, peuvent créer des fichiers exécutables dans les répertoires System32 et SysWOW64 lors de leur installation ou mise à jour.

Sysmon | Suspicious DLL Loading Activity

Description

Détecte les cas où le même processus charge plus de 3 fichiers DLL (.dll). Cette règle de détection permet d'identifier les comportements suspects liés au chargement de DLL, qui peuvent être indicatifs d'une compromission du système ou d'une tentative d'exécution de code malveillant

Classification MITRE ATT&CK

- **T1055 : Process Injection -** Injecter du code dans le processus d'un autre programme, souvent pour exécuter des actions malveillantes sans être détectés.

Scénario d'attaque

Après avoir obtenu un accès initial au système, l'attaquant peut utiliser une technique d'injection pour charger plusieurs DLL malveillantes dans un processus légitime. Cela peut lui permettre d'exécuter des commandes arbitraires, de voler des informations sensibles ou de maintenir une présence sur le système sans éveiller les soupçons.

Technique de détection

Événement ciblé : EventID 7 (chargement d'une image) | Déclenchée plus de 3 fois. Utilisation de Sysmon.

Priorité et niveau de sévérité

Priorité : Élevée | Le chargement anormal de DLL peut être un indicateur fort d'activités malveillantes.

Niveau de sévérité : Medium | Bien que le chargement excessif de DLL puisse signaler une activité suspecte, il peut également résulter de comportements légitimes dans certaines applications.

Actions de remédiation

- Examiner les logs associés pour identifier d'autres activités suspectes
- Analyse antivirus complète du système
- Si le chargement des DLL est confirmé comme malveillant, supprimer les fichiers concernés et toute autre artefact associé
- Renforcer les contrôles d'accès et appliquer des mises à jour de sécurité pour prévenir les futures compromissions

Faux-positifs

Les applications légitimes qui chargent des DLLs plusieurs fois.

2. Persistance sur le serveur

Exécution Suspecte de rundll32.exe

Description

Cette alerte identifie l'utilisation potentiellement malveillante de rundll32.exe pour exécuter des commandes sans paramètres de ligne de commande, ou avec des paramètres inhabituels, souvent en relation avec des DLL malveillantes

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Defense Evasion	T1070 – Indicator Removal on Host	Détection de transferts importants de données, pouvant indiquer une exfiltration de données.
Execution	T1218.011 – Signed Binary Proxy Execution: rundll32	Utilisation de rundll32.exe pour exécuter des fonctions malveillantes, contournant les solutions de sécurité

Scénario d'Attaque utilisant rundll32.exe avec Cobalt Strike

Phase d'Accès Initial : L'attaquant obtient un accès initial au système cible, par exemple, en utilisant du phishing pour introduire un malware dans le réseau de la victime.

Déploiement de Cobalt Strike : L'attaquant utilise Cobalt Strike, un outil de post-exploitation, pour déployer un agent ("beacon") sur la machine compromise, maintenant ainsi un accès persistant.

Utilisation de rundll32.exe sans Paramètres : Pour éviter la détection, l'attaquant utilise rundll32.exe sans paramètres ou avec des commandes modifiées. Cobalt Strike exploite ce comportement pour déclencher des charges utiles tout en restant furtif, exploitant le fait que rundll32.exe est un processus système légitime.

Mouvement Latéral et Évasion : En utilisant le beacon, l'attaquant procède à un déplacement latéral, essaie de compromettre d'autres machines et échappe aux solutions de détection en profitant du masque de légitimité de rundll32.exe.

Technique de Détection

Type de Log : Sysmon Event ID 1 (Création de Processus)

La détection repose sur l'analyse des exécutions de rundll32.exe en recherchant des commandes suspectes ou une absence de paramètres (anormal pour une utilisation légitime). La requête filtre également les processus parents exécutés depuis des chemins non standards pour détecter les comportements potentiellement malveillants.

Priorité et Niveau de Sévérité

Sévérité : Haute

Justification : L'utilisation de rundll32.exe de manière détournée peut permettre à un attaquant d'exécuter du code malveillant tout en contournant certains systèmes de détection.

Actions de Remédiation

- Analyse du Processus
- Isolation de la Machine
- Réinitialisation des Crédentiels

Faux Positifs :

Cette alerte détecte que les True Positifs

Création d'Utilisateur Caché

Description

Cette règle détecte la création de comptes utilisateurs cachés, souvent utilisés par les attaquants pour maintenir un accès non autorisé et persistant sur un système.

Classification MITRE ATT&CK

La règle "Création d'utilisateur caché" est classée sous la matrice MITRE ATT&CK dans la catégorie Persistance (Persistence). Elle correspond à la technique T1136.001 (Create Account: Local Account), permettant à un attaquant de créer des comptes qui peuvent être utilisés pour conserver un *accès furtif* au système.

Scénario d'attaque

Dans ce scénario, un attaquant ayant obtenu des privilèges suffisants sur un système crée un compte utilisateur caché pour accéder ultérieurement au système de manière discrète. Les comptes cachés sont souvent configurés avec des noms se terminant par un symbole $, rendant leur détection plus difficile dans les environnements Windows. Ces comptes sont ensuite utilisés pour des actions malveillantes sans éveiller les soupçons.

Technique de détection

La règle repose sur la détection de l'Event Code 4720, qui enregistre la création de nouveaux comptes utilisateurs. Elle vérifie spécifiquement les comptes dont le nom se termine par $, une pratique courante pour cacher les comptes dans l'Active Directory. La règle exclut les exceptions connues, telles que HomeGroupUser$, pour limiter les faux positifs.

Priorité et niveau de sévérité

Le niveau de sévérité est élevé, car la création de comptes cachés peut permettre à un attaquant de maintenir un accès persistant de façon furtif sur un système.

Actions de remédiation

En cas d'alerte, il est recommandé de :

1. Suspendre ou supprimer immédiatement le compte utilisateur suspect.
2. Analyser l'activité associée au compte pour identifier les actions malveillantes.
3. Vérifier les permissions et les groupes auxquels le compte appartient
4. Auditer les logs de sécurité pour détecter d'autres signes d'activité suspecte ou d'autres comptes créés de manière similaire.
5. Surveiller régulièrement les créations de comptes.

Faux-positifs

Des faux-positifs peuvent survenir si des comptes sont créés intentionnellement par des administrateurs pour des tâches spécifiques ou des configurations réseau. C’est pourquoi, une vérification avec les équipes responsables de la gestion des comptes est nécessaire pour évaluer leurs légitimités dans un scénario réel.

Script PowerShell Installé en Tant que Service

Description

Cette règle détecte l'installation d'un script PowerShell en tant que service, une méthode de persistance utilisée par les attaquants pour exécuter du code malveillant de manière furtive.

Classification MITRE ATT&CK

La règle "Script PowerShell installé en tant que service" est classée sous la matrice MITRE ATT&CK dans la catégorie Persistance (Persistence). Elle correspond à la technique T1543.003 (Create or Modify System Process - Windows Service), car elle permet aux attaquants de créer ou de modifier des processus système pour maintenir un accès persistant.

Scénario d’attaque

Dans ce scénario, un attaquant ayant déjà réussi à compromettre un système configure un script PowerShell comme un service Windows. Ce service peut exécuter des commandes malveillantes à chaque démarrage ou à des moments spécifiques, facilitant la persistance et permettant à l'attaquant de maintenir un contrôle discret sur l’hôte (ou bien télécharger d'autres charges utiles, exfiltrer des données, ou déployer des payloads furtifs).

Technique de détection

La règle repose sur la surveillance des événements Windows liés à la création de services, en se concentrant sur l'Event Code 4697. Elle détecte les scripts ou exécutables PowerShell installés comme services. Les chemins et noms des fichiers exécutés sont vérifiés pour identifier des exécutions suspectes. Les termes comme powershell et pwsh nous serviront ici d’indicateurs courants d’une activité potentiellement malveillante.

Priorité et niveau de sévérité

Le niveau de sévérité est élevé, car l’installation de scripts PowerShell en tant que service peut permettre une exécution persistante de code malveillant. Cette technique, offrant à l'attaquant une méthode fiable pour maintenir l'accès et exécuter des actions nuisibles, rend nécessaire une intervention rapide en cas de compromission.

Actions de remédiation

En cas d’alerte, il est recommandé de :

1. Suspendre ou désactiver immédiatement le service suspect pour empêcher toute exécution supplémentaire.
2. Analyser le script PowerShell ou les commandes associées pour comprendre l’intention et identifier les charges utiles potentielles.
3. Vérifier les permissions des utilisateurs ou des processus qui ont créé le service, pour voir si elles ont été abusées.
4. Renforcer les politiques de sécurité pour restreindre l'exécution de scripts PowerShell non autorisés.
5. Effectuer un audit complet de l'hôte pour vérifier la présence d'autres signes de compromission.

Faux-positifs

Des faux-positifs peuvent se produire si des administrateurs système installent des scripts PowerShell comme services pour des tâches de gestion ou d'automatisation. Ainsi, une validation avec les équipes IT est nécessaire pour déterminer si l'activité est légitime ou non.

Création de Tâche Planifiée Suspecte

Description

Cette règle détecte la création de tâches planifiées suspectes, utilisées très souvent pour maintenir un accès persistant sur un système compromis.

Classification MITRE ATT&CK

La règle "Création de tâche planifiée suspecte" est classée sous la matrice MITRE ATT&CK dans la catégorie Persistance (Persistence). Elle correspond à la technique T1053.005 (Scheduled Task/Job - Scheduled Task), car les tâches planifiées permettent de maintenir un accès persistant et d’exécuter des charges utiles de manière répétée ou à des moments précis.

Scénario d’attaque

Dans ce scénario, un attaquant ayant réussi à accéder à un système crée une tâche planifiée pour exécuter des commandes ou scripts malveillants à intervalles réguliers. Les emplacements ou programmes ciblés incluent souvent des répertoires vulnérables ou des outils connus pour exécuter du code de manière discrète, comme PowerShell, cmd.exe, ou d'autres binaires/exécutables utilisés à des fins malveillantes.

Technique de détection

La règle repose sur l'observation des événements Windows liés aux tâches planifiées. Elle cible spécifiquement l'Event Code 4698, qui indique la création d'une tâche. La règle extrait et analyse les chemins de scripts ou exécutables associés, en mettant en évidence les emplacements suspects comme AppData, Temp, ou les dossiers partagés. Des termes spécifiques comme powershell, cmd, et rundll32 sont utilisés pour identifier des tentatives d'exécution malveillante pour éviter de remonter les faux-positifs.

Priorité et niveau de sévérité

Le niveau de sévérité est élevé, car la création de tâches planifiées malveillantes peut permettre à un attaquant de maintenir un accès prolongé à un système, d'exécuter des commandes à volonté, et de s'assurer que son code malveillant reste opérationnel même après un redémarrage.

Actions de remédiation

En cas d'alerte, il est recommandé de :

1. Identifier la source de la tâche planifiée (compte utilisateur, processus, ou script) et suspendre l'exécution immédiate de la tâche.
2. Analyser les scripts ou fichiers exécutés pour comprendre leur but et rechercher d'autres traces d'activité malveillante.
3. Supprimer ou désactiver les tâches suspectes et renforcer les politiques de création de tâches planifiées.
4. Effectuer une analyse de l'hôte pour vérifier si d'autres signes de compromission existent et surveiller les événements similaires.

Faux-positifs

Des faux-positifs peuvent survenir si des administrateurs système créent des tâches planifiées dans des répertoires temporaires pour des raisons de maintenance ou d'automatisation. Cela peut aussi inclure des installations logicielles automatiques. Une vérification de la légitimité des tâches planifiées reste malgré tout nécessaire.

WEL:Security | Suspicious Access to Registry Keys

Description

Détecte plus de 3 accès non autorisés/suspects sur des clés de registre. Cette règle de détection permet d'identifier les tentatives d'accès suspectes aux clés de registre, qui peuvent signaler des comportements malveillants ou des tentatives d'indicateurs de compromission.

Classification MITRE ATT&CK

- **T1070.001 : Indicator Removal on Host** - Suppression ou modification d'indicateurs de compromission sur un hôte, souvent en accédant et en modifiant des clés de registre.

Scénario d'attaque

Un attaquant peut tenter d'accéder de manière répétée à des clés de registre sensibles pour extraire des informations critiques, modifier des paramètres système ou supprimer des indicateurs de compromission afin de masquer ses activités.

Technique de détection

Événement ciblé : **EventID 4663** (Tentative d'accès à un objet effectuée) + constater si sur une clé de registre (ObjectName), l'accès en lecture ('0x1') et écriture ('0x2') ont été accordés | Déclenchée au bout de 3 occurrences. Utilisation de WinEventLog:security.

Priorité et niveau de sévérité

Priorité : Élevée | Les accès non autorisés aux clés du registre peuvent signaler une compromission potentielle du système ou une tentative d'exfiltration d'informations sensibles.

Niveau de sévérité : High | Représente un risque significatif concernant les accès suspects aux clés du registre, qui peuvent permettre à un attaquant d'obtenir des informations sensibles ou d'altérer le fonctionnement normal du système.

Actions de remédiation

- Isoler immédiatement le système concerné du réseau
- Examiner les logs pour identifier d'autres activités suspectes
- Analyse antivirus complète du système
- Si l'accès est confirmé comme malveillant, modifier les clés affectées et restaurer les paramètres à partir d'une sauvegarde connue
- Renforcer les contrôles d'accès au registre et appliquer des mises à jour de sécurité

Faux-positifs

Les applications légitimes qui accèdent fréquemment aux clés du registre pour leur fonctionnement normal, comme les outils de gestion système ou les logiciels antivirus.

WEL:Security | Suspicious Changes to Sensitive Registry Keys

Description

Détecte plus de 5 modifications non autorisées/suspectes sur des clés de registre sensibles, comme la création ou la suppression. Cette règle de détection permet d'identifier les modifications suspectes apportées à des clés de registre critiques ; cela permet d'atténuer les risques et protéger l'intégrité du système.

Classification MITRE ATT&CK

- **T1112 : Modify Registry** - Modification des clés de registre pour masquer des activités malveillantes ou établir une persistance sur le système.

Scénario d'attaque

Un attaquant peut accéder à un système et modifier des clés de registre sensibles pour obtenir des informations sur les comptes utilisateurs, désactiver des mécanismes de sécurité ou maintenir un accès persistant au système.

Technique de détection

Événements ciblés : EventID 4657 (Tentative de modification d'un objet du registre a été effectuée) et EventID 4656 (Tentative d'accès à un objet a été effectuée) sur les clés de registres suivantes :

- "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" : Contient des paramètres de sécurité locaux
- "HKLM\SAM\SAM\Domains\Account\Users" : Stocke des informations sur les comptes utilisateurs
- "HKLM\SECURITY\Policy\Secrets" : Contient des secrets système sensibles
- "HKLM\SYSTEM\CurrentControlSet\Services" : Gère les services système

| Déclenchée au bout de 3 occurrences. Utilisation de WinEventLog:security.

Priorité et niveau de sévérité

Priorité : Élevée | Les modifications non autorisées aux clés du registre peuvent signaler une compromission potentielle du système, nécessitant une attention immédiate.

Niveau de sévérité : High | Représente un risque significatif associé aux modifications des clés sensibles, qui peuvent permettre à un attaquant d'obtenir un accès non autorisé ou d'altérer le fonctionnement normal du système.

Actions de remédiation

- Isoler immédiatement le système concerné du réseau
- Examiner les logs pour identifier d'autres activités suspectes
- Analyse antivirus complète du système
- Si les modifications sont confirmées comme malveillantes, restaurer les clés affectées à partir d'une sauvegarde
- Renforcer les contrôles d'accès au registre et appliquer des mises à jour de sécurité pour prévenir les futures compromissions

Faux-positifs

Les applications légitimes qui modifient fréquemment les clés du registre pour leur fonctionnement normal, comme les logiciels antivirus ou les outils de gestion système.

3. Compromission du système

Suspicious SQL Injection Attempt on Web

Description

Cette alerte est conçue pour détecter des requêtes web suspectes vers un serveur interne (IP : 192.168.10.21), qui peuvent indiquer des tentatives d'injection SQL

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Accès Initial	Exploitation d'une Application Publique	Les attaquants peuvent exploiter des vulnérabilités dans une application web en tentant d'injecter des commandes SQL malveillantes pour interagir directement avec une base de données..

Scénario d'Attaque

Reconnaissance : Un attaquant identifie un serveur web interne potentiellement vulnérable (tel qu'un système de gestion ou une interface d'administration).

Tentative d'Injection : En utilisant des commandes SQL spécifiques, l'attaquant envoie des requêtes HTTP au serveur cible. Ces requêtes contiennent des URLs ou des chaînes User-Agent inhabituelles, ainsi que des mots-clés SQL, pour exploiter une faiblesse potentielle de validation des entrées dans l'application.

Exfiltration Potentielle de Données : Si l'injection est réussie, l'attaquant peut accéder à la base de données, extraire des informations sensibles ou manipuler des données.

Technique de Détection

- **Type de Log** : Suricata

Méthode de Détection : La règle filtre les requêtes ayant :

- Des URLs dépassant 1024 caractères,
- Des User-Agent plus longs que 200 caractères,
- Des mots-clés SQL dans la requête (select, union, drop, insert, etc.).

Priorité et Niveau de Sévérité

- **Sévérité** : Élevée

Les attaques d'injection SQL peuvent entraîner des fuites de données, un accès non autorisé et une compromission du système

Actions de Remédiation

- **Réponse Immédiate** : Bloquer l'adresse IP source si elle est confirmée comme étant malveillante pour empêcher de nouvelles tentatives.
- Corriger les Vulnérabilités

Faux Positifs

Transferts de Données en Bloc : Certaines tâches administratives ou téléchargements/chargements automatiques de données peuvent inclure des URLs longues ou des volumes de données élevés.

Detection of Pass-the-Ticket Attack with Mimikatz

Description

Cette alerte détecte les tentatives d'attaques Pass-the-Ticket utilisant Mimikatz, un outil de post-exploitation populaire permettant l'extraction de crédentiels, la manipulation de tickets Kerberos, et l'escalade de privilèges

Classification - MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Credential Access	**T1003.006** - Dumping de crédentiels / DCSync, Pass-the-Ticket	Les attaquants cherchent à voler ou à injecter des tickets Kerberos pour se déplacer latéralement ou escalader des privilèges.
Mouvement latéral	**T1550.003** - Utilisation de matériel d'authentification alternatif / Pass-the-Ticket	Utilisation de tickets Kerberos volés pour accéder à d'autres ressources sans authentification supplémentaire.

Scénario d'Attaque

un attaquant obtient un accès initial à une machine cible, par exemple, par du phishing ou l'exploitation d'une vulnérabilité. Une fois dans le système, l'attaquant utilise Mimikatz pour extraire des tickets Kerberos depuis la mémoire, puis réutilise ces tickets volés pour se déplacer latéralement dans le réseau. Ce procédé permet à l'attaquant de se faire passer pour un utilisateur légitime, d'accéder à des ressources critiques et potentiellement d'escalader ses privilèges pour compromettre davantage le réseau

Technique de Détection

Source de Log : Windows Event Log (Sécurité et Sysmon)
Cette alerte identifie les patterns d'utilisation de Mimikatz dans le champ Process_Command_Line, en recherchant les commandes indiquant une extraction ou une injection de tickets Kerberos.
Des filtres sont appliqués pour ne détecter que les exécutions suspectes impliquant Mimikatz ou les commandes Kerberos liées au dumping et à l'injection de tickets.

Priorité et Niveau de Sévérité

Sévérité : High
Justification : Une attaque réussie Pass-the-Ticket permet à un attaquant de contourner les processus d'authentification, d'usurper l'identité d'utilisateurs légitimes et de se déplacer latéralement dans l'environnement. Cette menace est critique, car elle peut aboutir à une compromission complète du réseau.

Actions de Remédiation

- Isolation de la Machine Compromise
- Correction des Vulnérabilités
- Audit des Logs
- Réinitialisation et Rotation des Crédentiels

Faux Positifs :

L'utilisation de Mimikatz étant spécifiquement associée à des activités de compromission, cette alerte est conçue pour détecter uniquement des événements critiques et ne devrait normalement déclencher que des vrais positifs.

Accès Suspect aux Fichiers de Crédentiels SAM ou NTDS avec Esentutl

Description

L'alerte détecte l'utilisation de l'outil esentutl.exe pour accéder aux fichiers de crédentiels SAM et ntds.dit, situés dans le répertoire C:\Windows\System32\Config\. Ces fichiers contiennent des informations sensibles, notamment des hash de mots de passe pour les comptes d'utilisateurs locaux et Active Directory, qui peuvent être extraits pour des attaques de type *credential dumping*. Cette alerte est cruciale pour détecter une tentative d'escalade de privilèges et de mouvements latéraux potentiels.

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Credential Access	T1003 – OS Credential Dumping	L'attaque vise à extraire les hash de mots de passe stockés dans le SAM ou ntds.dit

		pour obtenir des privilèges supplémentaires.
Defense Evasion	T1070 – Indicator Removal on Host	Les attaquants peuvent également tenter de masquer leurs traces après extraction.

Scénario d'Attaque

Reconnaissance Préliminaire : L'attaquant obtient un accès initial à un hôte critique (tel qu'un contrôleur de domaine) en utilisant des identifiants compromis ou une vulnérabilité d'accès distant.
Escalade de Privilèges : En exécutant esentutl.exe avec des paramètres spécifiques, l'attaquant cherche à copier les fichiers SAM et ntds.dit dans un emplacement temporaire pour les extraire et les exploiter.
Mouvement Latéral : L'attaquant utilise ensuite les hash extraits pour obtenir des privilèges administratifs supplémentaires sur d'autres systèmes au sein du réseau.
Évasion Défensive : Après avoir extrait les informations, l'attaquant peut supprimer les logs ou masquer les traces de l'activité esentutl.exe pour éviter la détection.

Technique de détection

- **Type de Log** : Sysmon Event ID 1 (Processus Création)
La détection repose sur la capture des événements Sysmon qui enregistrent l'exécution de processus sur le système. Toute utilisation de esentutl.exe ciblant les fichiers SAM ou ntds.dit déclenche une alerte, car il s'agit d'un comportement anormal pour un processus système standard.

Priorité et Niveau de Sévérité

- Sévérité : Haute
- Justification : La compromission des fichiers de crédentiels SAM et NTDS peut donner un accès total au système. Si l'alerte est confirmée, il est essentiel de répondre rapidement pour éviter une compromission globale.

Action de Remédiation

- **Isolation de la Machine** : Isoler la machine pour éviter tout mouvement latéral potentiel.
- **Analyse du Processus** : Examiner les informations du processus parent et de la ligne de commande pour confirmer l'accès suspect.
- **Vérification des Crédentiels** : Valider les utilisateurs ayant initié l'accès et procéder à un changement des mots de passe si nécessaire.

Faux Positifs :

Opérations de Maintenance Légitimes : Les équipes d'administration peuvent exécuter esentutl.exe pour des sauvegardes, des récupérations, ou des audits de la base de données, surtout dans des environnements de test ou de développement. Ces activités peuvent sembler suspectes mais sont souvent justifiées dans un cadre opérationnel.

Tests de Sécurité et Audits : les équipes de sécurité peuvent volontairement accéder à ces fichiers dans le cadre de tests de vulnérabilité ou d'audits de sécurité réguliers.

Mise à jour ou Réinstallation de Composants Système : Lors de mises à jour de Windows ou de réparations système, certains processus légitimes peuvent également interagir avec les fichiers sensibles du système.

Metasploit SMB PsExec

Description

Cette règle identifie l'utilisation d'outils comme Metasploit et Impacket pour installer un service sur une machine cible via le protocole SMB.

Classification MITRE ATT&CK

La règle "Metasploit SMB PsExec" est classée sous la matrice MITRE ATT&CK dans la catégorie Mouvement Latéral (Lateral Movement). Elle correspond à la technique T1021.002 (Remote Services - SMB/Windows Admin Shares), utilisant les partages administratifs Windows pour exécuter des commandes ou des payloads à distance.

Scénario d'attaque

L'objectif principal de ce scénario pour un attaquant est : tirer parti du service SMB pour établir un point de pivot, permettant l'exécution de commandes à distance sur d'autres systèmes du réseau. En utilisant des outils comme Metasploit, l'attaquant peut déployer des payloads malveillants pour accéder et contrôler la machine compromise, par exemple en utilisant le module **psexec** de Metasploit. Impacket, de son côté, fournit des scripts comme psexec.py et wmiexec.py pour créer un service sur la cible, facilitant donc cette notion de remote control.

Technique de détection

La règle repose sur la détection de l'Event Code 4697, qui signale la création d'un nouveau service sur le système. Dans des emplacements plus spécifiques et dans un cadre plus général, nous maintenons avec cette règle une surveillance qui nous alerte à chaque services ajouter à ces endroits critiques (& détection des modifications de services pour alerter en cas de comportements suspects).

Priorité et niveau de sévérité

Le niveau de sévérité est élevé, car l'utilisation de SMB PsExec pour exécuter du code à distance peut entraîner un accès complet à un système et compromettre l'environnement. C'est un risque important nécessitant une réponse immédiate pour limiter la propagation de l'attaque.

Actions de remédiation

En cas d'alerte, il est recommandé de :

1. Isoler la machine cible pour empêcher tout mouvement latéral supplémentaire.
2. Vérifier et supprimer le service malveillant installé, ainsi que tous les processus ou payloads associés.
3. Auditer les connexions SMB et identifier l'origine de l'attaque pour contenir l'activité malveillante. - Ip de l'attaquant ?

4. Renforcer la sécurité des partages administratifs et désactiver l'accès SMB non essentiel.
5. Mettre en place des restrictions supplémentaires pour limiter la création de services par des utilisateurs non autorisés.

Faux-positifs

Des faux-positifs peuvent survenir lors de l'installation de logiciels légitimes qui créent des services via SMB pour des raisons administratives. Il faut donc bien analyser la source des logs avant d'engendrer une quelconque procédure.

Suppression des Logs de Sécurité

Description

Cette règle détecte la suppression des logs de sécurité, une action souvent entreprise par des attaquants pour masquer leur présence et compliquer les investigations.

Classification MITRE ATT&CK

La règle "Suppression des logs de sécurité" est classée sous la matrice MITRE ATT&CK dans la catégorie Évasion de la défense (Defense Evasion). Elle correspond à la technique T1070.001 (Indicator Removal on Host - Clear Windows Event Logs), car elle vise à effacer les preuves de l'activité malveillante en supprimant les journaux critiques.

Scénario d'attaque

Dans ce scénario, un attaquant ayant compromis un système utilise des privilèges élevés pour supprimer les logs de sécurité Windows. Cela peut arriver après l'exécution de commandes malveillantes, d'une élévation de privilèges, ou d'un mouvement latéral. L'objectif est de faire disparaître les traces de ses actions pour éviter la détection par les analystes SOC / équipes de sécurité.

Technique de détection

La règle repose sur la détection des événements 517 et 1102, qui sont respectivement associés à la suppression des journaux de sécurité et à la suppression des événements du journal Microsoft-Windows-Eventlog. L'analyse de l'utilisateur ou du processus initiant ces suppressions permet de déterminer si l'activité est légitime ou malveillante. Mais dans la majeure partie des scénarios, il est très peu probable que cet événement soit un faux-positif.

Priorité et niveau de sévérité

Le niveau de sévérité est critique, car la suppression des logs de sécurité indique souvent une tentative d'évasion de la détection. Une telle action justifie une réponse immédiate pour limiter les impacts d'une éventuelle compromission et pour enquêter sur les autres actions potentiellement malveillantes de l'attaquant.

Actions de remédiation

En cas d’alerte, il est recommandé de :

1. Identifier immédiatement l'origine de la suppression des journaux et d’isoler l’hôte pour empêcher toute autre activité.
2. Auditer les comptes administratifs et réinitialiser les identifiants si une compromission est suspectée.
3. Examiner d'autres systèmes connectés pour détecter une attaque potentiellement coordonnée.
4. Renforcer les politiques de journalisation pour s'assurer que les journaux sont protégés contre les suppressions non autorisées.
5. Effectuer une analyse complète de la sécurité de l'hôte pour évaluer l'étendue de la compromission.

Faux-positifs

Dans la majeure partie des scénarios, il est très peu probable que cet événement soit un faux-positif.

Suppression des Logs Système

Description

Cette règle détecte la suppression des journaux système, une action souvent entreprise pour couvrir des traces d'activités malveillantes.

Classification MITRE ATT&CK

La règle "Suppression des logs système" est classée sous la matrice MITRE ATT&CK dans la catégorie Évasion de la défense (Defense Evasion). Elle correspond à la technique T1070.001 (Indicator Removal on Host - Clear Windows Event Logs), car elle vise à supprimer des journaux de l'hôte pour dissimuler des preuves d'une compromission ou d'une activité malveillante.

Scénario d’attaque

Dans ce scénario, un attaquant ayant obtenu un accès administratif à une machine cible tente de supprimer les journaux système pour masquer ses actions. Cela peut inclure des tentatives d'élévation de privilèges, de mouvements latéraux, ou même des exfiltrations de données. En effaçant les traces de ses activités, l'attaquant complique les investigations et retarde la détection de la compromission.

Technique de détection

La règle repose sur l'analyse des logs de sécurité Windows. Elle se concentre sur l'Event Code 104, qui indique la suppression de journaux système. Les sources surveillées incluent des journaux critiques, tels que ceux de PowerShell, Sysmon, le journal de sécurité, et le journal système lui-même.

Priorité et niveau de sévérité

Le niveau de sévérité est critique, car la suppression des logs système peut indiquer que l'attaquant cherche activement à cacher ses traces, signalant une compromission avancée. Une réponse rapide est nécessaire.

Actions de remédiation

En cas d’alerte, il est impératif de :

1. Vérifier immédiatement l'activité de l'utilisateur ou du processus ayant initié la suppression.
2. Suspendre ou isoler l'hôte suspect pour empêcher toute action supplémentaire de l'attaquant.
3. Analyser l’ensemble des machines sur le réseau pour identifier d’autres signes de compromission.
4. Restaurer les journaux effacés si possible, pour mener à bien l’enquête.
5. Réviser les politiques de journalisation pour assurer que les journaux critiques sont correctement protégés.

Faux-positifs

Des faux-positifs peuvent se produire, même si très peu probable, dans un contexte où un administrateur effectue une maintenance régulière où il efface les journaux de manière légitime. Cela peut inclure des opérations de routine visant à libérer de l'espace disque. Pour atténuer ce risque, il est essentiel de vérifier si la suppression des journaux est conforme aux pratiques et horaires d'administration autorisés.

Utilisation Suspecte de l’Outil addinutil.exe

Description

Cette alerte vise à détecter toute exécution inhabituelle de l’outil addinutil.exe dans l'environnement Windows. Cet exécutable, destiné au fonctionnement et la mise à jour de plugins pour Microsoft Office, ne démarre pas en dehors d’un contexte Office. Une exécution imprévue de addinutil.exe pourrait indiquer une tentative de contournement des contrôles de sécurité pour installer des extensions malveillantes ou établir une connexion illégitime, en vue d’orchestrer une attaque.

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Exécution	T1218 – System Binary Proxy Execution	En utilisant addinutil.exe, l’attaquant peut exécuter des actions malveillantes tout en se cachant derrière des processus signés par Microsoft, rendant la détection plus complexe pour les solutions de sécurité qui se fient à la réputation des exécutables

Scénario d’Attaque

Accès initial : Un attaquant obtient un accès de base à une machine dans le réseau, via des identifiants compromis ou une faille de sécurité. Il arrive à charger un fichier .dll malveillant sur le/les postes auxquels il a accès.

Exploitation de addinutil.exe : L'attaquant utilise par exemple la commande: *addinutil.exe /i "C:\path\to\malicious\addin.dll"* pour installer discrètement son .dll malveillants, en abusant de la légitimité de addinutil.exe.

Persistance et Évasion de Détection : Une fois les extensions installées, l'attaquant peut maintenir un accès au système avec un risque minimal de détection, en raison de l'usage d'un outil système légitime. Il peut ensuite utiliser ce point d'entrée pour exécuter des commandes malveillantes ou installer des composants supplémentaires sans déclencher les alarmes de sécurité.

Technique de Détection

- **Type de Log** : Sysmon Event ID 1 (Création de Processus)
    - Cette détection repose sur les logs Sysmon, notamment l'Event ID 1, qui enregistre chaque création de processus. Toute exécution de addinutil.exe en dehors des opérations légitimes d'administration peut déclencher cette alerte. L'utilisation de l'outil pour des activités non planifiées ou par des comptes non administratifs est considérée comme suspecte.

Priorité et Niveau de Sévérité

- **Sévérité** : Medium à High
- **Justification** : Bien que addinutil.exe soit un binaire légitime, son usage inhabituel doit être surveillé de près. En cas de compromission, cet outil peut être utilisé pour installer des composants non autorisés, compromettant potentiellement la sécurité du système et facilitant une attaque plus large. Si cette alerte est confirmée, il est essentiel de réagir rapidement pour contenir les risques.

Actions de Remédiation

- **Analyse des Logs** : Identifier le contexte et l'utilisateur qui a lancé addinutil.exe. Examiner les logs Sysmon pour détecter d'autres signes d'activité suspecte.
- **Isolation de la Machine** : Si une activité malveillante est confirmée, isoler la machine pour éviter une propagation latérale.
- **Examen des Permissions** : Vérifier les permissions et les privilèges de l'utilisateur ayant lancé l'exécution de addinutil.exe.
- **Audit des Plugins/Extensions** : Si des composants additionnels sont identifiés, procéder à une analyse complète pour identifier les fichiers installés et leurs potentiels impacts.

Faux Positifs

- **Déploiements d'Extensions Légitimes** : Les équipes de développement peuvent utiliser addinutil.exe dans le cadre d'installations ou de mises à jour de plugins .NET, en particulier dans des environnements de test ou de développement.

- **Mises à jour de Composants** : Dans certains cas, des mises à jour du système ou des tâches de maintenance peuvent exiger l'utilisation de addinutil.exe. Ces opérations devraient être documentées pour éviter des alertes inutiles.
- **Tests de Sécurité et Audits** : Les équipes de sécurité peuvent également utiliser cet exécutable dans le cadre de vérifications de sécurité ou d'audits. Il est recommandé de coordonner ces activités avec les équipes concernées pour réduire les faux positifs.

4. Reconnaissance Active Directory (AD)

Détection de Tickets Kerberos avec Chiffrement Faible

Description

Cette alerte surveille les demandes TGS (Ticket Granting Service) pour des comptes de service critiques en se concentrant particulièrement sur les tickets utilisant des types de chiffrement faibles (ex. : 0x1, 0x3, 0x17). L'utilisation de chiffrement faible facilite le décryptage des tickets et rend les informations sensibles plus vulnérables à des attaques de type Kerberoasting

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Credential Access	T1003.006 - Dumping de crédentiels / DCSync, Pass-the-Ticket	L'attaque vise à extraire les hash de mots de passe depuis des tickets TGS pour accéder aux informations d'identifiants.
Mouvement latéral	T1558 - Kerberos Abuse	L'utilisation de tickets TGS compromis permet d'accéder à des comptes de service sensibles et d'obtenir des privilèges accrus

Scénario d'Attaque

Reconnaissance Interne : L'attaquant identifie les comptes de service critiques dans l'environnement cible.

Demande de Tickets TGS avec Chiffrement Faible : L'attaquant envoie des requêtes TGS spécifiquement pour des comptes de service avec des tickets à chiffrement faible (0x1, 0x3, 0x17), facilitant la compromission des données.

Extraction des Hashes : L'attaquant utilise les tickets extraits pour obtenir les hash de mots de passe, ciblant spécifiquement ceux qui sont plus faciles à déchiffrer.

Escalade de Privilèges et Mouvement Latéral : En exploitant les identifiants extraits, l'attaquant accède à d'autres systèmes et ressources critiques dans le réseau pour une compromission plus large.

Technique de Détection

Type de Log : Windows Security Event Log (EventCode 4769 - Service Ticket Request)

La détection repose sur l'identification de tickets TGS à chiffrement faible, qui sont plus vulnérables aux attaques de type Kerberoasting. Un nombre élevé de requêtes pour des comptes de service avec ce type de chiffrement est un indicateur de risque

Priorité et Niveau de Sévérité

Sévérité : Élevée

Justification : La compromission de tickets Kerberos par des chiffrements faibles pourrait permettre une escalade de privilèges généralisée et un accès non autorisé à des systèmes critiques.

Actions de Remédiation

- **Isolation de la Machine**
- **Vérification des Crédentiels** : Analysez les logs Kerberos pour déterminer l'étendue de la compromission. Envisagez de réinitialiser les mots de passe des utilisateurs compromis.
- **Audit et Durcissement des Configurations Kerberos** : Désactivez ou limitez l'utilisation de types de chiffrement faibles dans les configurations Kerberos. Renforcez les politiques de chiffrement pour limiter les risques futurs.

Faux Positifs

- **Usage Légitime** : Certaines configurations peuvent légitimement utiliser des types de chiffrement faibles pour des raisons de compatibilité. Validez avec les équipes d'administration si ces activités sont justifiées.

Backdoors Active Directory

Description

Cette règle détecte la présence de backdoors créés dans Active Directory en modifiant des attributs d'utilisateur pour maintenir un accès persistant et non autorisé.

Classification MITRE ATT&CK

La règle "Backdoors Active Directory" est classée sous la matrice MITRE ATT&CK dans la catégorie Persistance (Persistence) et Évasion de la défense (Defense Evasion). Elle correspond aux techniques T1098.002 (Account Manipulation - Domain Accounts) et T1078.002 (Valid Accounts - Domain Accounts), car elle se concentre sur la modification des attributs de comptes dans Active Directory pour maintenir l'accès.

Scénario d’attaque

Dans ce scénario, un attaquant ayant obtenu des privilèges suffisants dans Active Directory modifie des attributs comme msDS-AllowedToDelegateTo ou servicePrincipalName. Cela lui permet de contrôler certains aspects de la délégation ou de l'authentification au sein du domaine. De telles modifications sont difficiles à détecter, car elles exploitent des fonctionnalités légitimes d'AD, mais peuvent avoir des conséquences désastreuses si elles sont malveillantes.

Technique de détection

La règle repose sur la détection de l'Event Code 4738, indiquant la *modification des attributs des comptes utilisateurs*, et de l'Event Code 5136, pour les modifications d'objets dans Active Directory. Les attributs surveillés incluent *msDS-AllowedToDelegateTo*, *user*, et *msDS-AllowedToActOnBehalfOfOtherIdentity*. L'analyse de ces événements permet d'identifier des activités potentiellement suspectes et de mettre en évidence les modifications non autorisées.

Priorité et niveau de sévérité

Le niveau de sévérité est élevé, car les backdoors dans Active Directory peuvent permettre un accès persistant à des ressources critiques, compromettant la sécurité de l'ensemble du domaine.

Actions de remédiation

En cas d’alerte, il est recommandé de :

1. Vérifier les modifications apportées aux attributs des comptes et identifier si elles ont été autorisées ou effectuées par un acteur malveillant.
2. Révoquer les modifications suspectes des attributs et renforcer les permissions des comptes administratifs.
3. Auditer les contrôles de sécurité et les journaux d'AD pour s'assurer qu'il n'y a pas d'autres backdoors ou altérations.
4. Mettre en place une surveillance continue des modifications de schéma et d'attributs critiques dans Active Directory.
5. Envisager de restreindre les privilèges d'administration pour limiter l'impact potentiel d'une compromission.

Faux-positifs

Des faux-positifs peuvent survenir si des administrateurs modifient intentionnellement ces attributs pour des configurations ou déploiements spécifiques. Une vérification auprès des équipes responsables de la gestion d'Active Directory est essentielle.

Tentative de Compromission Overpass-the-Hash

Description

Cette règle détecte les tentatives de compromission de comptes via l'attaque overpass-the-hash, qui permet à un attaquant d'utiliser un hash NTLM pour s'authentifier sans connaître le mot de passe en clair.

Classification MITRE ATT&CK

La règle "Tentative de compromission Overpass-the-Hash" est classée sous la matrice MITRE ATT&CK dans la catégorie Accès aux informations d'identification (Credential Access) et Mouvement Latéral (Lateral Movement). Elle correspond à la technique T1550.002 (Use Alternate Authentication Material - Pass the Hash), car l'attaquant utilise un hash volé pour s'authentifier et accéder à d'autres ressources.

Scénario d'attaque

Dans ce scénario, un attaquant ayant compromis un système parvient à extraire des hashes NTLM (protocole d'authentification) stockés en mémoire. Il utilise ces hashes pour s'authentifier sur d'autres systèmes du réseau sans avoir besoin des mots de passe en clair, ce qui lui permet de contourner les mécanismes d'authentification standards et de se déplacer latéralement dans l'infrastructure.

Technique de détection

La règle repose sur la surveillance des événements Windows liés aux connexions suspectes. Elle se base sur l'Event Code 4624, qui enregistre les tentatives de connexion, et spécifiquement sur les connexions de type Logon_Type=9 avec le processus seclogon (processus seclogon) et le package d'authentification Negotiate (package qui choisit automatiquement entre NTLM et Kerberos pour l'authentification).

Priorité et niveau de sévérité

Le niveau de sévérité est élevé, car cette technique d'attaque permet à un acteur malveillant de s'authentifier et de se déplacer latéralement dans l'environnement.

Actions de remédiation

En cas d'alerte, il est recommandé de :

1. Isoler le système compromis pour empêcher tout mouvement latéral supplémentaire.
2. Réinitialiser les identifiants des comptes touchés pour invalider les hashes volés.
3. Auditer les systèmes voisins pour détecter d'autres signes de compromission.
4. Appliquer des stratégies de sécurité avancées, telles que la restriction des ports et des services SMB et l'activation de l'authentification Kerberos uniquement.
5. Mettre en place des mesures pour protéger les informations d'identification en mémoire, comme l'utilisation de Credential Guard.

Faux-positifs

Des faux-positifs peuvent se produire lors de configurations spécifiques d'authentification ou de scripts de surveillance réseau. Une évaluation manuelle des connexions suspectes est nécessaire pour différencier une activité légitime d'une attaque potentielle. Même si ce scénario de faux-positifs reste bien moins probable.

Accès Suspect aux Fichiers Sensibles de Stratégies de Groupe dans SYSVOL

Description

Cette alerte détecte les tentatives d'accès à des fichiers sensibles situés dans le dossier SYSVOL, sous le répertoire des stratégies (Policies). Ce dossier contient des fichiers de configuration critiques pour les stratégies de groupe Windows, comme audit.csv, Files.xml, GptTmpl.inf, et d'autres fichiers utilisés pour gérer les paramètres de sécurité et les configurations du domaine. Un accès non autorisé ou suspect à ces fichiers pourrait indiquer une tentative de compromission visant à modifier les stratégies de groupe, permettant potentiellement une escalade de privilèges ou une altération des configurations de sécurité dans le domaine.

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Defense Evasion, Privilege Escalation	**T1484.001** – Domain Policy Modification: Group Policy **T1003** – OS Credential Dumping (si les modifications visent à exposer des informations d'identification)	Un attaquant ayant accès aux fichiers de stratégie de groupe pourrait modifier les configurations de sécurité, désactiver certains contrôles ou ajouter des paramètres qui facilitent l'exfiltration de données ou la persistance. En accédant aux fichiers SYSVOL et Policies, il peut préparer des modifications qui affectent tous les utilisateurs et machines d'un domaine.

Scénario d'Attaque

- **Initialisation** : Un attaquant obtient un accès initial à un système dans le domaine Windows, potentiellement en utilisant un compte compromis ou des vulnérabilités.
- **Accès aux Fichiers de Stratégies** : L'attaquant accède aux fichiers sensibles dans le dossier SYSVOL\Policies, tels que audit.csv, Registry.pol, et autres, afin de comprendre ou de modifier les configurations de sécurité du domaine.

- **Modification des Stratégies** : En modifiant certains de ces fichiers, l'attaquant peut désactiver des journaux de sécurité, introduire des tâches planifiées malveillantes, ou injecter des scripts qui lui accordent un contrôle persistant sur le domaine.
- **Mouvement Latéral et Persistance** : Avec des configurations de groupe modifiées, l'attaquant peut utiliser ses nouveaux privilèges pour se déplacer latéralement dans le réseau ou maintenir un accès continu.

Technique de Détection

- **Type de Log** : Windows Event Logs
    - La détection repose sur l'analyse des événements Windows enregistrant les accès aux fichiers spécifiques dans SYSVOL\Policies. L'alerte est déclenchée lorsque des processus inhabituels (ne faisant pas partie des chemins de programme ou de système autorisés) accèdent à ces fichiers sensibles, signalant ainsi une activité potentiellement suspecte.

Priorité et Niveau de Sévérité

- **Sévérité** : High
- **Justification** : La compromission des fichiers de stratégie de groupe SYSVOL peut affecter l'ensemble du domaine Active Directory. En altérant les fichiers de configuration du domaine, l'attaquant pourrait influencer des politiques de sécurité essentielles, menant potentiellement à une compromission complète du réseau. Une réponse rapide est cruciale pour éviter des impacts majeurs.

Actions de Remédiation

- **Isolation du Système** : Si l'accès suspect est confirmé, isolez immédiatement la machine compromise pour empêcher d'autres modifications aux fichiers de stratégie de groupe.
- **Analyse des Modifications de Stratégie de Groupe** : Comparez les fichiers de configuration actuels avec une sauvegarde pour identifier toute modification non autorisée. Si des altérations sont détectées, restaurez les paramètres de sécurité à leur état antérieur.
- **Audit des Comptes Utilisateurs et des Permissions** : Revoyez les permissions des utilisateurs et des processus accédant au dossier SYSVOL\Policies pour identifier et restreindre les accès non autorisés.
- **Surveillance Renforcée des Stratégies** : Mettez en place une surveillance plus stricte des fichiers SYSVOL\Policies pour détecter toute modification future non autorisée.
- **Rotation des Identifiants** : Si un compte utilisateur légitime a été compromis, effectuez immédiatement une rotation des identifiants pour éviter une nouvelle exploitation.

Faux Positifs

- **Activités de Maintenance Systèmes** : Dans certains environnements, les administrateurs peuvent accéder aux fichiers SYSVOL\Policies pour des maintenances ou des audits réguliers. Ces accès doivent être documentés et ne pas générer d'alertes.
- **Mises à Jour et Configurations Légitimes** : Les mises à jour de logiciels de sécurité ou de configuration peuvent également entraîner des accès à ces fichiers par des processus légitimes. Une liste blanche de ces processus et activités peut réduire les faux positifs.

- **Outils de Supervision et d'Audit** : Certaines solutions de gestion de configurations et de sécurité peuvent interagir avec ces fichiers pour des audits ou des mises à jour de stratégie. Assurez-vous que ces outils sont identifiés dans les exclusions pour éviter des alertes non pertinentes.

5. Exfiltration de Données

Suricata | SRV-PRD-... made connections to malicious IPs addresses

Description

Détecte les connexions effectuées par SRV-PRD-... (-DC, -WEB, -DB, -SHARE) vers des adresses IP malveillantes en se basant sur une liste générée automatiquement ajoutée en tant que "lookup table". Cette règle de détection permet d'identifier toute tentative de communication entre les serveurs de production et des infrastructures potentiellement malveillantes, ce qui pourrait indiquer une compromission du système ou une tentative d'exfiltration de données.

Classification MITRE ATT&CK

- **T1071.001 : Application Layer Protocol: Web Protocols -** Utilisation de protocoles web pour établir des communications.
- **T1071.004 : Application Layer Protocol: DNS** - Utilisation du DNS pour la communication avec des serveurs de commande et de contrôle.
- **T1071 : Command and Control** - Techniques générales utilisées pour établir des communications C2.
- **T1105 : Ingress Tool Transfer** - Transfert d'outils depuis un adversaire vers un environnement compromis.

Scénario d'attaque

Après avoir obtenu l'accès initial à un des serveurs, l'attaquant peut établir une connexion avec son infrastructure de commande et contrôle (C2) pour maintenir sa présence, exfiltrer des données ou télécharger des outils supplémentaires.

Technique de détection

- **Sélection d'adresses IP sources** afin de surveiller les connexions sortantes des adresses IP liés aux serveurs SRV-PRD
- **Vérification de l'adresse IP** de destination dans le lookup table "malicious-ips.csv"
- **Exclusion** pour 93.184.221.240 + flowbit "ET.INFO.WindowsUpdate"
  Utilisation de Suricata.

Priorité et niveau de sévérité

Priorité : Élevée | Toute connexion vers une adresse IP malveillante peut signaler une compromission potentielle du système.

Niveau de sévérité : High | Représente un risque significatif que représente toute communication avec des infrastructures malveillantes, pouvant entraîner des violations de données ou l'installation de logiciels malveillants.

Actions de remédiation

- Isoler immédiatement le serveur concerné du réseau
- Analyser le trafic réseau pour identifier l'étendue ainsi que la nature des connexions suspectes.
- Examiner les logs pour déterminer comment l'accès à l'adresse IP malveillante a été établi
- Analyse complète du système à la recherche de malware ou d'autres compromissions
- Renforcer les règles de pare-feu et appliquer des mises à jour de sécurité sur tous les systèmes concernés

Faux-positifs

Activités normales liées à des mises à jour logicielles ou à des communications avec des serveurs externes qui sont temporairement sur la liste noire.

Utilisation Suspecte d'un Pipe pour de l'exfiltration de la donnée

Description

Cette alerte vise à détecter les accès non autorisés au pipe \\MICROSOFT##WID\\tsql\\query. Ce pipe fait en effet partie d'un mécanisme de communication inter-processus (IPC, Inter-Process Communication) utilisé par SQL Server pour faciliter les échanges entre différents processus ou services. L'accès à ce pipe est généralement réservé aux processus systèmes et services de confiance, comme svchost.exe ou sqlservr.exe. Toute tentative d'accès par un autre processus pourrait indiquer une tentative d'accès non autorisé, une possible escalade de privilèges ou une exploitation malveillante pour extraire des informations sensibles de la base de données.

Classification MITRE ATT&CK

Tactic	Technique/Sub-Technique	Description
Credential Access, Discovery	**T1078** – Valid Accounts **T1083** – File and Directory Discovery **T1003** – OS Credential Dumping (lorsque le pipe est utilisé pour obtenir des informations sensibles)	Les attaquants peuvent essayer d'accéder à \\MICROSOFT##WID\\tsql\\query pour interagir avec des bases de données WID dans le but d'exfiltrer des informations sensibles ou de découvrir des configurations système. Cette technique est souvent utilisée pour contourner les permissions et accéder à des données critiques, comme les configurations de services d'annuaire ou les credentials stockés.

Scénario d'Attaque

1. **Préparation** : Un attaquant obtient un accès initial au système via des identifiants volés ou une vulnérabilité exploitée sur le serveur.
2. **Accès au Pipe** : En tentant d'accéder au pipe \\MICROSOFT##WID\\tsql\\query, l'attaquant essaie de lire ou manipuler des données de la base WID pour obtenir des informations sensibles.
3. **Exploitation de l'Information** : Si l'attaque est réussie, les informations obtenues peuvent inclure des configurations de système, des comptes d'administration ou même des hash de mots de passe, utilisés pour étendre leur accès à d'autres systèmes dans le réseau.
4. **Mouvement Latéral** : Une fois en possession de ces informations, l'attaquant pourrait se déplacer latéralement vers d'autres systèmes ou élever ses privilèges en utilisant des informations obtenues.

Technique de Détection

- **Type de Log** : Événements Windows (ID Sysmon correspondant aux accès de pipe nommés)
    - La détection repose sur les événements capturés par Sysmon ou les logs Windows Event pour les accès au pipe. Toute tentative d'accéder à \\MICROSOFT##WID\\tsql\\query par un processus non autorisé (autre que mmc.exe, svchost.exe, sqlwriter.exe, etc.) déclenchera une alerte. Ce comportement est considéré comme suspect et pourrait être le signe d'une activité malveillante.

Priorité et Niveau de Sévérité

- **Sévérité** : High
- **Justification** : L'accès non autorisé aux bases de données internes de Windows peut permettre une compromission majeure du système. Si cette alerte est déclenchée, il est impératif de réagir rapidement pour empêcher une potentielle exfiltration de données sensibles ou une escalade de privilèges.

Actions de Remédiation

- **Vérification des Processus** : Identifier le processus ayant initié l'accès au pipe et vérifier son chemin et son contexte d'exécution pour confirmer ou infirmer sa légitimité.
- **Isolation de la Machine** : En cas de compromission avérée, isoler la machine affectée pour limiter la propagation.
- **Audit des Permissions** : Examiner les permissions et privilèges des comptes d'utilisateurs actifs sur la machine pour identifier une potentielle élévation de privilèges.
- **Changement des Credentials Sensibles** : Si des informations d'identification sensibles ont pu être exposées, procéder immédiatement au changement des mots de passe et renforcer les politiques de sécurité.

Faux Positifs

- **Tâches de Maintenance et Sauvegarde** : Les administrateurs système peuvent accéder légitimement à \\MICROSOFT##WID\\tsql\\query lors de tâches de maintenance, de mises à jour ou de sauvegardes. Ces accès devraient être documentés pour éviter des alertes inutiles.
- **Scripts de Supervision** : Certains scripts ou outils de monitoring peuvent interagir avec les bases de données WID à des fins d'audit. Il est recommandé de vérifier si les équipes de supervision utilisent des outils qui pourraient déclencher cette alerte.

- **Tests de Sécurité** : Les équipes de sécurité effectuant des audits peuvent également accéder à ce pipe pour des vérifications de conformité. Assurer une communication adéquate avec ces équipes pour réduire le risque de faux positifs.

6. Mouvement Latéral

Connexion à une Ressource Partagée

Description

Cette règle détecte les connexions suspectes à des ressources partagées sur le réseau, en particulier celles qui pourraient signaler l'accès anonyme aux partages administratifs.

NB : Une autre règle nommée “Accès à un Objet de Partage Réseau” et moins restrictif a également été créée. A la différence de celle-ci, elle a une priorité low car elle peut remonter beaucoup de faux-positifs.

Classification MITRE ATT&CK

La règle "Connexion à une ressource partagée" est classée sous la matrice MITRE ATT&CK dans la catégorie Mouvement Latéral (Lateral Movement). Elle correspond à la technique T1021.002 (Remote Services - SMB/Windows Admin Shares), car elle implique l'utilisation de services distants, comme SMB, pour accéder aux ressources partagées dans un environnement Windows.

Scénario d’attaque

Dans ce scénario, un attaquant utilise des connexions SMB pour accéder aux ressources partagées sur un hôte, ce qui peut être une étape préparatoire pour exfiltrer des données, déployer des charges utiles malveillantes, ou obtenir des informations sensibles. Les connexions anonymes (ANONYMOUS LOGON) ou les accès à des partages administratifs comme \\IPC$ sont des indicateurs typiques de tentatives de compromission.

Technique de détection

La règle repose sur la détection de l'Event Code 5150, qui enregistre les tentatives de connexion à des ressources partagées. Elle surveille les partages \\IPC$ et les connexions effectuées avec des comptes anonymes. L'analyse de ces événements permet de détecter des activités suspectes indiquant une compromission ou une reconnaissance active.

Priorité et niveau de sévérité

Le niveau de sévérité est moyen, car bien que certaines connexions puissent être légitimes, des accès anormaux ou anonymes à des ressources partagées peuvent signaler des tentatives de reconnaissance ou de déplacement latéral.

Actions de remédiation

En cas d’alerte, il est recommandé de :

1. Vérifier l'activité de l'utilisateur ou du processus ayant initié la connexion pour évaluer sa légitimité.
2. Restreindre l'accès aux partages administratifs et limiter les connexions anonymes.
3. Analyser les journaux réseau pour détecter d'autres tentatives d'accès suspectes ou des modèles d'attaque.
4. Configurer des politiques de sécurité pour restreindre l'utilisation de SMB et protéger les ressources critiques.
5. Mettre en place un monitoring avancé des partages réseau pour détecter les activités anormales en temps réel.

Faux-positifs

Des faux-positifs peuvent se produire en raison de scripts d'administration légitimes ou de tâches de maintenance qui utilisent des connexions SMB.

Surveillance des Connexions SSH Externes Suspectes via le Processus sshd

Description

Cette alarme détecte des connexions SSH provenant de sources non légitimes. On se base sur l'adresse du segment réseau pour identifier une source légitime. Une alerte est générée quand les adresses sources des connexions ne sont pas dans les plages prédéfinies et autorisées.

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Lateral Movement, Initial Access	**T1021.004** – Remote Services: SSH **T1078** – Valid Accounts (si un compte légitime est compromis)	Les attaquants peuvent utiliser SSH pour établir des connexions distantes vers un système compromis, facilitant ainsi le déplacement latéral ou l'accès initial. Si un système écoute pour des connexions SSH et que les adresses IP de connexion sont externes ou non autorisées, cela pourrait indiquer une activité suspecte visant à exploiter des identifiants valides pour accéder au réseau.

Scénario d'Attaque

- **Préparation Initiale** : Un attaquant peut avoir obtenu un accès initial à un système via des identifiants compromis ou une vulnérabilité. Ce système est configuré pour écouter sur le port SSH (sshd) afin d'accepter des connexions.
- **Connexion Externe** : L'attaquant utilise SSH pour établir une connexion externe. La plage d'adresses IP externe est détectée, car elle ne correspond pas aux plages IP internes autorisées (par exemple, 192.168.10.*, 10.100.0.*, 192.168.20.*).
- **Command & Control (C2)** : Une fois connecté, l'attaquant pourrait exécuter des commandes à distance, exfiltrer des données sensibles, ou configurer d'autres outils de persistance.
- **Mouvement Latéral** : Si l'accès initial est réussi, l'attaquant pourrait l'utiliser pour se déplacer latéralement dans le réseau en accédant à d'autres hôtes via SSH.

Technique de Détection

- **Type de Log** : Événement Windows (Event ID 4)
    - La détection repose sur l'analyse des logs Windows Event (Event ID 4), où le processus sshd met en écoute un serveur SSH. Le payload "Server listening on *" indique que sshd est prêt pour une connexion. Toute connexion d'une IP externe (en dehors des plages autorisées) déclenchera cette alerte.

Priorité et Niveau de Sévérité

- **Sévérité** : High
- **Justification** : L'accès non autorisé par SSH à partir d'adresses IP externes est un indicateur d'une possible tentative d'intrusion ou de compromission. SSH est couramment utilisé pour des connexions sécurisées, mais une écoute non autorisée peut indiquer une prise de contrôle potentielle d'un point d'accès critique. Une réponse rapide est essentielle pour prévenir l'accès non autorisé ou le mouvement latéral dans le réseau.

Actions de Remédiation

- **Isolation du Système** : En cas de confirmation d'une activité suspecte, isoler la machine concernée pour empêcher toute connexion supplémentaire par SSH.
- **Vérification des Comptes Utilisés** : Analyser les comptes utilisateurs ayant initié les connexions SSH, vérifier leur origine et les activités associées pour déterminer si des comptes ont été compromis.
- **Audit des Règles de Pare-feu** : Examiner les règles de pare-feu pour limiter l'accès SSH aux plages IP internes uniquement, afin de prévenir de futures tentatives de connexion non autorisées.
- **Surveillance des Activités Connexes** : Mettre en place une surveillance renforcée des connexions SSH sur l'ensemble du réseau, pour détecter d'autres éventuelles tentatives de connexion externe.
- **Rotation des Credentials** : Si un compte d'accès est compromis, procéder immédiatement à la rotation des credentials associés et renforcer les politiques d'authentification (par exemple, en imposant une authentification multi-facteur).

Faux Positifs

- **Maintenance ou Configuration Système** : Dans certains cas, les administrateurs peuvent temporairement activer SSH pour effectuer des maintenances distantes. Ces accès devraient être prévus et documentés pour éviter de générer des faux positifs.
- **Tests de Sécurité et Audits** : Les équipes de sécurité ou de conformité peuvent déclencher cette alerte en accédant à distance via SSH pour des vérifications de sécurité. Il est recommandé de synchroniser les activités de test pour éviter de fausses alertes.
- **Automatisation de Scripts de Surveillance** : Certains scripts de monitoring automatisés peuvent initier des connexions SSH externes pour superviser les systèmes. Assurez-vous que ces scripts sont bien documentés et que leurs adresses IP sont incluses dans les plages IP autorisées.

7. Evasion de Défense

Tentative de modification des paramètres de sécurité du registre SAM

Description

Cette alerte détecte les tentatives de modification des paramètres critiques du registre Windows liés aux restrictions d'accès à la base de données SAM, qui contient des informations sensibles sur les comptes et identifiants des utilisateurs. La clé de registre

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Accès aux informations d'identification	T1003.002 – Extraction d'identifiants OS (SAM)	L'attaque vise à extraire les hachages de mots de passe stockés dans le SAM pour obtenir des privilèges supplémentaires.
Defense Evasion	T1070 – Masquage d'indicateurs sur l'hôte	Les attaquants peuvent également tenter de masquer leur activité en nettoyant les logs ou en cachant leur accès.

Scénario d'Attaque

Un attaquant cherche à élever ses privilèges en modifiant une clé de registre critique, contournant ainsi les restrictions d'accès aux informations d'identification du SAM. Pour masquer son activité, il nettoie les journaux et évite les processus suspects. Finalement, il utilise les informations collectées pour se déplacer latéralement dans le réseau, compromettant d'autres systèmes et augmentant les risques pour l'infrastructure globale.

Technique de Détection

Type de Log : Sysmon Event ID 13 (Modification de valeur du registre)

La détection repose sur l'analyse des événements du registre capturés par Sysmon. L'alerte se déclenche dès qu'un processus non autorisé modifie cette clé de registre sensible.

Priorité et Niveau de Sévérité

Sévérité : Haute

La modification de cette clé de registre peut permettre à l'attaquant d'accéder aux hachages des mots de passe, augmentant considérablement le risque de compromission du réseau.

Actions de Remédiation

- **Isolation de la Machine** : Isoler la machine compromise pour empêcher tout mouvement latéral.
- **Vérification des Modifications du Registre** : Confirmer toute modification apportée à la clé en consultant les logs Sysmon.
- **Réinitialisation des Identifiants** : Changer les mots de passe des comptes sensibles si des informations d'identification ont pu être exposées.
- **Renforcement des Politiques d'Audit** : S'assurer que l'audit des modifications de registre est activé et que les alertes sont bien configurées pour détecter toute action suspecte.

Faux Positifs

Les faux positifs peuvent provenir d'opérations de maintenance légitimes, notamment des actions menées par les administrateurs dans des environnements de test ou lors d'opérations de sécurité planifiées

Tentative d'Accès Non Autorisé aux Fichiers de Sécurité SAM, SYSTEM, et SECURITY

Description

Cette alerte détecte les tentatives d'accès non autorisé aux fichiers de sécurité critiques de Windows, notamment les fichiers SAM, SYSTEM et SECURITY, situés dans le répertoire C:\Windows\System32\Config

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Credential Access	T1003.002 – OS Credential Dumping	L'attaquant cherche à extraire des hachages de mots de passe stockés dans les fichiers SAM ou SYSTEM pour obtenir des privilèges supplémentaires.
Defense Evasion	T1070.004 – Indicator Removal on Host	Les attaquants peuvent également tenter de masquer leurs traces après extraction.

Scénario d'attaque :

un attaquant accède à une machine cible, souvent par phishing ou en exploitant une vulnérabilité. Il escalade ensuite ses privilèges pour accéder aux fichiers SAM ou SYSTEM dans le répertoire de configuration de Windows, cherchant à extraire les hachages de mots de passe. Pour éviter la détection, il efface les journaux d'audit. Avec les identifiants récupérés, il peut se déplacer latéralement dans le réseau et accéder à d'autres systèmes ou augmenter ses privilèges, ce qui compromet la sécurité globale de l'infrastructure.

Technique de Détection

Type de Log : Windows Security Event Log, Event ID 4663 (Audit Object Access)

Cette alerte repose sur la capture d'événements de sécurité relatifs aux accès aux fichiers critiques du système. Le déclencheur est basé sur la présence d'un accès aux fichiers SAM, SYSTEM, ou SECURITY par tout processus autre que dllhost.exe

Priorité et Niveau de Sévérité

Sévérité : Haute
L'accès non autorisé aux fichiers SAM ou SYSTEM est un indicateur majeur d'une tentative de compromission de crédentiels et peut entraîner une compromission plus large du système si l'attaque n'est pas stoppée à temps.

Actions de Remédiation

- Isolation de la Machine
- Audit des Comptes et Crédentiels
- Audit des logs

8. Brute Force

Tentatives de Connexion Échouées Multiples

Description

Cette alerte surveille les tentatives de connexion échouées répétées, ce qui peut indiquer une attaque par force brute. Elle est configurée pour se déclencher lorsque plus de 100 tentatives échouées sont détectées dans un intervalle de 15 minutes, provenant soit de la même adresse IP, soit du même utilisateur.

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Credential Access	T1110.001 - Brute Force	Tentative d'accès aux identifiants via des essais de mots de passe répétés pour obtenir un accès non autorisé.

Scénario d'Attaque :

l'attaquant commence par identifier des cibles potentielles, en se concentrant généralement sur des comptes administratifs ou des utilisateurs réguliers. Ensuite, il lance une attaque en utilisant un script automatisé qui effectue des tentatives de connexion répétées en testant différentes combinaisons de noms d'utilisateur et de mots de passe. Dès qu'un nombre élevé d'échecs de connexion est détecté, une alerte se déclenche, signalant un risque potentiel de compromission.

Technique de Détection

- **Type de Log** : Windows Security Event Log (EventCode 4625 - Échec de Connexion)

La détection repose sur la capture d'événements d'échec de connexion répétés, indiquant une activité inhabituelle qui pourrait signaler une attaque par force brute. L'alerte se déclenche lorsque le seuil de 100 tentatives échouées est atteint en 15 minutes.

Priorité et Niveau de Sévérité

- **Sévérité** : Élevée
- **Justification** : Les attaques par force brute visant à deviner des identifiants peuvent permettre à un attaquant d'obtenir un accès non autorisé, compromettant la sécurité de l'ensemble du réseau si elles aboutissent.

Actions de Remédiation

Isolation de l'IP : Bloquez l'adresse IP à l'origine des tentatives répétées de connexion échouée pour interrompre l'attaque.

Modification des Identifiants : Réinitialisez les mots de passe des comptes ciblés et appliquez des politiques de mots de passe forts.

Implémentation de Mécanismes de Verrouillage de Compte : Configurez des règles de verrouillage de compte après plusieurs tentatives échouées pour empêcher les attaques par force brute continues.

Faux Positifs

Il est peu probable qu’un utilisateur légitime tente de se connecter plus de 100 fois en 15 minutes. Ce comportement est généralement caractéristique d'une attaque automatisée par force brute,.

9. Surveillance des anomalies réseau

Anomalie Réseau Détectée

Description

Cette alerte identifie des anomalies réseau en analysant le volume de données et de paquets échangés entre des adresses IP, ainsi que les valeurs TTL (Time-to-Live). Elle inclut également une vérification

des adresses IP sources et destinations via une liste noire (malicious-ips.csv) pour repérer les communications avec des adresses associées à des activités malveillantes.

Classification MITRE ATT&CK

Tactic	Technique/Sub-technique	Description
Exfiltration	T1048.001 – Exfiltration Over C2 Channel	Détection de transferts importants de données, pouvant indiquer une exfiltration de données.
Reconnaissance	T1595.002 – Active Scanning	Détection de scans intensifs et d'un trafic anormal, indiquant une reconnaissance en cours.

Scénario d'Attaque :

Reconnaissance Réseau : Un attaquant, ayant compromis une machine, tente de scanner le réseau pour repérer des points faibles. L'activité se caractérise par un grand nombre de paquets échangés, parfois avec des TTL anormaux.
Exfiltration de Données : Une fois des données sensibles rassemblées, l'attaquant effectue un transfert massif en utilisant une communication chiffrée ou non conventionnelle, déclenchant ainsi l'alerte.
Évasion Défensive : L'attaquant modifie le TTL pour brouiller les pistes ou utilise des IP malveillantes pour dissimuler l'exfiltration.

Technique de détection

Type de Log : Suricata (Analyse du trafic réseau)

La détection repose sur l'analyse de plusieurs critères :

- Volume de données échangé supérieur à 10Go (Communication suspect avec un C2)
- Nombre de paquets supérieur à 10 000
- Anomalies dans les valeurs TTL (ex. : TTL maximal >128 et TTL minimal <64) pouvant signaler du spoofing
- Vérification de l'implication d'adresses IP malveillantes répertoriées dans le fichier malicious-ips.csv

Priorité et Niveau de Sévérité:

Sévérité : Haute

Les transferts de données inhabituels ou les communications avec des IP malveillantes peuvent indiquer des tentatives d'exfiltration de données ou d'accès non autorisé.

Action de Remédiation

- Isolation de la Machine
- Analyse du Trafic

- Analyser les IP Malveillantes

Faux Positifs :

Opérations de Maintenance ou Sauvegardes : Des transferts volumineux lors de sauvegardes ou migrations de données peuvent parfois déclencher l'alerte.

Mise à Jour des Systèmes : Les mises à jour de logiciels, surtout si elles impliquent des téléchargements de correctifs ou de gros fichiers, peuvent également produire des volumes de données.