Documentation SOC - Règles de Détection et Fiches Réflexes

1.1 Règles Active Directory

1.1.1 Kerberoasting

Description : Détection des tentatives d'extraction des tickets de service Kerberos (TGS) pour le craquage hors ligne des comptes de service.

Indicateurs de détection :

- Multiples requêtes TGS depuis un même compte sur une courte période
- Requêtes TGS pour des comptes à privilèges élevés
- System.IdentityModel.Tokens.KerberosRequestorSecurityToken.Get(Request()

Fiche réflexe :

- Identifier l'utilisateur source et les comptes ciblés
- Vérifier l'historique d'authentification du compte source
- Bloquer le compte source si comportement confirmé malveillant
- Forcer la réinitialisation des mots de passe des comptes de service exposés
- Vérifier l'utilisation de SPN non standards

1.1.2 AS-REPRoasting

Description : Exploitation des comptes n'exigeant pas de pré-authentification Kerberos pour extraire des hash crackables.

Indicateurs de détection :

- Event ID 4768 avec code d'erreur 0x25 (pré-authentification non requise)
- Multiples tentatives AS-REQ sans pré-authentification

Fiche réflexe :

- Identifier les comptes ciblés et la source des requêtes
- Activer la pré-authentification sur les comptes concernés
- Analyser les permissions et la légitimité des comptes identifiés
- Investiguer les activités récentes du compte source

1.1.3 Shadow Credentials

Description : Détection de l'ajout frauduleux d'attributs msDS-KeyCredentialLink permettant l'authentification via certificats.

Indicateurs de détection :

- Event ID 5136 avec modification de msDS-KeyCredentialLink

Fiche réflexe :

- Identifier l'objet modifié et l'auteur de la modification
- Supprimer immédiatement les KeyCredentials non légitimes
- Bloquer le compte à l'origine de la modification
- Auditer les permissions WriteProperty sur les objets sensibles
- Rechercher d'autres modifications similaires dans l'environnement

1.1.4 DCSync

Description : Réplication non autorisée des secrets Active Directory via les droits de réplication.

Indicateurs de détection :

- Event ID 4662 avec droits Replicating Directory Changes All

Fiche réflexe :

- Bloquer immédiatement le compte source
- Identifier les secrets potentiellement compromis
- Forcer la réinitialisation du mot de passe krbtgt (deux fois)
- Auditer les permissions de réplication dans l'AD
- Investiguer le point d'entrée initial de l'attaquant

1.1.5 Ajout d'un utilisateur à un groupe critique

Description : Détection de l'ajout non autorisé de comptes dans des groupes privilégiés.

Indicateurs de détection :

- Event ID 4728 pour les groupes : Domain Admins, Enterprise Admins, Schema Admins, Administrators, Backup Operators, Account Operators, Print Operators, Server Operators, Administrateurs

Fiche réflexe :

- Retirer immédiatement le compte du groupe
- Identifier et bloquer le compte à l'origine de l'ajout
- Vérifier les actions effectuées par le compte ajouté
- Auditer les modifications récentes dans l'AD
- Vérifier l'intégrité des GPO et des délégations

1.1.6 Délégation Kerberos

Description : Création ou modification de délégations Kerberos non contraintes ou contraintes.

Indicateurs de détection :

- Event ID 5136 avec modification de userAccountControl (délégation non contrainte) ou modification de msDS-AllowedToDelegateTo (délégation contrainte)

Fiche réflexe :

- Identifier le compte configuré avec la délégation
- Supprimer la délégation si non légitime
- Bloquer le compte ayant effectué la modification
- Auditer les comptes avec délégation existante
- Rechercher des authentifications suspectes utilisant la délégation

1.1.7 Dump NTDS.DIT

Description : Extraction de la base de données Active Directory contenant tous les hash de mots de passe.

Indicateurs de détection :

- Accès au fichier C:\Windows\NTDS\ntds.dit
- Utilisation de wbadmin.exe

Fiche réflexe :

- Isoler immédiatement le contrôleur de domaine concerné
- Identifier la méthode d'extraction (ntdsutil, VSS, WMI)
- Bloquer les comptes compromis identifiés
- Considérer tous les secrets AD comme compromis
- Lancer un plan de rotation des mots de passe à l'échelle du domaine
- Réinitialiser le krbtgt

2 Règles Linux

1.2.1 Multiples commandes d'énumération

Description : Exécution rapprochée de commandes de reconnaissance système.

Indicateurs de détection :

- Exécution séquentielle de : whoami, id, uname, hostname, ifconfig/ip, ps, netstat
- Utilisation de scripts d'énumération automatisés (linpeas, linenum)
- Commandes d'énumération depuis des shells non interactifs

Fiche réflexe :

- Identifier le compte et le processus parent
- Analyser l'origine de la session (SSH, cron, web shell)
- Vérifier les fichiers récemment créés ou modifiés
- Auditer les connexions réseau actives
- Rechercher des backdoors ou des mécanismes de persistance

1.2.2 Activité de password looting

Description : Recherche et extraction de mots de passe stockés en clair ou faiblement protégés.

Indicateurs de détection :

- Accès à /etc/passwd, /etc/shadow, .bash_history, .ssh/
- Recherche de fichiers contenant "password", "passwd", "pwd"
- Utilisation de grep/find avec patterns de mots de passe
- Lecture de fichiers de configuration d'applications

Fiche réflexe :

- Identifier les fichiers consultés et leur contenu
- Changer les mots de passe potentiellement exposés
- Bloquer le compte compromis
- Auditer les permissions sur les fichiers sensibles
- Vérifier les connexions sortantes (exfiltration)

1.2.3 Accès à /etc/shadow

Description : Lecture du fichier contenant les hash de mots de passe.

Indicateurs de détection :

- Ouverture de /etc/shadow par un processus non système
- Copie ou exfiltration du fichier
- Utilisation de cat, less, grep sur le fichier

Fiche réflexe :

- Forcer le changement de tous les mots de passe utilisateurs
- Identifier le processus et l'utilisateur ayant accédé au fichier
- Vérifier les permissions du fichier (devrait être 000 ou 400)
- Rechercher des copies du fichier sur le système
- Analyser le trafic réseau pour détecter une exfiltration

1.2.4 Installation d'un module kernel

Description : Chargement de modules kernel pouvant servir de rootkit.

Indicateurs de détection :

- Utilisation de insmod, modprobe avec des modules non signés

Fiche réflexe :

- Identifier le module chargé et son origine
- Décharger immédiatement le module (rmmod)
- Analyser le module en environnement isolé
- Vérifier l'intégrité du kernel
- Rechercher d'autres indicateurs de rootkit (fichiers cachés, ports, processus)
- Envisager une réinstallation système si rootkit confirmé

3 Règles Windows

1.3.1 Création d'une tâche planifiée suspecte

Description : Création de tâches planifiées pour l'exécution de code malveillant ou la persistance.

Indicateurs de détection :

- Utilisation de l'image schtasks.exe
- Tâches avec privilèges élevés créées par des comptes non administratifs

Fiche réflexe :

- Désactiver et supprimer la tâche immédiatement
- Analyser le payload de la tâche
- Identifier le compte créateur et bloquer si compromis
- Vérifier l'exécution de la tâche (Event ID 4700, 4702)
- Rechercher d'autres mécanismes de persistance

1.3.2 Création d'un service suspect

Description : Installation de services Windows malveillants pour persistance ou élévation de privilèges.

Indicateurs de détection :

- Utilisation de l'exécutable sc.exe
- Services avec chemins binaires inhabituels (temp, appdata)
- Services exécutant des commandes PowerShell ou cmd

Fiche réflexe :

- Arrêter et désactiver le service
- Isoler le binaire pour analyse
- Identifier le compte ayant créé le service
- Vérifier les privilèges du service (SYSTEM, LocalService)
- Rechercher d'autres services suspects sur le réseau

1.3.3 Création ou modification de clé RUN

Description : Modification des clés de registre d'autoexécution pour la persistance.

Indicateurs de détection :

- Modifications de HKLM\Software\Microsoft\Windows\CurrentVersion\Run et autres
- Utilisation de l'exécutable reg.exe

Fiche réflexe :

- Supprimer la clé malveillante
- Analyser le fichier référencé
- Identifier le processus ayant modifié le registre
- Vérifier d'autres clés d'autoexécution (RunOnce, RunServices, etc.)

- Scanner le système pour des IOCs similaires

1.3.4 Dump LSASS

Description : Extraction de la mémoire du processus LSASS contenant les credentials en cache.

Indicateurs de détection :

- Utilisation du processus lsass.exe

Fiche réflexe :

- Isoler immédiatement la machine
- Identifier les credentials potentiellement compromis
- Forcer la rotation des mots de passe des comptes connectés
- Analyser le processus parent et la chaîne d'exécution
- Rechercher des connexions réseau sortantes (exfiltration)
- Vérifier les authentifications récentes depuis cette machine

1.3.5 Installation de drivers vulnérables

Description : Installation de drivers vulnérables pour élévation de privilèges vers le kernel (BYOVD).

Indicateurs de détection :

- Hash correspondant à des drivers malveillants connus

Fiche réflexe :

- Arrêter et désinstaller le driver immédiatement
- Vérifier les actions effectuées avec privilèges kernel
- Analyser le driver en environnement isolé
- Rechercher d'autres drivers suspects
- Activer ou vérifier la politique de signature de drivers

1.3.6 Utilisation de LOLBIN

Description : Détournement de binaires légitimes Windows (Living Off The Land Binaries) pour des actions malveillantes.

Indicateurs de détection :

- Utilisation de certutil pour télécharger des fichiers
- Mshta.exe exécutant du code distant
- Regsvr32.exe
- Rundll32.exe
- Action menée par des utilsateurs autre que Authority NT\System et les membres du groupe Administrateurs

Fiche réflexe :

- Identifier le LOLBIN utilisé et son action
- Bloquer les URLs ou fichiers associés

- Analyser les artefacts créés ou téléchargés
- Vérifier la chaîne de processus parent
- Rechercher d'autres utilisations similaires dans l'environnement

1.3.7 Clear des eventlogs

Description : Suppression des logs d'événements pour masquer les traces d'activité malveillante.

Indicateurs de détection :

- Event ID 1102 (Security log cleared)
- Event ID 104 (System log cleared)

Fiche réflexe :

- Escalader immédiatement en incident majeur
- Identifier le compte ayant effacé les logs
- Récupérer les logs sauvegardés ou centralisés
- Reconstruire la timeline à partir des sources alternatives
- Rechercher d'autres systèmes affectés
- Considérer comme compromission avérée

1.3.8 Modification de la politique d'audit

Description : Désactivation ou modification de la politique d'audit pour éviter la détection.

Indicateurs de détection :

- Modifications via auditpol.exe

Fiche réflexe :

- Restaurer immédiatement la politique d'audit
- Identifier le compte responsable de la modification
- Escalader en incident de sécurité majeur
- Analyser la période pendant laquelle l'audit était désactivé
- Rechercher des activités malveillantes non loguées

4 Règles Réseau

1.4.1 DNS Tunnelling

Description : Utilisation du protocole DNS pour l'exfiltration de données ou la communication C2.

Indicateurs de détection :

- Requêtes DNS avec des noms de domaine encodés

Fiche réflexe :

- Bloquer le domaine au niveau DNS et firewall
- Isoler la machine source
- Analyser le contenu des requêtes DNS

- Identifier le processus générant les requêtes
- Rechercher des IOCs similaires dans le réseau
- Analyser les données potentiellement exfiltrées

1.4.2 Utilisation du réseau TOR

Description : Connexion au réseau TOR pour anonymisation ou communication C2.

Indicateurs de détection :

- Connexions vers des IPs de nœuds TOR connus
- Trafic sur le port 9050, 9150
- Utilisation du client TOR (tor.exe)

Fiche réflexe :

- Bloquer les connexions TOR au niveau firewall
- Identifier l'utilisateur et le système source
- Analyser l'objectif de l'utilisation de TOR
- Vérifier si des données ont été exfiltrées
- Auditer les activités récentes de l'utilisateur
- Évaluer si l'utilisation est légitime ou malveillante