Rapport d’Incident :
Analyse et plan d’action

Remplissez ce document avec les informations demandées, pour chaque alerte qui représente une menace. N’oubliez pas d’inclure des captures d’écran dans toutes les instances indiquées.

NB: Un seul gabarit est fourni par section. Copiez et collez le gabarit autant de fois que nécessaire pour représenter le nombre d’alertes et/ou dossiers concernés.

I. Investigation

Alerte : Privileged User Created – Une alerte signalant la création suspecte d'un utilisateur avec des privilèges élevés, nécessitant une analyse détaillée pour comprendre son origine et ses implications.
Risque: Elevé

Détails d’investigation

Reportez ici toutes les informations que vous avez pu recueillir sur l’alerte. Ajoutez ou enlevez des points au besoin.

Date et Heure de l’Alerte : 17 mai 2023 à 10:02
09h50 – Problèmes de Firewall : Plusieurs erreurs indiquant l’incapacité du pare-feu Windows à appliquer des règles (mDNS, Teredo, IPHTTPS). IP concernée : 192.168.56.103.
10h06 et 10h36 – Redémarrage du Service de Protection Logicielle : Deux redémarrages planifiés.
10h21 – Opérations Privilégiées : Multiples tentatives d'accès à des objets via LSASS.exe avec le privilège SeSecurityPrivilege. Compte : LOCAL SERVICE (NT AUTHORITY).
10h50 et 11h50 – Problèmes de Firewall Continus : Règles de pare-feu toujours défaillantes.

Indicateurs de compromission

Détaillez ici les éléments qui permettent d’identifier cette menace dans l'avenir. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Adresse IP Suspecte : 192.168.56.103 – Associée à des erreurs de pare-feu et des tentatives d'accès privilégié.
Hash Malveillant : SHA256 : 613e6cc9610507f555e6a261375c9cd33d20c7e7925cedf93c14a0871bda2a6d – Identifié comme Backdoor.Tofsee.
Tentatives d’Accès Privilégié : LSASS.exe demandant SeSecurityPrivilege, activité inhabituelle pour le compte LOCAL SERVICE.

Actifs impactés

Détaillez ici les machines, applications et utilisateurs impactés par cette alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Serveurs de Domaine : FR-SRV-DC01, FR-SRV-DC02, FR-SRV-DC03, FR-SRV-DC04 (notamment FR-SRV-DC04, IP : 10.11.2.12).
Serveurs de Sauvegarde : FR-SRV-BKP-1, FR-SRV-BKP-2, FR-SRV-BKP-3.
Pare-feu : FR-SRV-FW (problèmes de pare-feu notés).

Informations supplémentaires

Remplissez le tableau avec les informations indiquées.

Source et raison de levée de l'alerte	Qualification de l'alerte *(faux positif ou incident vérifié)*	Justification de la qualification
Wazuh – Détection d'une potentielle création de compte privilégié avec des anomalies dans les logs.	Risque: Elevé	Éléments suspects : erreurs de pare-feu, tentatives d'opérations privilégiées, et hash malveillant associé.

II. Analyse

Dossier : Activités Malveillantes Ciblant les Comptes Privilégiés et le Contrôleur de Domaine FR-SRV-DC04

Alertes :

Listez ici les alertes regroupées dans ce dossier. Ajoutez ou enlevez des points au besoin.

- Multiple Authentication Failures Followed by Success
- Privileged User Created
- Potential Dump Memory

Caractéristiques

Détaillez ici les éléments communs qui réunissent ces alertes. Ajoutez ou enlevez des points au besoin.

Adresses IP :

10.11.2.12 (FR-SRV-DC04) impliquée dans les activités suspectes.
Tentatives de connexion bruteforce et manipulations suspectes sur les contrôleurs de domaine.
Serveur critique commun :

FR-SRV-DC04 comme point central des attaques.

Commentaires/observations

Si vous avez des observations à signaler par rapport à ce dossier, notez-les ici. Ajoutez ou enlevez des points au besoin.

L'absence de logs explicites de création d'utilisateur suggère une dissimulation ou un contournement des systèmes de surveillance.
Les redémarrages de services de protection logicielle sont suspects en lien avec des tentatives d'accès.

Scénario : *résumez brièvement le scénario d'attaque que vous concevez pour ce dossier. Ajoutez ou enlevez des points au besoin.*

Une tentative d'élévation de privilèges via LSASS.exe a été détectée, potentiellement pour obtenir des accès administratifs.
Des erreurs de pare-feu récurrentes pourraient indiquer des manipulations pour désactiver la protection.
Absence de logs explicites laissant penser à une tentative de dissimulation.

III. Plans d'action

Dossier : Privileged User Created

Plan d'action : *résumez brièvement le plan d'action que vous concevez pour ce dossier, en fonction du scénario associé. Ajoutez ou enlevez des points au besoin.*

Contenir la menace :

Suspendre les comptes affectés
Bloquer l'accès réseau depuis l'IP 192.168.56.103, source des activités suspectes.

Sécuriser les systèmes :

Supprimer tout ajout suspect dans le groupe Administrateurs.
Analyser et protéger lsass.exe contre des manipulations non autorisées.

Investiguer les activités :

Revoir les logs pour identifier les tentatives d'accès avec SeSecurityPrivilege.
Vérifier les anomalies réseau autour de l'IP 192.168.56.103 et les serveurs concernés (FR-SRV-DC01 à DC04).

Renforcer la sécurité :

Corriger les problèmes de pare-feu et limiter l'accès aux services sensibles.
Activer des alertes SIEM pour détecter les modifications de privilèges ou les activités inhabituelles.