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 : **Multiple Authentication Failures Followed by Success :** Signalant des tentatives échouées suivies d'une connexion réussie, indiquant une potentielle attaque bruteforce.
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.

Les tentatives d'authentification ont été enregistrées le 3 janvier 2023, de 17:23:58 à 17:44:48.
Nom d’utilisateur : carter
Adresse IP source : IP : 10.11.2.12 (Description selon l’extrait CMDB : Cette adresse IP correspond au contrôleur de domaine FR-SRV-DC04.)
Code d'erreur 0xC000006A : Mot de passe incorrect pour plusieurs tentatives.
Code d'erreur 0x0 : Authentification réussie, indiquant un accès au compte carter.
Une série de tentatives échouées a été suivie d'une réussite, indiquant une attaque bruteforce potentielle.

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.

Nom d’utilisateur : carter
Adresse IP source : 10.11.2.12
Codes d’erreur : Multiples 0xC000006A suivis d'un code 0x0.
Fréquence des tentatives : Tentatives rapprochées, indiquant un processus automatisé.

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.

Utilisateur : carter
Serveur : kali
Contrôleur de domaine : FR-SRV-DC04

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
Détection par le SIEM en raison des échecs suivis d'une tentative réussie	Risque: Elevé	Succès après des échecs répétés, signe d'une attaque bruteforce

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.

Une tentative réussie après des échecs répétés signale un risque de compromission élevé
Pas de lien avec des activités TOR connues

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

Un attaquant semble avoir utilisé un script pour tester des mots de passe sur le compte carter. Après plusieurs tentatives échouées, l'accès a été obtenu, compromettant potentiellement le compte.

III. Plans d'action

Dossier : **Auth_Failures_Followed_By_Success**

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 :

Désactiver temporairement le compte Carter.
Bloquer l'accès réseau depuis l'IP 10.11.2.12.

Sécuriser le compte et les systèmes :

Réinitialiser le mot de passe de Carter avec des règles renforcées.
Activer l'authentification multi-facteurs (MFA) sur les comptes sensibles.
Ajouter authentification à multiples facteurs.

Auditer les logs :

Vérifier les logs de FR-SRV-DC04 pour détecter des tentatives bruteforce et des accès suspects.
Renforcer la sécurité :

Configurer des alertes SIEM pour surveiller les tentatives échouées répétées.
Auditer les paramètres de sécurité du contrôleur de domaine.