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 : **Massive Authentication Failures:** Détection de multiples tentatives d'authentification échouées.
Risque: faible

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 : 5 janvier 2023, de 23:04:41 à 23:30:31
Utilisateur ciblé : printer3
Adresse IP source : 10.11.2.12 (Identifiée comme le contrôleur de domaine FR-SRV-DC04
Code d'erreur : 0xC000006A, indiquant un mot de passe incorrect pour chaque tentative
Événement ID : 4776, correspondant à une tentative de validation d'identification échouée
Fréquence des Tentatives : Très rapprochées dans le temps, avec des intervalles de quelques minutes, indiquant un processus potentiellement automatisé

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 source : 10.11.2.12
Nom d'utilisateur : printer3
Échec répété : Code d'erreur 0xC000006A observé de manière continue

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.

Serveur : FR-SRV-DC04, contrôleur de domaine qui reçoit les tentatives
Utilisateur : printer3
Réseau : Segment LAN serveurs 10.11.0.0/16, réseau Carochan

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
Détectée par le SIEM en raison du nombre élevé de tentatives d'authentification échouées	Faux positif	Volume élevé de tentatives échouées en peu de temps, provenant de la même IP cependant rien dans les logs ne semble indiquer une quelquonque compromission.

II. Analyse

Dossier :

Alertes :

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

Caractéristiques

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

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'IP source étant un contrôleur de domaine, cela pourrait signaler une mauvaise configuration ou un simple oublie de mot de passe. Dans tous les cas rien n'indique dans les logs une quelquonque menace ou compromission.

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

L'utilisateur semble chercher à se connecter sans succés. Rien ne permet d'affirmer qu'il s'agisse d'une menace . Le mieux serait d'auditionner le concerné.

III. Plans d'action

Dossier : **Massive_Auth_Failures_Investigation**

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.*

Auditionner l'utilisateur pour en savoir plus sur ces connections échouées.