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 : **Nmap_Scanner_Investigation :** Un scan Nmap a été détecté, impliquant une activité de reconnaissance sur le réseau interne. L’alerte provient du SIEM, identifiée comme un événement de pare-feu. Ce scan semble être légitime.
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.

Source IP : 10.11.2.13, identifiée comme le serveur de monitoring FR-SRV-MGMT (service Prometheus)(Extrait+CMDB+Carochan).
Port de Destination : 9182 (port TCP), souvent utilisé par des applications de monitoring telles que Prometheus.
Protocole : TCP
Période d'activité : Du 2 janvier 2023 à 6h00 jusqu’au 7 janvier 2023 à 6h00, sans interruption.
Destination IPs : Multiples cibles dans le LAN des serveurs (10.11.0.0/16), couvrant des machines critiques.

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.

Ce scan semble tout à fait légitime, il provient du serveur de monitoring FR-SRV-MGMT. Aucun élément dans les logs permettant d'affirmer qu'il s'agit d'une menace.

Pas d'éléments à ajouter pour identifier cette alerte comme une menace actuelle ou futur.

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.

Pas d'actifs impactés car ce scan semble légitime.

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 de tentatives de connexion fréquentes et rapprochées, suggérant un scan réseau automatisé.	Faux positif	Le scan Nmap s'est poursuivi sans interruption pendant plusieurs jours, ciblant de nombreuses adresses IP avec une fréquence élevée. Mais rien ne permet d'affirmer qu'il n'est pas légitime.

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 10.11.2.13, associée au serveur de monitoring FR-SRV-MGMT, a exécuté un scan Nmap sur le réseau interne pendant cinq jours sans interruption.
Cela provient peut-être d'un oublie de l'admin?
Rien dans les logs ne semble démontrer que ce serveur est compromis ou que ce scan n'est pas légitime.

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

Scénario : L'IP 10.11.2.13, associée au serveur de monitoring FR-SRV-MGMT, a exécuté un scan Nmap sur le réseau interne pendant cinq jours sans interruption.

III. Plans d'action

Dossier : Nmap_Scanner_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.*

Pas de plan d'action à entreprendre pour ce scan légitime .

Questionner l'administrateur sur la raison de la durée du scan.