1. Leaked file

Une image contenant texte, logiciel, Page web, Site web

Description générée automatiquementPour commencer, j’ai choisi l’outil Microsoft Purview.

Pour ensuite utiliser le «Content search ».

J’ai ensuite du choisis une série de paramètre pour retrouver le fichier qui a leak. Voici mes choix :

Une image contenant texte, capture d’écran, cercle

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

J’ai par la suite exporté les résultats.

Et choisis les fichiers pertinents.

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

1. Investigate Amari in Sentinel & Defender

Je suis allé dans Microsoft Sentinel pour commencer, dans la section incident j’ai remarqué plusieurs incidents de niveau moyen a élevée au niveau de la gravité. Dont Password Spray Incident dans celui-ci j’ai retrouvé une adresse IP et une adresse mail et un incident créer directement par Microsoft Defender

Une image contenant texte, logiciel, Page web, Icône d’ordinateur

Description générée automatiquement

Une image contenant texte, Police, capture d’écran

Description générée automatiquement2 alertes ont été créée : qui sont composé des détails de l’attaque

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Si on clique sur le « Reflective dll loading detected » il y a une courte description de l’alerte et des recommandations

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Ensuite je suis allé dans le Microsoft Defender dans la fenêtre devices, il y a le pc105 celui qui est compromis, dans la Timeline nous pouvons retrouver un tas d’informations intéressante

Une image contenant texte, logiciel, Page web, Icône d’ordinateur

Description générée automatiquement

Dans la fenêtre Evidence and Response, j’ai pu remarquer 1 processus suspect

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

1. Investigate Amari in Azure AD Identity Protection

En allant dans Azure AD Identity Protection -> Risky User, j’ai trouvé des informations sur Amari Riveira.

Une image contenant capture d’écran, texte, ligne, nombre

Description générée automatiquement

En me baladant dans Risky sign-in j’ai remarqué quelque chose de suspect venant d’une certaines Emily Braun qui s’est d’abord connecté a Budapest et 1 heure plus tard se connecté en Espagne a Barcelone



Une image contenant texte, capture d’écran, Page web, logiciel

Description générée automatiquement

Dans la partie Risk Detection, on peut remarqué plusieurs choses. La première est que Emily Braun et Amari Riveira utilise la même adresse IP. Et que Emily Braun a encore changer de lieu, elle se trouve au Texas.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Nestor Mike est aussi un user a risque

Une image contenant texte, capture d’écran

Description générée automatiquement

1. Set up an Insider Risk Policy

Voila l’ensemble des paramètres que j’ai sélectionner.

Une image contenant texte, capture d’écran

Description générée automatiquement

Afternoon investigation

1. Set Up Compliance Policies

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquementVoici mes options pour la «policy »

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

1. Investigate Amari’s Device in Microsoft 365 Defender

En investiguant je suis tombé sur un outil qui permet de chercher dans la machine 105 grâce a cela j’ai pu retrouver des fichiers qui ont été leak.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Dans la partie ci-dessous j’ai découvert beaucoup d’indiceUne image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

1. Sarch for Internal Communication Containing the IP Address

Pour retrouver une IP dans un Teams chat, j’ai utiliser Content Search

Une image contenant texte, ligne, Police, reçu

Description générée automatiquement

J’ai retrouvé une conversation étrange entre Angel et Amari. Angel me semble suspecte.

Une image contenant capture d’écran, texte, ligne

Description générée automatiquement

1. Investigate IP Address in Sentinel

J’ai créé une règle pour automatiser la réponse lors d’une connexion a distance

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

1. Configure Windows Security Baseline

Evening investigation

1. Configure Azure AD Identity Protection

J’ai commencé par créer une User risk policy et la même chose pour sign-in risk policy

Une image contenant texte, capture d’écran, Police

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

1. Investigate Angel's Sign-In Logs
2. Reda

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

1. Compliance Search
2. Investigate Tomo’s Device in Sentinel and Microsoft 365 Defender

Une image contenant texte, capture d’écran, Police, Graphique

Description générée automatiquement