Table des matières

[Morning Investigation 1](#_Toc150937590)

[Search For Leaked File 2](#_Toc150937591)

[Investigate Amari in Sentinel & defender 2](#_Toc150937592)

[Investigate Amari in Azure AD Identity Protection 3](#_Toc150937593)

[Set Up Insider Risk Policy 4](#_Toc150937594)

[Afternoon Investigation 6](#_Toc150937595)

[Set UP Compliance Policies 6](#_Toc150937596)

[Investigate Amari’s Device In microsoft 365 defender 6](#_Toc150937597)

[Search for internal communication containing the IP adress 6](#_Toc150937598)

[Investigate IP Address in sentinel 7](#_Toc150937599)

[Configure Windows Security Baseline 7](#_Toc150937600)

[Evenning Investigation 10](#_Toc150937601)

[Configure Azure AD Identity protection 10](#_Toc150937602)

[Investigate Angel’s Sign-in logs 10](#_Toc150937603)

[Investigate Angel in sentinel and microsoft 365 defender 10](#_Toc150937604)

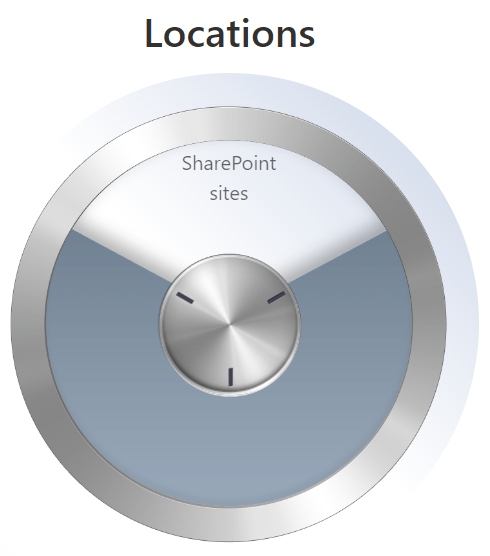
[Communication Compliance Search 11](#_Toc150937605)

[Investigate Tomo's Device in Sentinel and Microsoft 365 Defender 11](#_Toc150937606)

# Morning Investigation

## Search For Leaked File

Dans cette piste, j’ai utilisé la recherche Purview Content pour localiser le fichier exfiltré dans mon environnement. Et grâce à l’outil « Content search » j’ai pu affiner mes recherches en spécifiant une location, un mot clé, et une condition

 Une image contenant cercle, horloge, capture d’écran, conception

Description générée automatiquement Une image contenant cercle, capture d’écran, horloge, conception

Description générée automatiquement

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

Description générée automatiquement

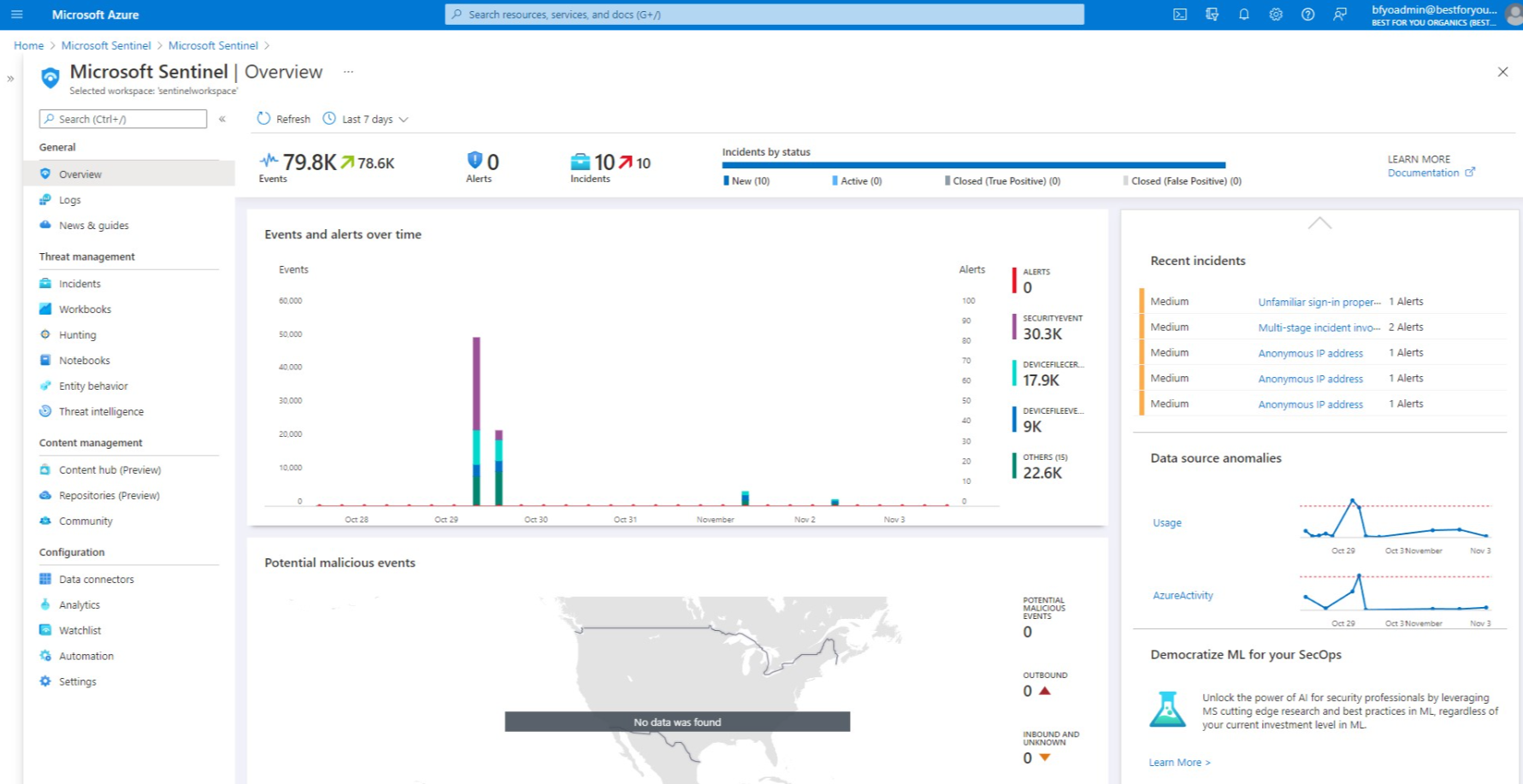
Après exportation des résultats, j’ai pu avoir quelques informations , notamment le nombre de copies, qui y avait accès et ce qu'il fallait protéger.

## Investigate Amari in Sentinel & defender

À partir du tableau Security Alert, j’ai trouvé l'appareil qu'Amari utilisait et il y avait effectivement une activité suspecte. Puisqu'il y a eu une alerte de sécurité intéressante, j’ai vérifié les incidents dans Microsoft Sentinel. J’ai trouvé quelques incidents intéressants. Il y a eu un 3 incidents de « Anonymous IP adress » de niveau moyen, un incident « Unfamiliar Sign-in » qui a généré une alerte

Un autre incident plus intéressant « Multi-stage incident Execution and Defense evasion » qui a généré 2 alertes.

J’ai aussi pu voir une anomalie dans l’usage des données et l’AzureActivity dans la journée du 29 octobre.



J’ai sélectionné le processus spécifique qui présente le plus grand nombre d'activités suspectes. Comme je ne disposais pas encore de suffisamment d'informations pour répondre à la question, j’ai consulté les Alertes pour trouver plus d'informations sur les Processus.

Après avoir examiné l'historique pour les deux alertes, un ID de processus (PID) s'est démarqué. Cela m’a permis de sélectionner le processus dans la liste de trois. En enquêtant sur l'appareil, j’ai examiné la chronologie et découvert de nombreux événements intéressants qui pointaient vers une piste d'activité suspecte me poussant à conclure que Cet appareil aurait été compromis

## Investigate Amari in Azure AD Identity Protection

J’ai étudié le compte d’Amari dans la section des rapports Azure AD Identity Protection pour rechercher une activité malveillante qui pourrait indiquer que le compte est compromis. j’ai vu trois comptes . Parmi lesquels celui de Amari. Les deux autres comptes ont été mis à jour avec High bien avant Amari. Sur la base de la chronologie de l'incident, les informations sur les utilisateurs à risque d'Amari étaient les seules informations pertinentes.

Une image contenant texte, logiciel, Icône d’ordinateur, capture d’écran

Description générée automatiquement

j’ai trouvé des informations supplémentaires sur les attaques d’identité qui ne sont probablement pas liées à cet incident. Dans le rapport de détection des risques, j’ai constaté une attaque par password spray sur le compte d'Amari. Cela m’a fourni suffisamment d’informations pour considérer ce compte comme potentiellement compromis. En revenant au rapport Utilisateurs à risque, j’ai pu « Confirmer l'utilisateur compromis », puis réinitialiser le mot de passe.

## Set Up Insider Risk Policy

J’ai décidé de configurer une détection à l'aide de Purview Insider Risk.

* J’ai configuré une stratégie basée sur les fuites de données générales.
* Les autres politiques fournissaient des détections similaires, mais l'environnement ne disposait pas des informations supplémentaires requises, comme la connexion à un système RH, pour être au courant des utilisateurs qui partaient

Une image contenant texte, capture d’écran, Police, Bleu électrique

Description générée automatiquement

* Au lieu d’appliquer la détection à tous les membres de l’entreprise, j’ai étendu la stratégie au groupe d’applications de commerce électronique.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* Ensuite, j’ai configuré la stratégie pour qu'elle se concentre sur les sites SharePoint, les informations sensibles et les types d'activités d'exfiltration.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Premier Bilan :

La machine de Amari aurait été compromise par un malware Notamment grâce à une connexion établie entre l’éxécutable patch.exe et sa machine.

# Afternoon Investigation

## Set UP Compliance Policies

Pour protéger les informations sensibles concernant les données client :

* J’ai configuré des Labels et des stratégies de sensibilité de protection des informations dans Microsoft Purview.
* J’ai d’abord créé un label dans la zone Protection des informations. Le label a été configurée pour crypter les fichiers et les e-mails. Les autorisations de labels ont été définies pour autoriser l'accès uniquement à l'équipe de l'application de commerce électronique en ligne.

Une image contenant cercle, horloge, conception

Description générée automatiquement Une image contenant cercle, horloge, capture d’écran, conception

Description générée automatiquement Une image contenant cercle, horloge, capture d’écran, conception

Description générée automatiquement

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

Description générée automatiquement

* Ensuite, j’ai configuré une stratégie Auto-Labelling avec le modèle de stratégie financière par défaut appliqué aux comptes Exchange, SharePoint et OneDrive pour appliquer mon Label nouvellement créée

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* La politique était en mode simulation pour me permettre de vérifier l'exactitude, puis d'augmenter la portée de la politique. Cela m’a également permis d'estimer le temps nécessaire à la pose des étiquettes.

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

Description générée automatiquement

## Investigate Amari’s Device In microsoft 365 defender

J’ai décidé d'enquêter sur l'appareil d'Amari pour trouver d'autres preuves de l'activité des attaquants. Tout d’abord, j’ai effectué une recherche avancée à l’aide de KQL pour trouver les occurrences de l’adresse IP des attaquants. J’ai inspecté chaque enregistrement de l’ensemble de résultats.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Ensuite, sur la page Appareil de Microsoft 365 Defender, j’ai vérifié l’onglet Alertes et trouvé une activité évidente d’attaquant. J’ai lancé une session « Live Response » pour que l'appareil puisse accéder à distance. Avec une ligne de commande sur l'appareil, j’ai trouvé des répertoires et des fichiers intéressants. Cela m’a fourni une image claire des fichiers impliqués dans l’attaque.

## Search for internal communication containing the IP adress

j’ai décidé de rechercher des informations relatives à l'adresse IP dans les e-mails et les communications Teams dans Microsoft Purview Content Search. La recherche a été configurée en spécifiant les emplacements et la condition.

Une fois la recherche terminée, j’ai exporté tous les éléments vers un seul fichier .pst. Une fois l'exportation terminée, j’ai sélectionné l'exportation dans l'onglet Exporter. Avec la clé d'exportation copiée dans le presse-papiers, j’ai téléchargé les résultats. J’ai trouvé un message de discussion Teams.

## Investigate IP Address in sentinel

À ce stade, je disposais d’une adresse IP pour l’attaquant. Je devais surveiller l’adresse IP dans mon environnement. Dans Microsoft Sentinel, j’ai commencé par une recherche KQL dans les journaux pour l'adresse IP. Tous les résultats étaient attendus sur la base des indices médico-légaux déjà collectés.

J’ai ensuite créé une règle d'analyse NRT (Near-Real-Time) à partir de l'option Analytics de la zone Configuration du portail Sentinel. J’ai configuré la requête de règle pour surveiller les événements réseau liés à l'adresse IP. Pour apporter plus de clarté aux autres analystes, j’ai inclus des mappages d'entités pour le compte, l'adresse IP, l'hôte et le processus. Avec la détection active, un incident sera créé si l'adresse IP est détectée dans les données de journal nouvellement ingérées.

## Configure Windows Security Baseline

Je devais m’assurer que les appareils soient automatiquement configurés avec la ligne de base de sécurité Windows afin de fournir les meilleures pratiques pour la réduction de la surface d'attaque.

* J’ai accédé à Endpoint Security dans Microsoft Endpoint Manager.

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

Description générée automatiquement

* J’ai créé un profil pour la ligne de base de sécurité Windows afin de déployer une version modifiée de la ligne de base pour tous les utilisateurs de votre environnement
* J’ai confirmé la configuration des règles de réduction de la surface d'attaque basée sur le vecteur d'attaque commun d'un document Word qui exécute PowerShell pour communiquer avec l'attaquant.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Description générée automatiquement

Une image contenant texte, logiciel, Icône d’ordinateur, Logiciel multimédia

Description générée automatiquement

Deuxième Bilan : Plusieurs autres fichiers ont été exfiltrés,

# Evenning Investigation

## Configure Azure AD Identity protection

Au cours de l'enquête, j’ai découvert qu'Azure AD Identity Protection n'était pas configuré pour automatiquement gérer le risque utilisateur et le risque de connexion. Dans Azure AD Identity Protection

* j’ai configuré la stratégie de risque utilisateur et Politique de connexion exigeant la correction appropriée du contrôle d’accès.

## Investigate Angel’s Sign-in logs

L'identité d'Angel aurait-elle pu être compromise ? j’ai effectué une recherche dans les journaux de connexion Azure AD pour Données de connexion d'Angel autour de l'heure pivot UTC du message de discussion. Je n’ai rien trouvé ; aucune preuve, ni des indices.

Une image contenant cercle, horloge, capture d’écran, conception

Description générée automatiquement Une image contenant cercle, horloge, capture d’écran, conception

Description générée automatiquement Une image contenant cercle, capture d’écran, texte, conception

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

## Investigate Angel in sentinel and microsoft 365 defender

Ensuite, j’ai enquêté sur Angel pour activité suspecte à l’aide de Microsoft Sentinel et Microsoft 365 Defender. dans les journaux Microsoft Sentinel, j’ai recherché le compte d'Angel. J’ai trouvé l'appareil qu'Angel utilisait. Dans Microsoft 365 Defender, j’ai accédé à la page de l'appareil d'Angel. Rien de suspect pour l'instant. J’ai ensuite accédé à la recherche avancée pour rechercher le nom de l'appareil. Je n’ai pas pu trouver de preuve de compromis pour l'appareil.

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

Description générée automatiquement

## Communication Compliance Search

Avec les indices médico-légaux supplémentaires que j’ai découverts, j’ai mené une autre enquête sur les communications. en utilisant la recherche de contenu dans Microsoft Purview. Cette fois, j’ai concentré la recherche sur la communication d'Angel autour de l’heure pivot UTC de nos autres indices médico-légaux. Après avoir créé l'Export pour la recherche, j’ai téléchargé l'exportation. J’ai recherché dans les résultats des indices pertinents

## Investigate Tomo's Device in Sentinel and Microsoft 365 Defender

À ce stade, je savais que l'appareil de Tomo était connecté à celui d'Angel. L'appareil de Tomo a-t-il été compromis ? Dans Microsoft Sentinel Logs :

* j’ai recherché des informations relatives au compte de Tomo.
* Ensuite j’ai cherché les appareils utilisés par Tomo Et j’ai trouvé un appareil pc034
* Ensuite, j’ai recherché les alertes de sécurité liées à l'appareil de Tomo. Dans Microsoft 365 Defender, j’ai recherché Page de l'appareil de Tomo. En vérifiant la chronologie de l'appareil, j’ai trouvé les événements attendus liés au RDP connexion. je n’ai rien trouvé de suspect.

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

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

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

Description générée automatiquement

Conclusion :

C’est Angel qui est derrière la breach, et l’attaque a été effectuée en envoyant les commandes d’attaque via une session RDP

Une image contenant texte, capture d’écran, Police

Description générée automatiquement