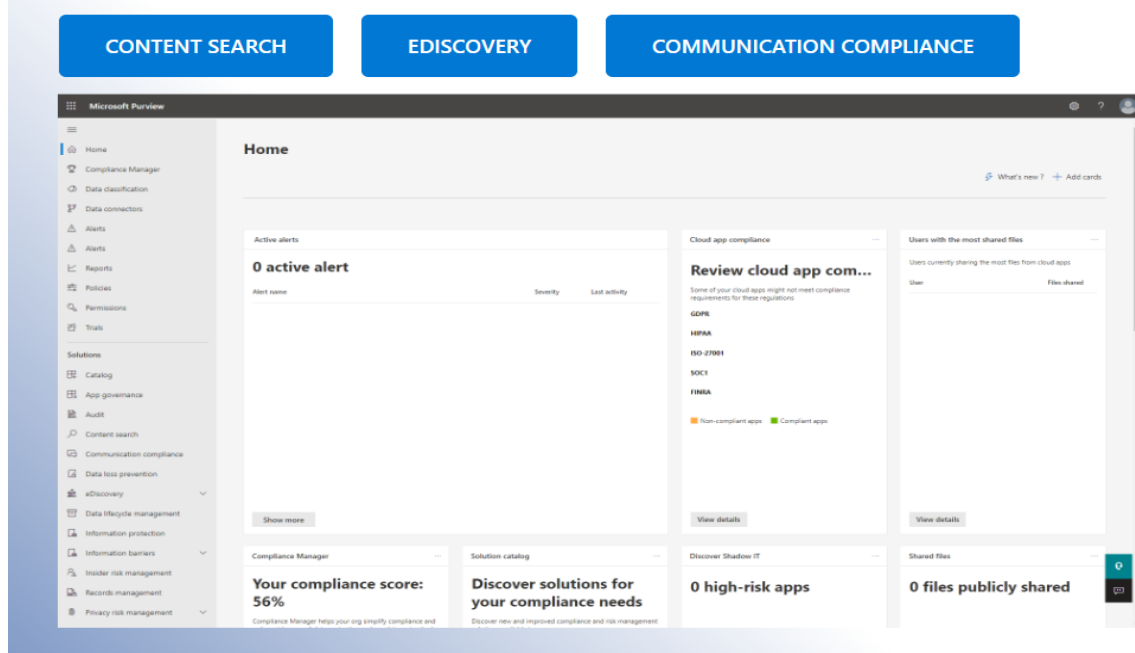


Pour localiser le fichier divulgué, j'ai employé Microsoft Purview, un outil efficace pour déterminer rapidement l'emplacement précis des fichiers au sein de notre réseau d'entreprise.

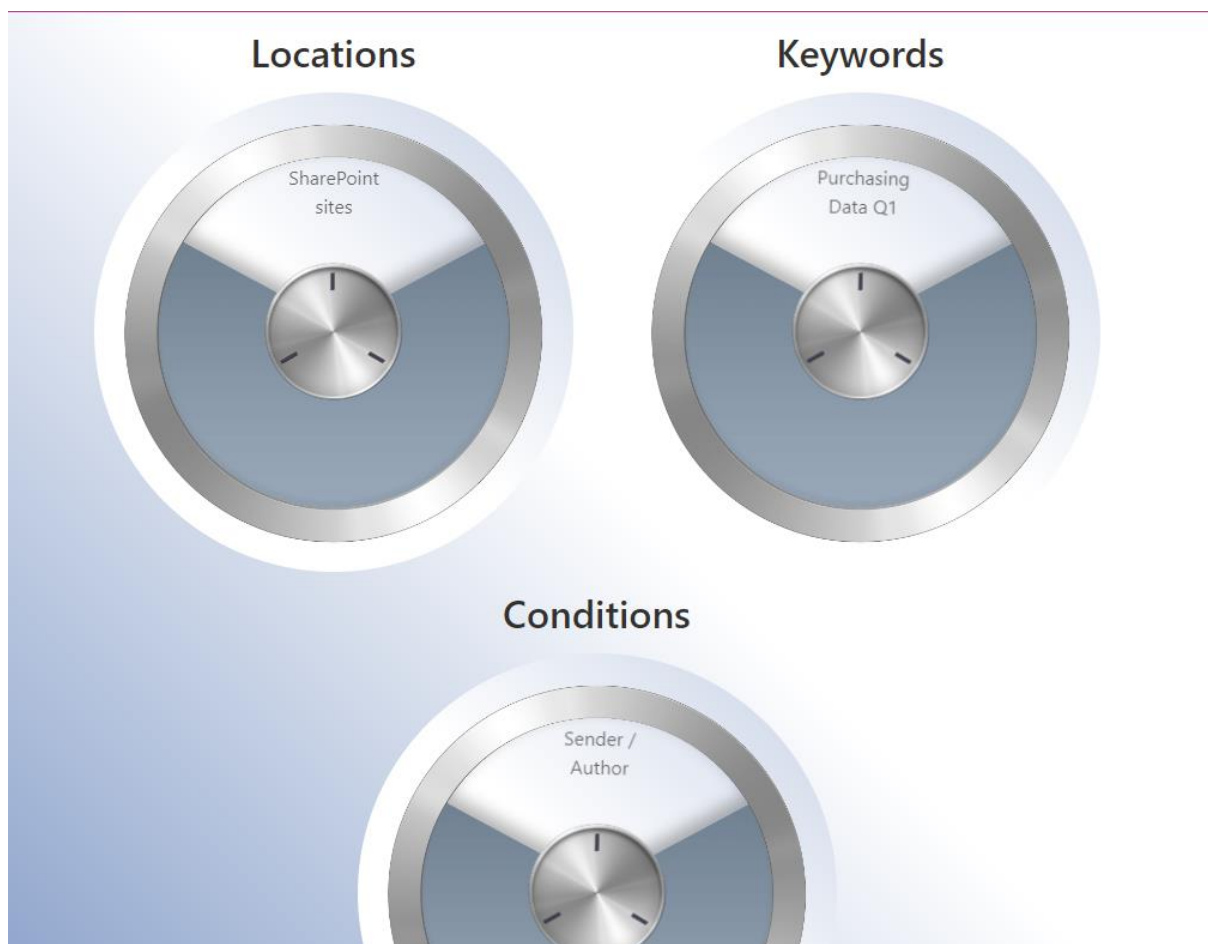


Here's the Microsoft Purview. What tool do you want to use?



J'ai affiné la recherche en spécifiant le mot-clé associé à l'emplacement du fichier et en définissant les conditions de recherche pertinentes pour cibler les documents suspects.

Pour trouver le fichier qu'on cherche



Pour comprendre comment la machine d'Amari a été compromise, j'ai initié l'investigation avec Microsoft Sentinel, la plateforme centrale pour le suivi et l'analyse de tous les incidents de sécurité.

Nous avons identifié un incident indiquant une attaque par 'Password Spray', une forme spécifique de brute force ciblant le compte Amari.

The screenshot shows the Microsoft Sentinel interface. On the left is a navigation pane with sections: General (Overview, Logs, News & guides), Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence), Content management (Content hub (Preview), Repositories (Preview), Community), Configuration (Data connectors, Analytics), and a search bar. The main area displays incident statistics: 10 Open incidents, 10 New incidents, 0 Active incidents. Below this is a bar chart 'Open incidents by severity' with categories: High (1), Medium (9), Low (0), and Informational (0). A search bar and filters (Severity: All, Status: 2 selected, Product name: All, Owner: All) are present. A table of incidents follows, with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, Last update time, and Owner. The table lists 10 incidents, with the 6th incident (ID 6) highlighted as 'High' severity and titled 'Password Spray'.

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	Un...
Medium	12	Multi-stage incident involin...	2	Microsoft 365 Defe...	10/29/21, 04:26 PM	10/29/21, 04:30 PM	Un...
Medium	9	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:41 AM	10/28/21, 10:41 AM	Un...
Medium	8	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:37 AM	10/28/21, 10:37 AM	Un...
Medium	7	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:35 AM	10/28/21, 10:35 AM	Un...
High	6	Password Spray	1	Azure Active Direct...	10/28/21, 06:44 AM	10/28/21, 06:44 AM	Un...
Medium	4	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM	Un...
Medium	3	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM	Un...
Medium	2	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM	Un...
Medium	1	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM	Un...

**Password Spray**  
 Incident ID: 6

Unassigned  
Owner

New  
Status

High  
Severity

Description  
 Password spray attack detected

Alert product names
 

- Azure Active Directory Identity Protection

Evidence
 

**N/A**  
Events

**1**  
Alerts

**0**  
Bookmarks

Last update time  
 10/28/21, 06:44 AM

Creation time  
 10/28/21, 06:44 AM

Entities (2)
 

amari.rivera@bestf...
 199.249.230.167

Tactics (1)
 

Credential Access

View full details >

Incident workbook  
[Incident Overview](#)

Analytics rule  
 Create incidents based on Azure Active Directory Identity Protection al...

Maintenant on passe au log pour crée le timeline de l'évènement

Microsoft Sentinel | Logs

Selected workspace: 'sentinelworkspace'

New Query 1\*

AzureSentinelWorkspace

Run

Time range: Last 7 days

Save

Share

+ New alert rule

Export

Pin to dashboard

Format query

1 search in (SecurityAlert) 'amari.rivera'

Results

Chart

Columns

Add bookmark

Display time (UTC+00:00)

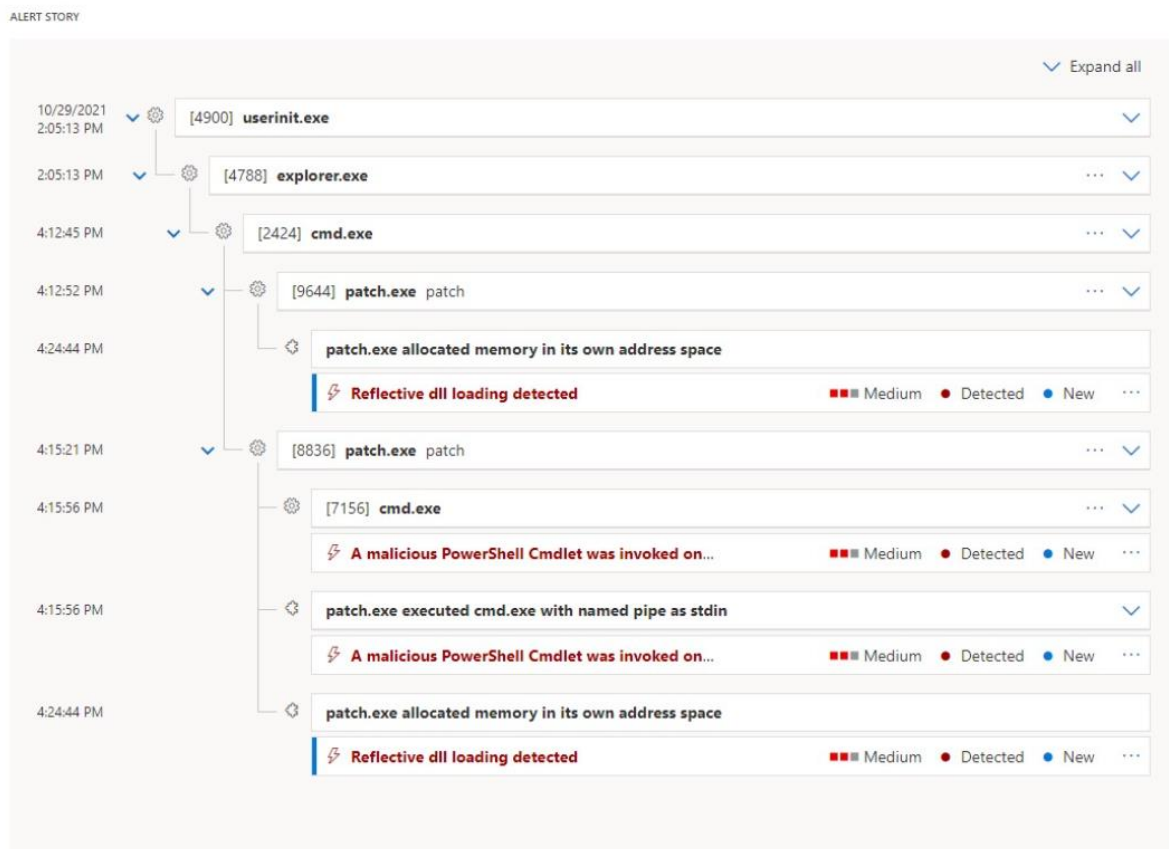
Group columns

Completed. Showing results from the last 7 days.

	TimeGenerated [UTC]	Stable	DisplayName	AlertName	AlertSeverity	Description
>	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 Pow
▼	10/29/2021, 11:31:39.959 PM	SecurityAlert	Reflective dll loading detected	Reflective dll loading detected	Medium	Suspicious memory allocation patte
...						
Stable		SecurityAlert				
TenantId		2de9d6df-9300-4ed8-8b9b-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 loading bypasses the operating system provided mechanism to load a				
ProviderName		MDATP				

Schema and Filter

Et pour avoir tous les détails on va sur Microsoft 365 Defender.



Ici on a les processus suspects.

Processes (3)

Verdict	Process Name	Process ID
✓ Suspicious	patch.exe	8836
— Suspicious	patch.exe	9644
— Suspicious	cmd.exe	7156

Concernant Azure AD Identity Protection, j'ai procédé en suivant les indices relevés, permettant de tracer les activités suspectes liées aux identifiants d'Amari.

Dans Identity Protection | Risky users on peut trouver les détails de Amari Rivera

### 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-bf11-558dcb64b60b

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

Et dans le Risk detections on trouve Amari avec plus de details.

## Risk Detection Details

User's risk report User's sign-ins User's risky sign-ins ...

✓ Detection type	Password spray
Risk state	-
✓ Risk level	High
Risk detail	-
Source	Identity Protection
✓ 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; rv:78.0)
✓ Sign-in request id	<a href="#">9c21b43f-f9c7-4507-b4a4-768d1fbb9b01</a>
Sign-in correlation id	<a href="#">110d108f-cad8-418d-979f-7c31b924b383</a>

J'ai trouvé des informations supplémentaires pour des connexion suspectes.

### Risk Info - Emily : BONUS CLUE

- ★ Risk level: High
- ★ Sign-in time: 8/27/2021, 3:47:05 PM
- ★ IP address: 185.100.87.250
- ★ Sign-in Location: Barcelona, Barcelona, ES

### Risk Info - Nestor : BONUS CLUE

- ★ Risk level: High
- ★ Sign-in time: 8/31/2021, 12:31:01 PM
- ★ IP address: 178.17.174.14
- ★ Sign-in Location: Chisinau, Chisinau, MD

Pour mettre en place du Insider Risk Policy, on va sur Microsoft purview et ont choisi les paramètres de la Policy.

Microsoft Purview

Insider risk management > New insider risk policy

✓ Policy template

✓ Name and description

✓ Users and groups

✓ Content to prioritize

✓ Triggers

✓ Indicators

● Finish

## Review settings and finish

Review the settings for your insider risk policy. The policy will take effect immediately after you create it, but may take up to 24 hours to start generating alerts. We recommend letting your users know how these changes will impact them.

**Policy template**  
General data leaks  
[Edit policy type](#)

**Policy name and description**  
eCommerce Insider Risk Policy  
[Edit policy name and description](#)

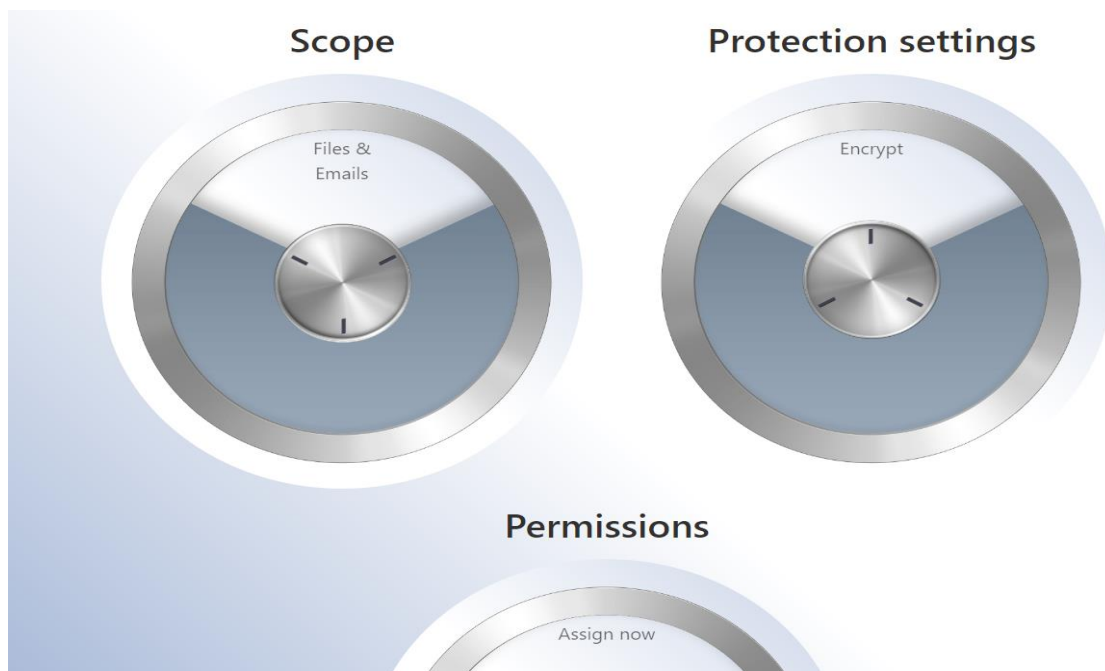
**Users and groups**  
eCommerceAppTeam@bestforyouorganic.onmicrosoft.com  
[Edit users and groups](#)

**Content to prioritize**  
<https://bestforyouorganic.sharepoint.com/sites/eCommerceAppTeam>  
Credit Card Number  
[Edit content to prioritize](#)

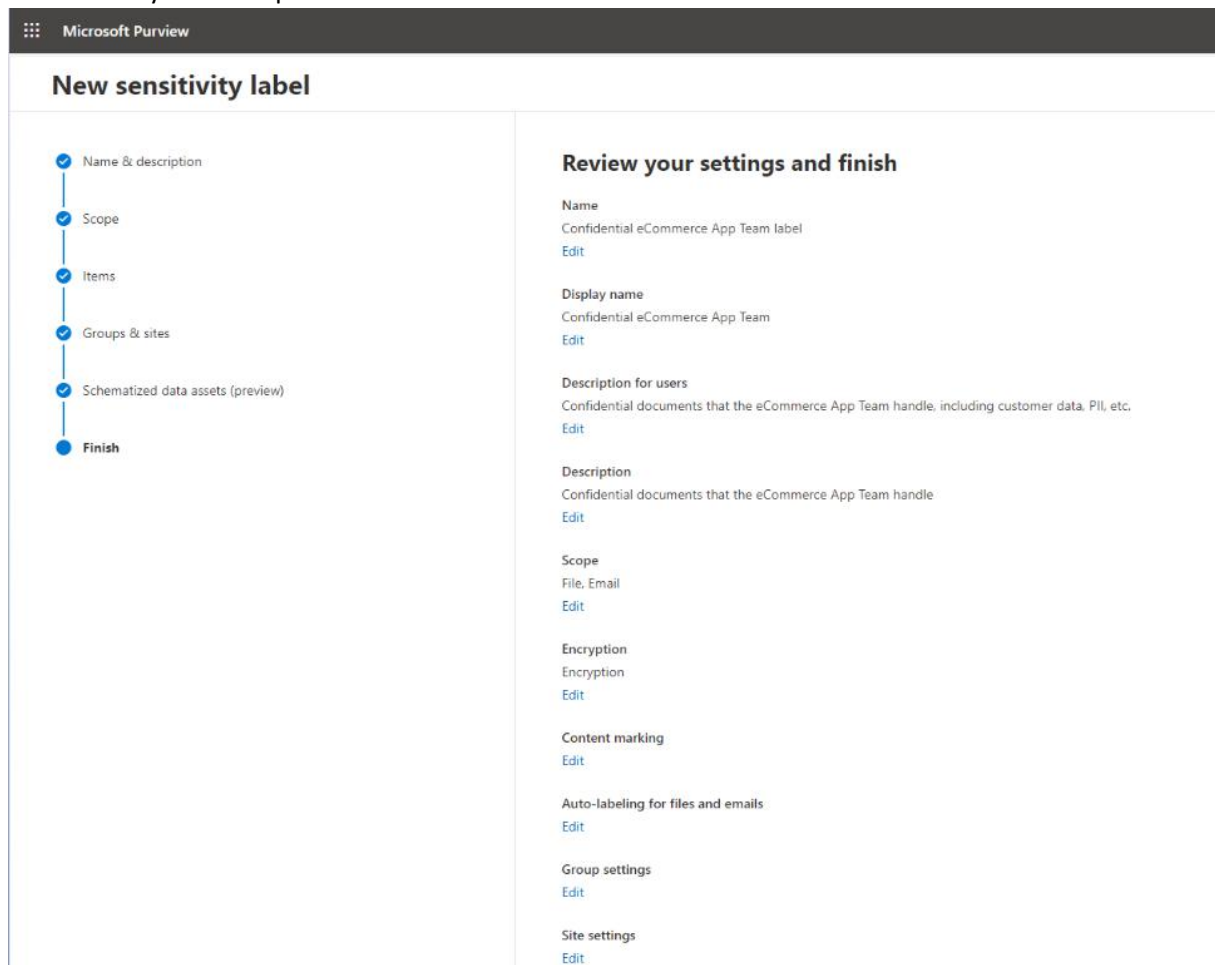
**Triggering event**  
Built-in data leak trigger  
[Edit triggers](#)

**Policy indicators**  
39/56 selected  
No customized thresholds  
[Edit policy indicators](#)

Maintenant il faut configurer des politiques de conformité. On spécifie les paramètres du sensitivity label.



Le sensitivity label est prêt.





Il reste de le déployer.

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](#)

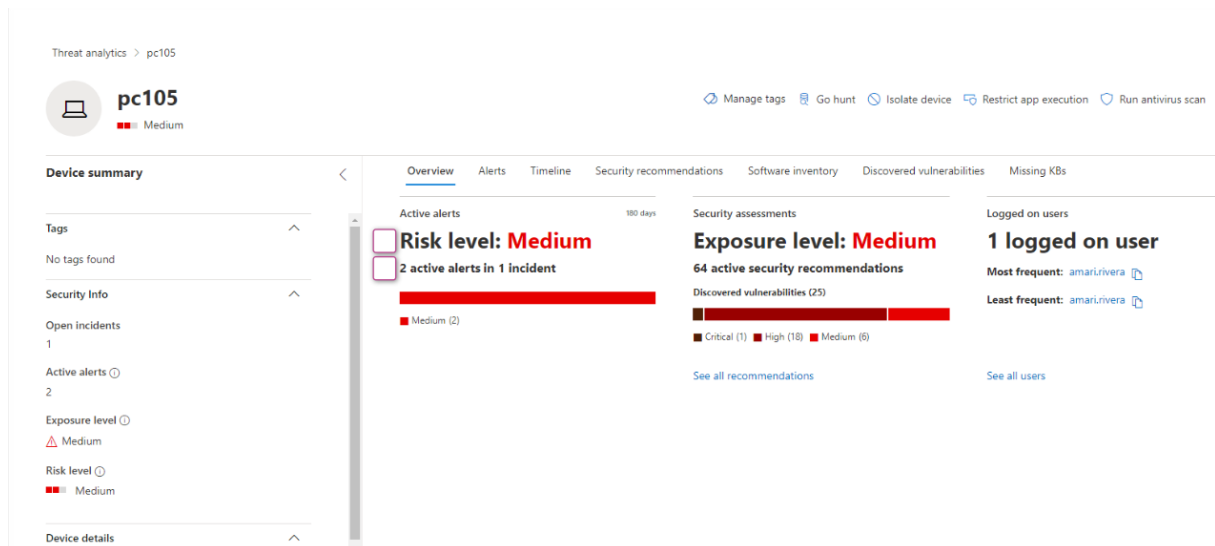
**Rules for auto-applying this label**  
Exchange email 1 rule  
SharePoint 1 rule  
OneDrive 1 rule  
[Edit](#)

**Mode**  
Simulation

Back

Create policy

On continue la recherche sur la machine de Amari dans Microsoft 365 Defender



On peut même avoir un Shell sur la machine pour checker les fichiers.

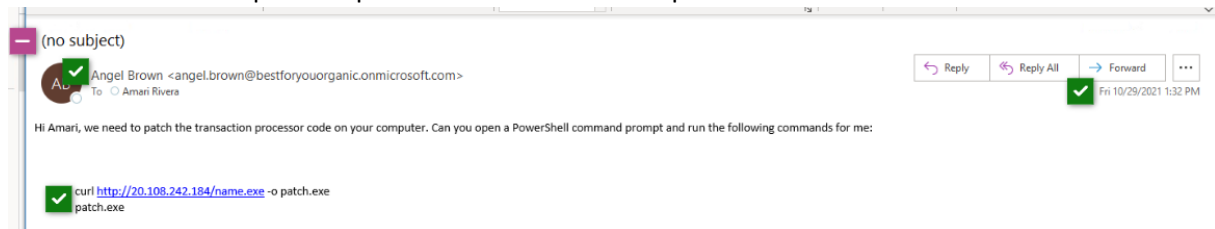
Command console    Command log

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

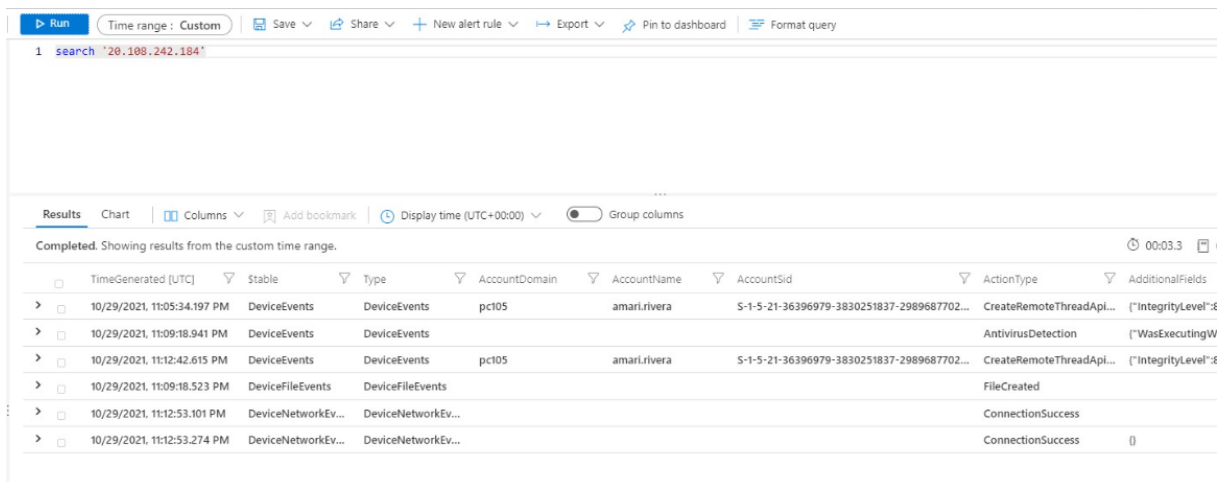
C:\> cd \patch

C:\patch> dir
Path                Created             Modified            Size    Is Directory  Read OnlyH
-----
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
```

J'ai utilisé Microsoft purview pour trouver ou l'adresse ip a été mentionné.



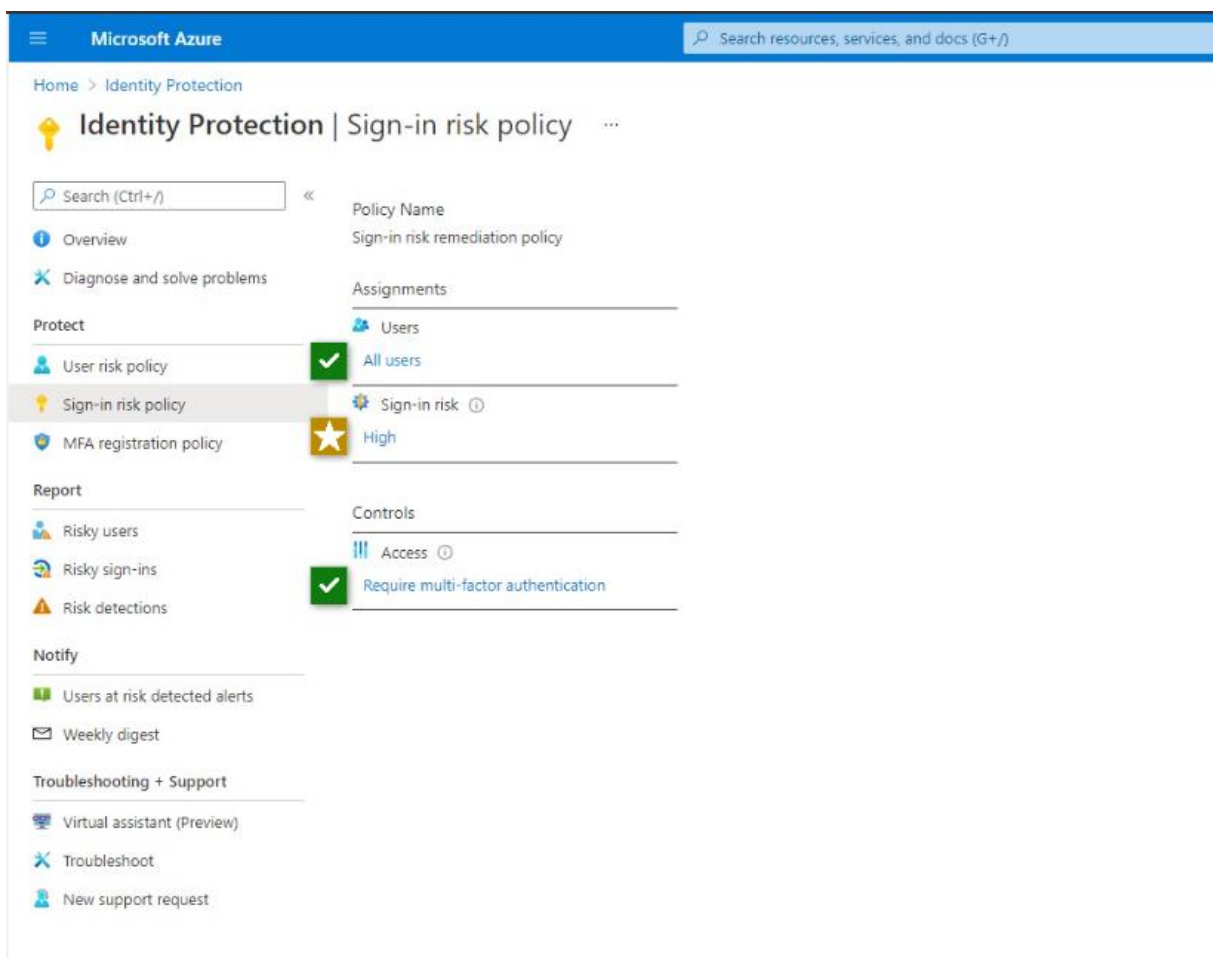
Dans Microsoft Sentinel on peut checker s'il y a d'autre machine connecter à l'adresse IP suspectieuse.



The screenshot shows the Microsoft Sentinel interface with a query executed. The query is: `search "20.108.242.184"`. The results are displayed in a table with columns: TimeGenerated (UTC), Stable, Type, AccountDomain, AccountName, AccountSid, ActionType, and AdditionalFields. The results show several events, including DeviceEvents, DeviceFileEvents, and DeviceNetworkEvents, all originating from the account 'amari.rivera' in the 'pct105' domain. The events include actions like 'CreateRemoteThreadApi...', 'AntivirusDetection', 'FileCreated', and 'ConnectionSuccess'.

TimeGenerated (UTC)	Stable	Type	AccountDomain	AccountName	AccountSid	ActionType	AdditionalFields
10/29/2021, 11:05:34.197 PM		DeviceEvents	pct105	amari.rivera	S-1-5-21-36396979-3830251837-2989687702...	CreateRemoteThreadApi...	["IntegrityLevel":d
10/29/2021, 11:09:18.941 PM		DeviceEvents				AntivirusDetection	["WasExecutingW
10/29/2021, 11:12:42.615 PM		DeviceEvents	pct105	amari.rivera	S-1-5-21-36396979-3830251837-2989687702...	CreateRemoteThreadApi...	["IntegrityLevel":d
10/29/2021, 11:09:18.523 PM		DeviceFileEvents				FileCreated	
10/29/2021, 11:12:53.101 PM		DeviceNetworkEv...				ConnectionSuccess	
10/29/2021, 11:12:53.274 PM		DeviceNetworkEv...				ConnectionSuccess	

Sur Azure AD on configure la protection de l'identité et des politiques de connexion pour se protéger contre les attaques d'identité. On veut assurer que les utilisateurs à risque sont corrigés avant d'accéder à l'environnement.



The screenshot shows the Microsoft Azure portal interface for Identity Protection. The left sidebar contains navigation links: Overview, Diagnose and solve problems, Protect, Report, and Notify. The main content area is titled 'Identity Protection | Sign-in risk policy'. It shows the 'Sign-in risk remediation policy' with the following configuration:

- Policy Name:** Sign-in risk remediation policy
- Assignments:**
  - Users:** All users (checked)
  - Sign-in risk:** High (checked)
- Controls:**
  - Access:** Require multi-factor authentication (checked)

The 'Protect' section is expanded, showing the 'Sign-in risk policy' selected. The 'Report' section shows 'Risky users', 'Risky sign-ins', and 'Risk detections'. The 'Notify' section shows 'Users at risk detected alerts' and 'Weekly digest'. The 'Troubleshooting + Support' section shows 'Virtual assistant (Preview)', 'Troubleshoot', and 'New support request'.

Durant l'enquête, il a été révélé que la machine d'Angel Brown était compromise. Cependant, aucun incident ou alerte n'avait été préalablement signalé.

The screenshot shows the Microsoft Defender Security Center interface for device **pc067**. The left sidebar contains a 'Device summary' section with 'Tags' (No tags found), 'Security Info' (Open incidents: 0, Active alerts: 0, Exposure level: Medium, Risk level: None), and 'Device details' (Domain: Workgroup, OS: Windows 11 64-bit, Version 21H2, Build 22000, Health state: Inactive, Data sensitivity: None, IP addresses). The main area has tabs for Overview, Alerts, Timeline, Security recommendations, Software inventory, Discovered vulnerabilities, and Missing KBs. The 'Overview' tab is active, showing 'Active alerts' (Risk level: No known risks), 'Security assessments' (Exposure level: Medium, 29 active security recommendations, Discovered vulnerabilities: 26), and 'Logged on users' (1 logged on user: angel.brown).

On investigate la machine de Tomo car il est lié a la machine de Angel.

The screenshot shows the Microsoft Defender Security Center interface for device **pc034**. The left sidebar contains a 'Device summary' section with 'Tags' (No tags found), 'Security Info' (Open incidents: 0, Active alerts: 0, Exposure level: None, Risk level: None), and 'Device details' (Domain: Workgroup, OS: Windows 11 64-bit, Version 21H2, Build 22000, Health state: Inactive, Data sensitivity: None, IP addresses). The main area has tabs for Overview, Alerts, Timeline, Security recommendations, and Software inventory. The 'Timeline' tab is active, showing a list of events. One event is selected: 'mstsc.exe established connection with 13.68.237.45:3389'. The right pane shows the 'Event info' and 'Event entities graph' for this event. The 'Event info' section includes: Event (mstsc.exe established connection with 13.68.237.45:3389), Event time (12/15/2021, 4:55 PM), Action type (ConnectionSuccess), User (pc034\Tomo.Takanashi), and Entities (explorer.exe > mstsc.exe > 13.68.237.45). The 'Event entities graph' section shows a process tree starting with explorer.exe, which spawned mstsc.exe. The details for mstsc.exe are: Process name (mstsc.exe), Execution time (12/15/2021, 4:55:03.011 PM), Path (c:\windows\system32\mstsc.exe), Integrity level (Medium), Access privileges (IUA), Process ID (5968), Command line (\"mstsc.exe\"), File name (mstsc.exe), Full path (c:\windows\system32\mstsc.exe), SHA1 (6069582d43c237b44540b37431d0ee13b0cef4f5), SHA256 (1b5716270bc74247306d67f220cbb98fa1cacb3), Signer (Microsoft Windows), Issuer (Microsoft Windows Production PCA 2011), and Is PE (False).

En conclusion, après analyse de tous les indices, j'ai pu identifier la personne responsable de cette attaque : Angela.

Elle a utilisé la machine d'Amari pour télécharger le fichier malveillant et ainsi compromettre le système.

Mes résultats :

# Thanks for Playing!

Who Hacked? Keeping Up Appearances



**El Mehdi**

**12257** /20,000 Points

**14** Leads Completed