# |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.

A screenshot of a computer

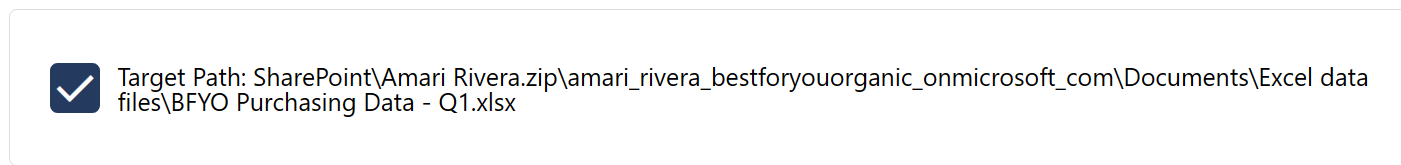
Description automatically generated

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

A diagram of a diagram of a keyword and conditions

Description automatically generated with medium confidence

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



1. Nous avons achevé cette étape

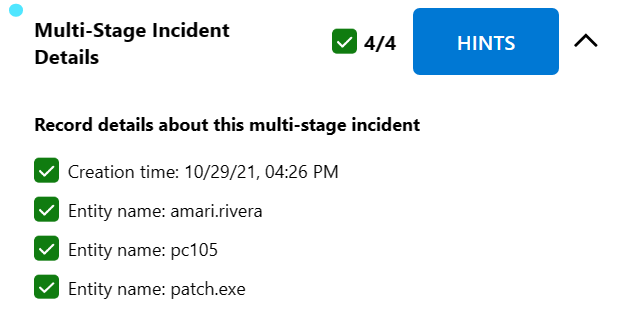
A computer screen shot of a computer screen

Description automatically generated

## 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)



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

1. Aller dans « Logs »

A screenshot of a computer

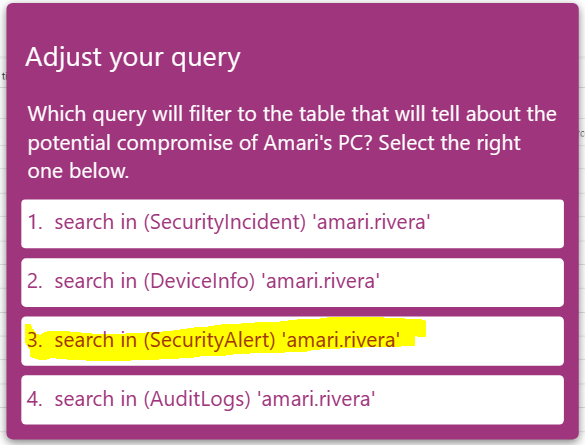
Description automatically generated

1. Mettre la query «search ‘amari.rivera’ »

A screenshot of a computer

Description automatically generated

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

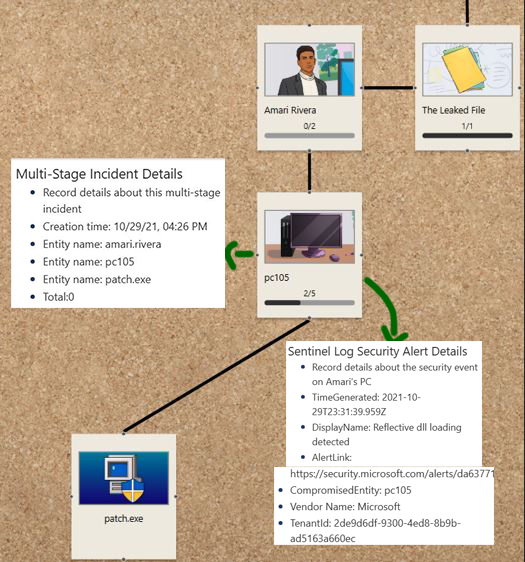


1. Nous retrouvons plusieurs détails importants pour mener notre enquête (2/4 Clues Collected)

A screenshot of a computer error message

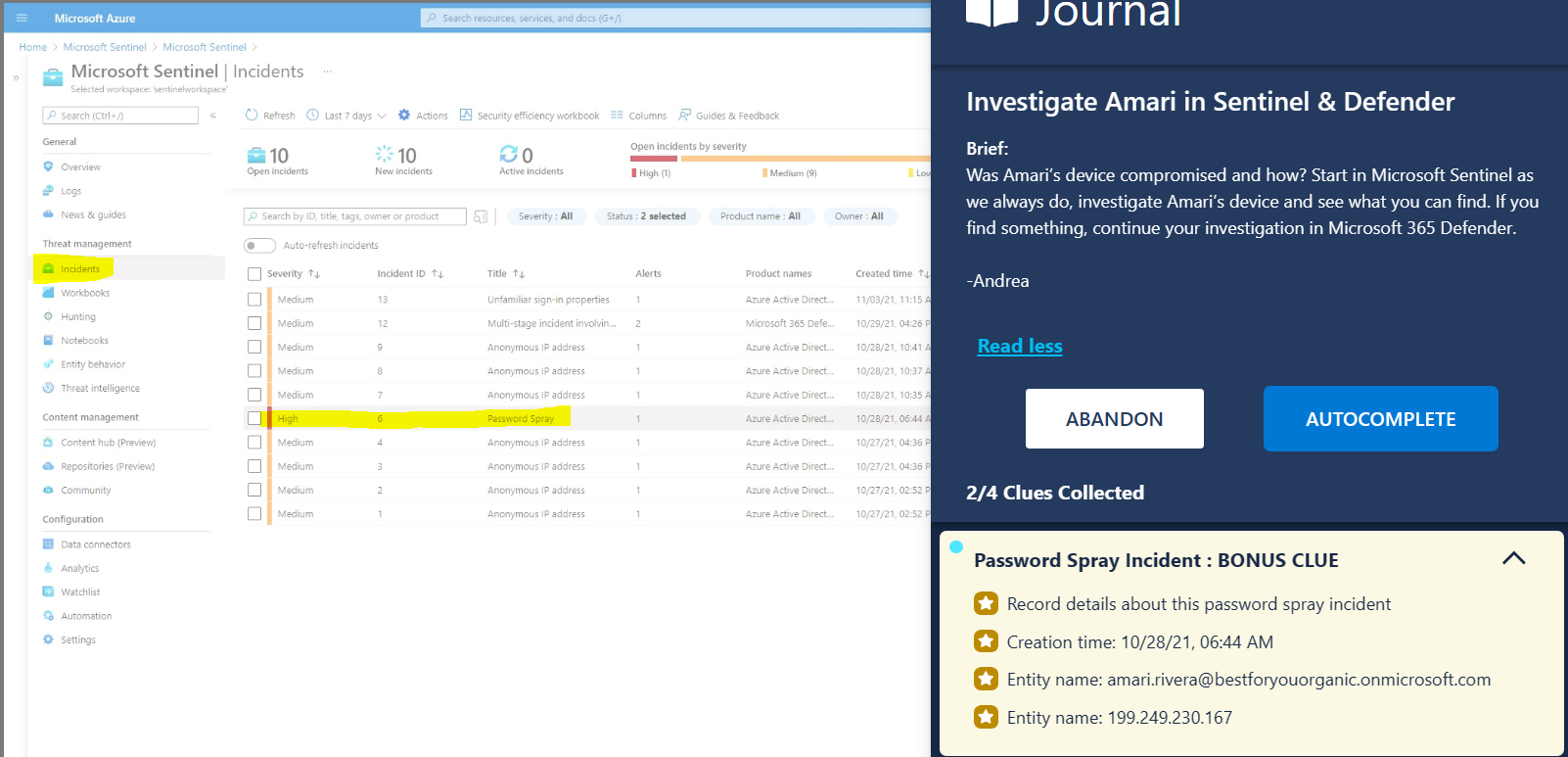
Description automatically generated

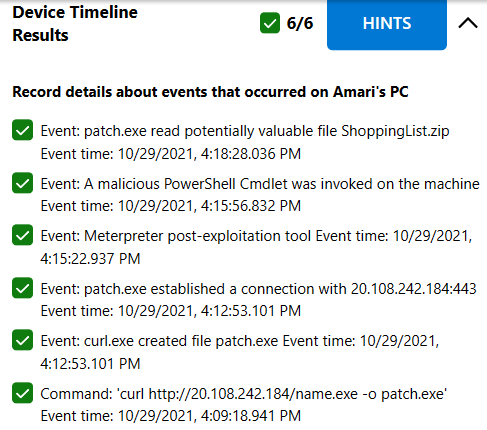
Nous observons une update de notre « Evidence Map »



Bonus :

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

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)



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

A screenshot of a computer

Description automatically generated

## 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 »

A screenshot of a phone

Description automatically generated

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

A close up of a password

Description automatically generated

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

A close-up of a sign

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

A screenshot of a phone

Description automatically generated

De même pour Emily Braun (4/4 Bonus)

A screenshot of a phone

Description automatically generated

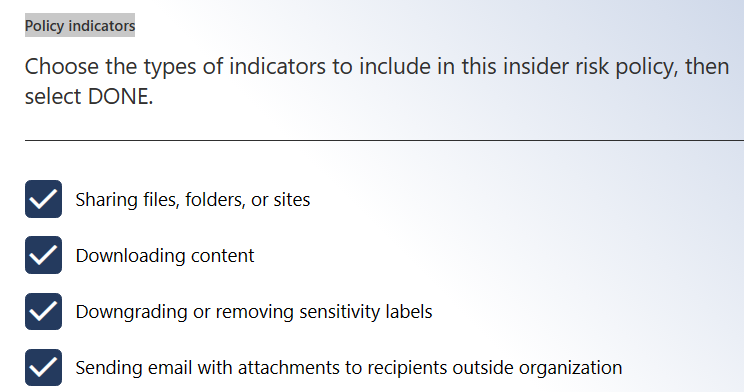
## Set Up Insider Risk Policy

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](mailto: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 »



# | 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
* A close-up of a computer screen

  Description automatically generatedPolicy Name: eCommerce PCI DSS auto-labeling policy : tout cocher
* Choose a label to auto-apply : Confidential eCommerce App Team

A screenshot of a computer screen

Description automatically generated

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

A screenshot of a computer

Description automatically generated

## 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

A screenshot of a search bar

Description automatically generated

* Results : Cliquer sur le premier device network events :

A screenshot of a device network event

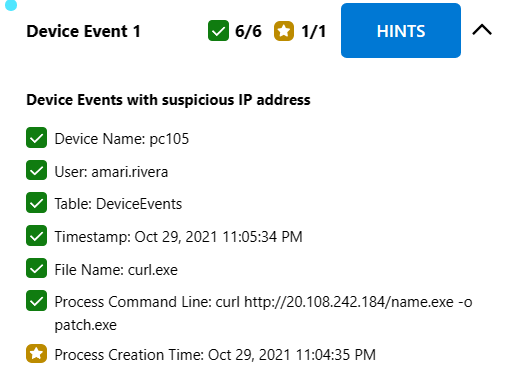
Description automatically generated

* Results : Cliquer sur le deuxième device network events :

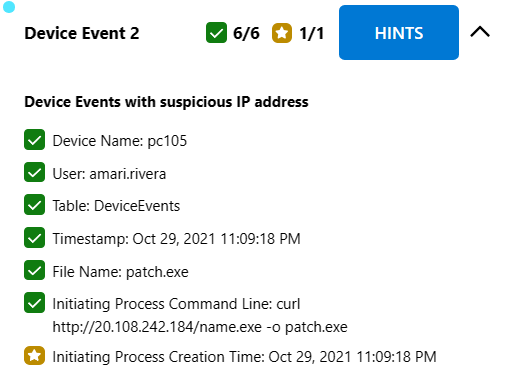
A screenshot of a device network

Description automatically generated

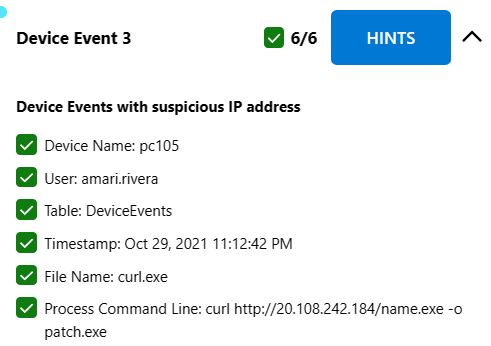
* Results : Cliquer sur le DeviceEvents 1 :



* Results : Cliquer sur le DeviceEvents 2 :



* Results : Cliquer sur le DeviceEvents 3 :



* Results : Cliquer sur le DeviceFileEvents:

A screenshot of a device file events

Description automatically generated

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

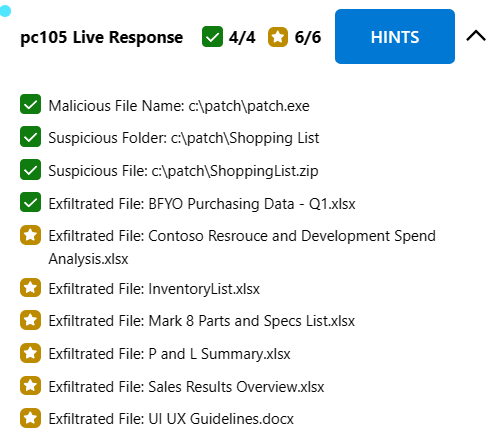
A screenshot of a computer

Description automatically generated

Nous pouvons aussi naviguer dans l’ordinateur compromis :

A screenshot of a computer program

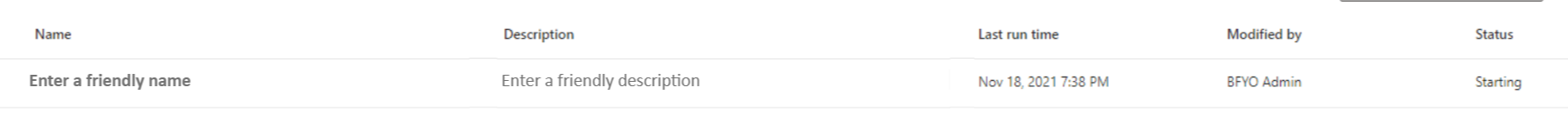
Description automatically generated



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

A screenshot of a computer

Description automatically generated

## 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.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## 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

A computer screen with a white background

Description automatically generated

A screenshot of a computer

Description automatically generated

# | 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

A screenshot of a computer screen

Description automatically generated

Sign-in risk policy

A screenshot of a sign in policy

Description automatically generated

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’

A screenshot of a phone

Description automatically generated

A screenshot of a computer error

Description automatically generated

A screenshot of a test

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A white background with black text

Description automatically generated

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?

A screenshot of a phone

Description automatically generated

A screenshot of a computer

Description automatically generated

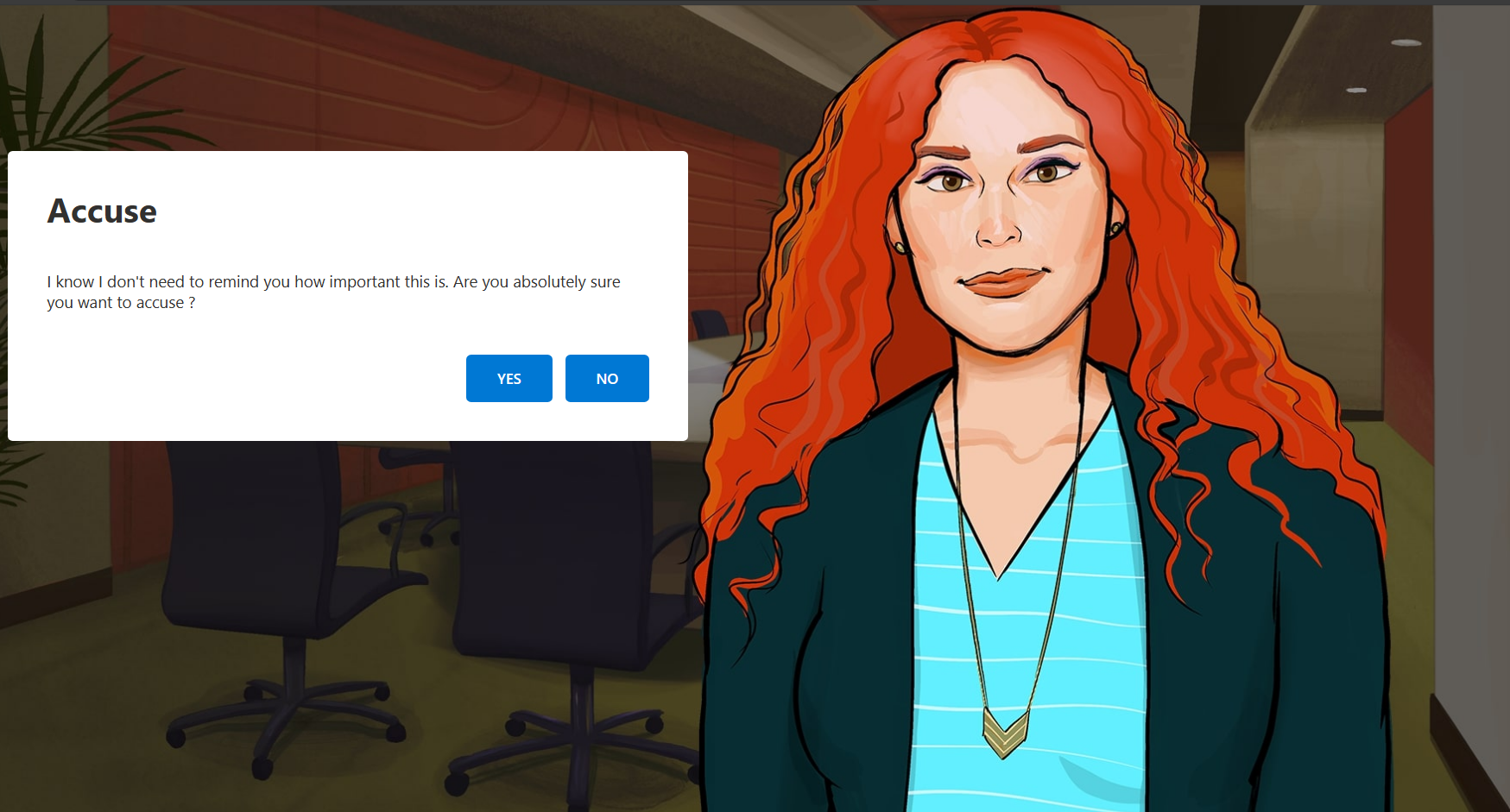
Investigate Tomo’s Device in Sentinel and Microsoft 365 Defender

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.

A screenshot of a computer

Description automatically generated

Nous ne trouvons rien de suspect



A screenshot of a computer screen

Description automatically generated