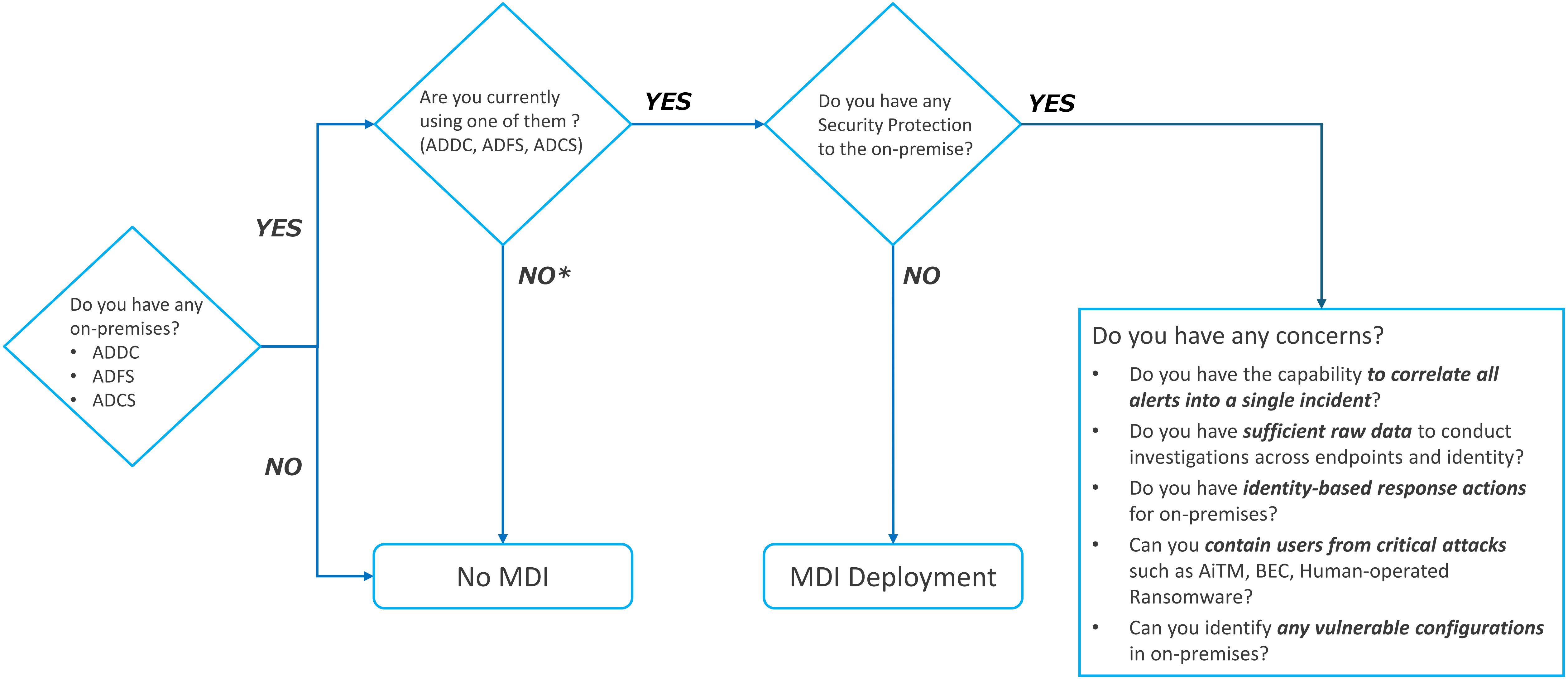
# The reasons to consider deploying

## Microsoft Defender for Identity

*Kijo Ninja*

# You might need cloud-based on-premise protection ?



Do you have any on-premises?

- ADDC
- ADFS
- ADCS

YES

NO

Are you currently using one of them ? (ADDC, ADFS, ADCS)

YES

NO*

No MDI

Do you have any Security Protection to the on-premise?

YES

NO

MDI Deployment

Do you have any concerns?

- Do you have the capability ***to correlate all alerts into a single incident***?
- Do you have ***sufficient raw data*** to conduct investigations across endpoints and identity?
- Do you have ***identity-based response actions*** for on-premises?
- Can you ***contain users from critical attacks*** such as AiTM, BEC, Human-operated Ransomware?
- Can you identify ***any vulnerable configurations*** in on-premises?

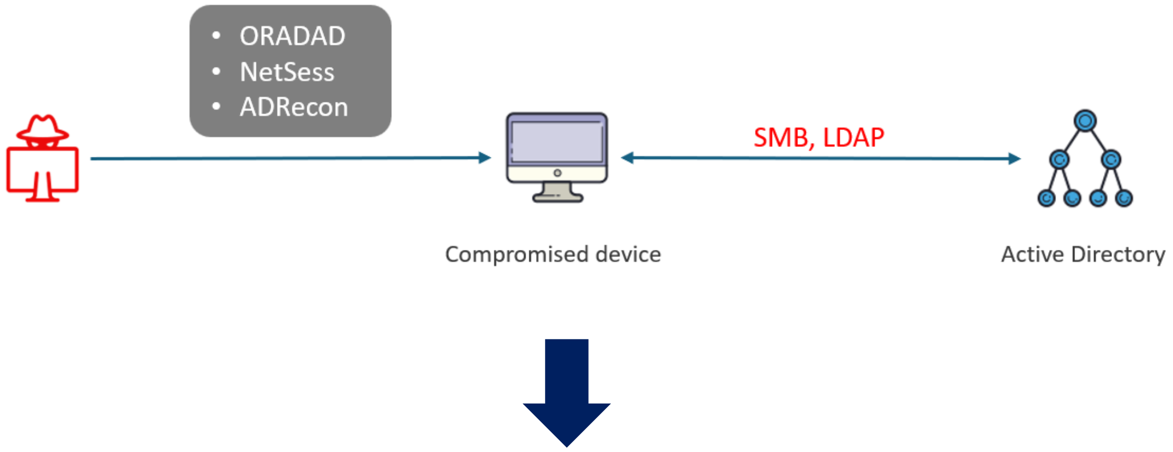
*Even if you are not currently using on-premises, you might have to consider deploying MDI due to potential security risks as long as you have them.

# Agenda

- Do you have the capability ***to correlate all alerts into a single incident***?
- Do you have ***sufficient raw data*** to conduct investigations across endpoints and identity?
- Do you have ***identity-based response actions*** for on-premises?
- Can you ***contain users from critical attacks*** such as AiTM, BEC, Human-operated Ransomware?
- Can you identify ***any vulnerable configurations*** in on-premises?

# MDE + MDI better together – Reconnaissance (SMB/LDAP)

Expand the visibility of breaches from endpoint to identity



- ORADAD
- NetSess
- ADRecon

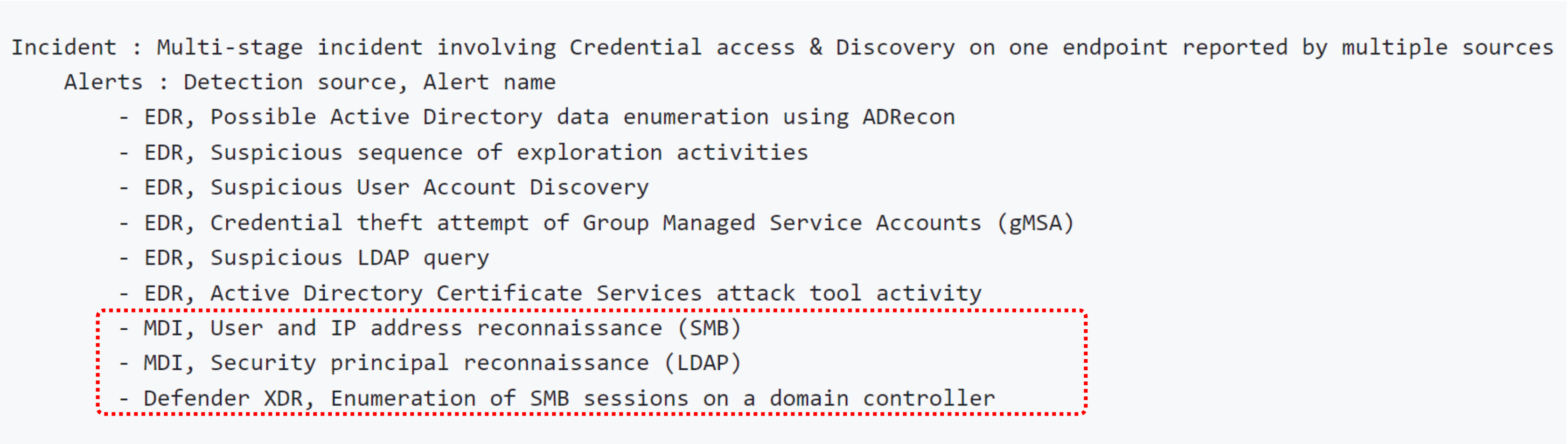
SMB, LDAP

Compromised device

Active Directory

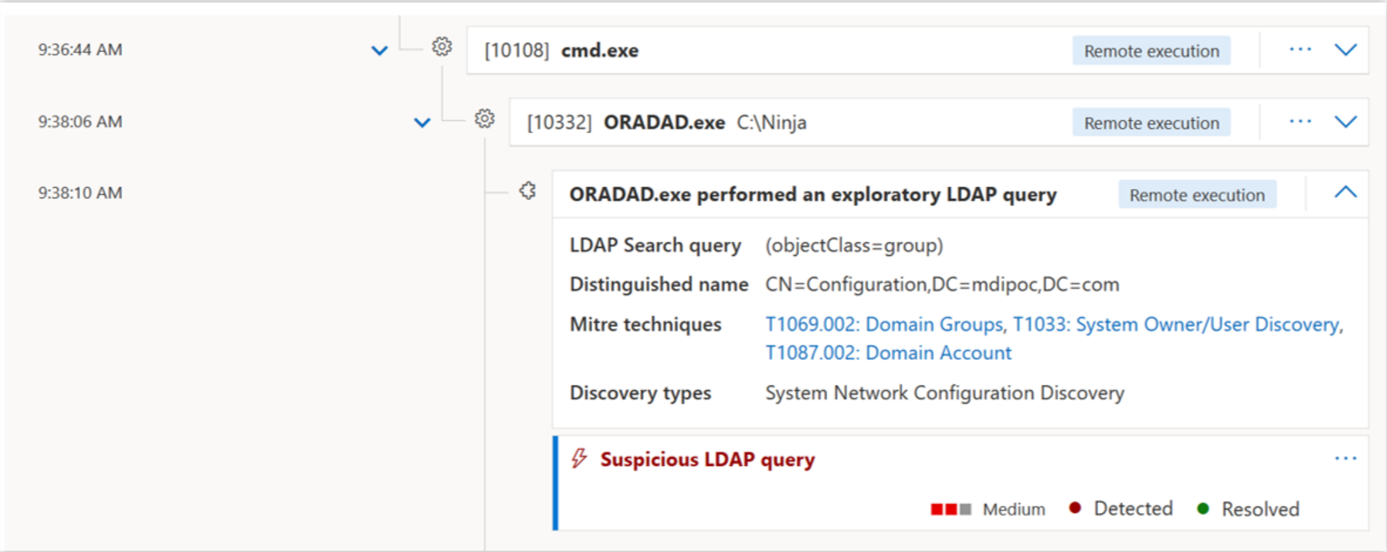
If you have these products, they generate alerts across endpoint and identity. Ultimately, these alerts correlate into one single incident.

Microsoft Defender XDR
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity



```
Incident : Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources
    Alerts : Detection source, Alert name
        - EDR, Possible Active Directory data enumeration using ADRecon
        - EDR, Suspicious sequence of exploration activities
        - EDR, Suspicious User Account Discovery
        - EDR, Credential theft attempt of Group Managed Service Accounts (gMSA)
        - EDR, Suspicious LDAP query
        - EDR, Active Directory Certificate Services attack tool activity
        - MDI, User and IP address reconnaissance (SMB)
        - MDI, Security principal reconnaissance (LDAP)
        - Defender XDR, Enumeration of SMB sessions on a domain controller
```

https://github.com/LearningKijo/SecurityResearcher-Note/blob/main/ProductResearch-Note-Folder/Day02-MDE-MDI-BetterTogether-Part2.md



9:36:44 AM [10108] **cmd.exe** Remote execution

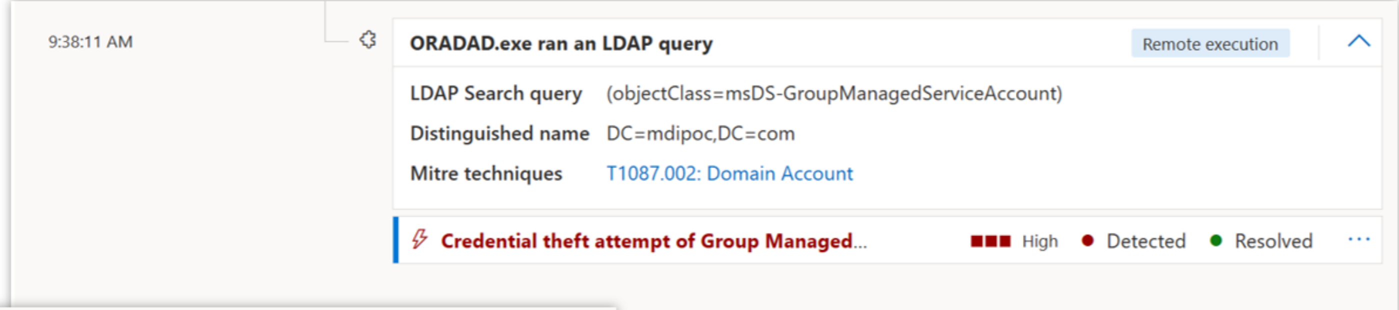
9:38:06 AM [10332] **ORADAD.exe** C:\Ninja Remote execution

9:38:10 AM **ORADAD.exe performed an exploratory LDAP query** Remote execution

| | |
|---|---|
| **LDAP Search query** | (objectClass=group) |
| **Distinguished name** | CN=Configuration,DC=mdipoc,DC=com |
| **Mitre techniques** | T1069.002: Domain Groups, T1033: System Owner/User Discovery, T1087.002: Domain Account |
| **Discovery types** | System Network Configuration Discovery |

**Suspicious LDAP query**

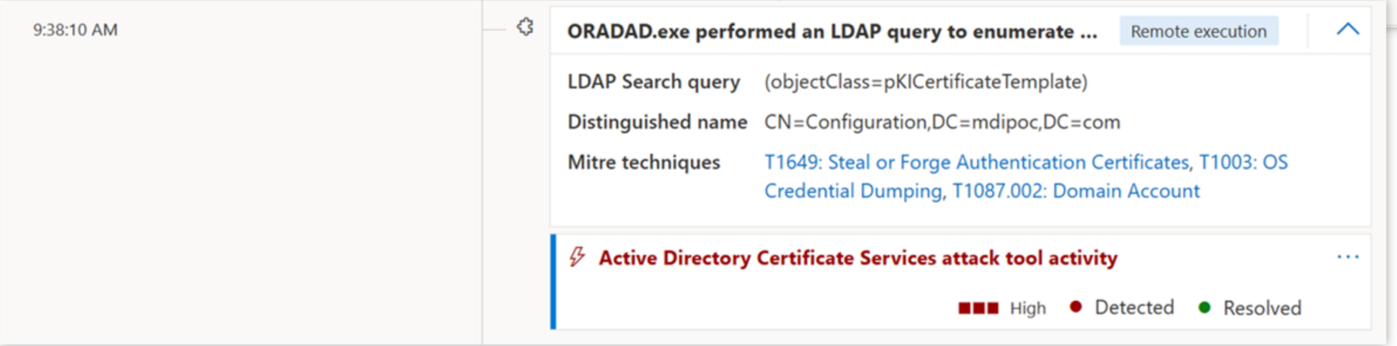
Medium ● Detected ● Resolved



9:38:11 AM **ORADAD.exe ran an LDAP query** Remote execution

| | |
|---|---|
| **LDAP Search query** | (objectClass=msDS-GroupManagedServiceAccount) |
| **Distinguished name** | DC=mdipoc,DC=com |
| **Mitre techniques** | T1087.002: Domain Account |

**Credential theft attempt of Group Managed...** High ● Detected ● Resolved



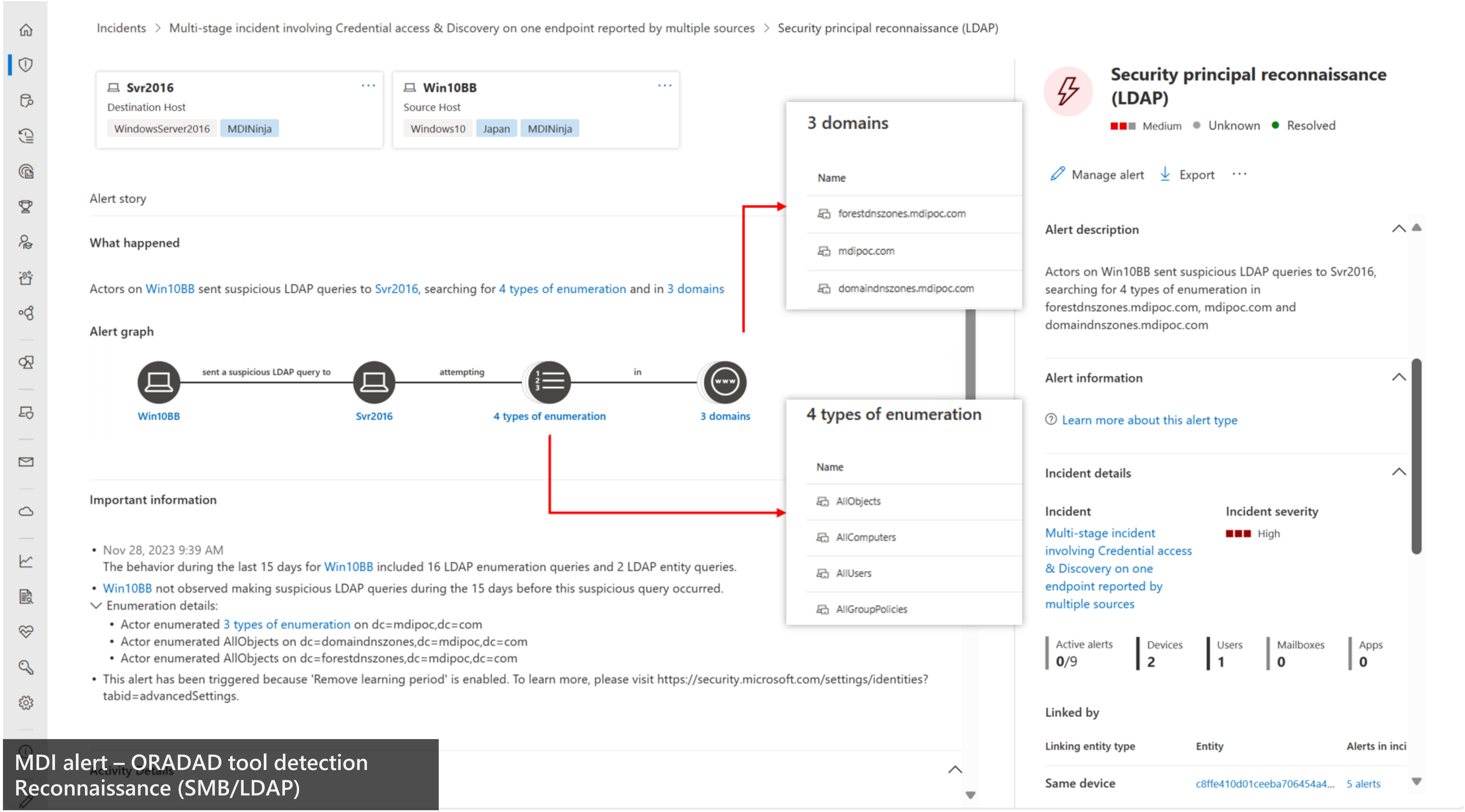
9:38:10 AM **ORADAD.exe performed an LDAP query to enumerate ...** Remote execution

| | |
|---|---|
| **LDAP Search query** | (objectClass=pKICertificateTemplate) |
| **Distinguished name** | CN=Configuration,DC=mdipoc,DC=com |
| **Mitre techniques** | T1649: Steal or Forge Authentication Certificates, T1003: OS Credential Dumping, T1087.002: Domain Account |

**Active Directory Certificate Services attack tool activity**

High ● Detected ● Resolved

## MDE alerts – ORADAD tool detection Reconnaissance (SMB/LDAP)



Incidents > Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources > Security principal reconnaissance (LDAP)

**Svr2016**
Destination Host
WindowsServer2016 | MDINinja

**Win10BB**
Source Host
Windows10 | Japan | MDINinja

Alert story

**What happened**

Actors on Win10BB sent suspicious LDAP queries to Svr2016, searching for 4 types of enumeration and in 3 domains

**Alert graph**

**3 domains**

| Name |
|---|
| forestdnszones.mdipoc.com |
| mdipoc.com |
| domaindnszones.mdipoc.com |

**4 types of enumeration**

| Name |
|---|
| AllObjects |
| AllComputers |
| AllUsers |
| AllGroupPolicies |

**Important information**

- Nov 28, 2023 9:39 AM
  The behavior during the last 15 days for Win10BB included 16 LDAP enumeration queries and 2 LDAP entity queries.
- Win10BB not observed making suspicious LDAP queries during the 15 days before this suspicious query occurred.
- Enumeration details:
  - Actor enumerated 3 types of enumeration on dc=mdipoc,dc=com
  - Actor enumerated AllObjects on dc=domaindnszones,dc=mdipoc,dc=com
  - Actor enumerated AllObjects on dc=forestdnszones,dc=mdipoc,dc=com
- This alert has been triggered because 'Remove learning period' is enabled. To learn more, please visit https://security.microsoft.com/settings/identities?tabid=advancedSettings.

Activity Details

**Security principal reconnaissance (LDAP)**

Medium ● Unknown ● Resolved

**Alert description**

Actors on Win10BB sent suspicious LDAP queries to Svr2016, searching for 4 types of enumeration in forestdnszones.mdipoc.com, mdipoc.com and domaindnszones.mdipoc.com

**Alert information**

Learn more about this alert type

**Incident details**

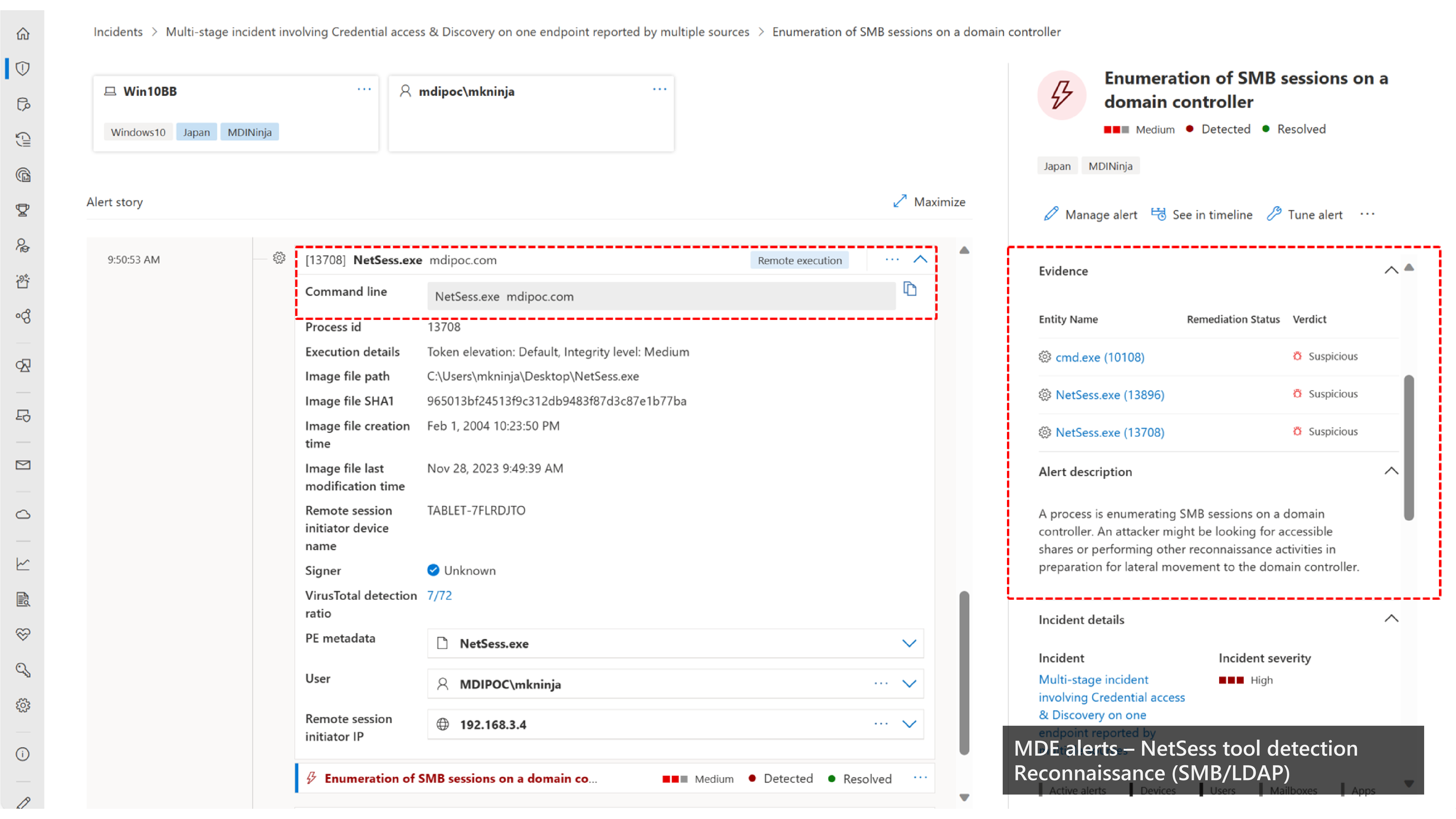
| Incident | Incident severity |
|---|---|
| Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources | High |

| Active alerts | Devices | Users | Mailboxes | Apps |
|---|---|---|---|---|
| 0/9 | 2 | 1 | 0 | 0 |

**Linked by**

| Linking entity type | Entity | Alerts in inci |
|---|---|---|
| Same device | c8ffe410d01ceeba706454a4... | 5 alerts |

MDI alert – ORADAD tool detection
Reconnaissance (SMB/LDAP)



Incidents > Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources > Enumeration of SMB sessions on a domain controller

**Win10BB**

Windows10 · Japan · MDINinja

**mdipoc\mkninja**

Alert story

9:50:53 AM

[13708] **NetSess.exe** mdipoc.com — Remote execution

| | |
|---|---|
| Command line | NetSess.exe mdipoc.com |
| Process id | 13708 |
| Execution details | Token elevation: Default, Integrity level: Medium |
| Image file path | C:\Users\mkninja\Desktop\NetSess.exe |
| Image file SHA1 | 965013bf24513f9c312db9483f87d3c87e1b77ba |
| Image file creation time | Feb 1, 2004 10:23:50 PM |
| Image file last modification time | Nov 28, 2023 9:49:39 AM |
| Remote session initiator device name | TABLET-7FLRDJTO |
| Signer | Unknown |
| VirusTotal detection ratio | 7/72 |
| PE metadata | **NetSess.exe** |
| User | **MDIPOC\mkninja** |
| Remote session initiator IP | **192.168.3.4** |

**Enumeration of SMB sessions on a domain co...** Medium ● Detected ● Resolved

## Enumeration of SMB sessions on a domain controller

Medium ● Detected ● Resolved

Japan · MDINinja

Manage alert · See in timeline · Tune alert

### Evidence

| Entity Name | Remediation Status | Verdict |
|---|---|---|
| cmd.exe (10108) | | Suspicious |
| NetSess.exe (13896) | | Suspicious |
| NetSess.exe (13708) | | Suspicious |

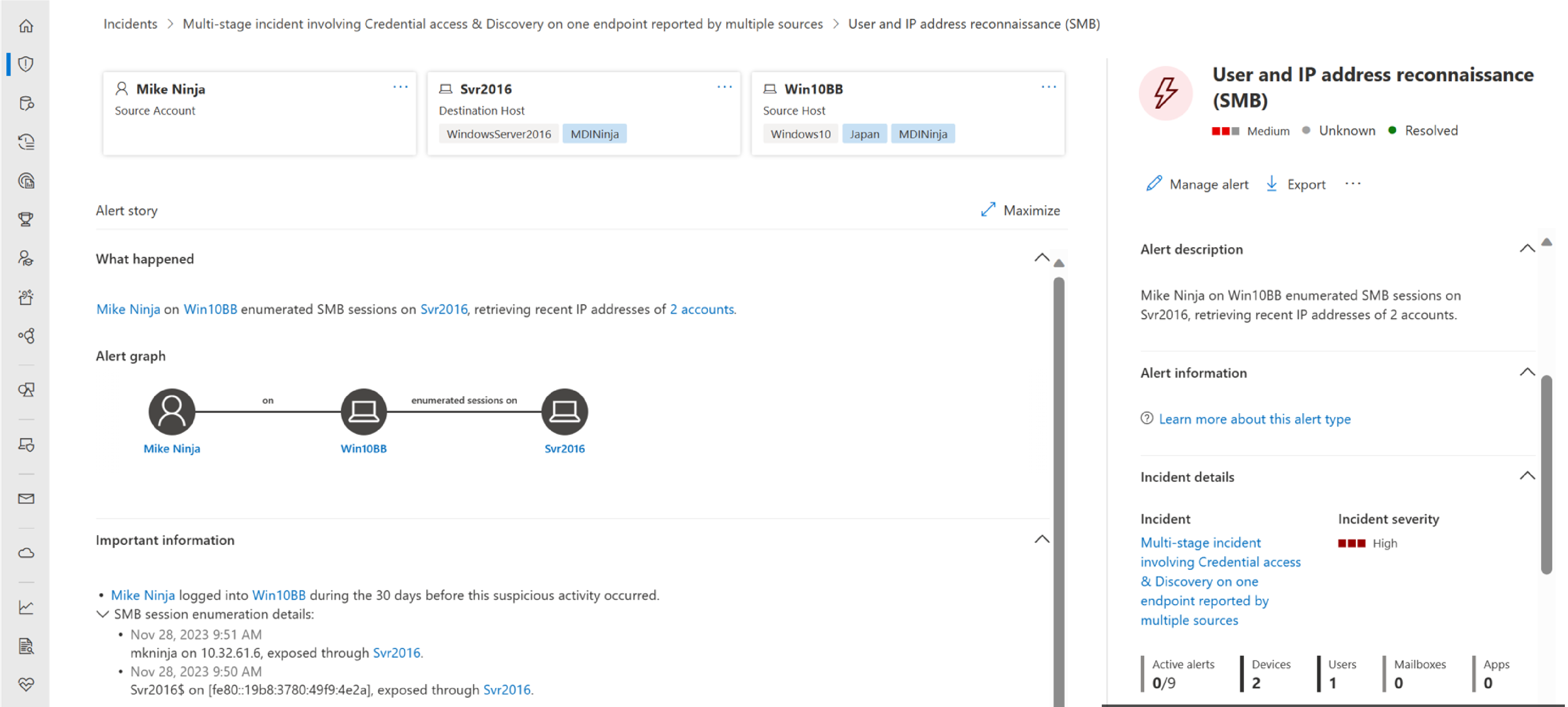
### Alert description

A process is enumerating SMB sessions on a domain controller. An attacker might be looking for accessible shares or performing other reconnaissance activities in preparation for lateral movement to the domain controller.

### Incident details

| Incident | Incident severity |
|---|---|
| Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources | High |

MDE alerts – NetSess tool detection Reconnaissance (SMB/LDAP)



Incidents > Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources > User and IP address reconnaissance (SMB)

**Mike Ninja**
Source Account

**Svr2016**
Destination Host
WindowsServer2016 MDINinja

**Win10BB**
Source Host
Windows10 Japan MDINinja

Alert story

Maximize

**What happened**

Mike Ninja on Win10BB enumerated SMB sessions on Svr2016, retrieving recent IP addresses of 2 accounts.

**Alert graph**

**Important information**

- Mike Ninja logged into Win10BB during the 30 days before this suspicious activity occurred.
- SMB session enumeration details:
  - Nov 28, 2023 9:51 AM
    mkninja on 10.32.61.6, exposed through Svr2016.
  - Nov 28, 2023 9:50 AM
    Svr2016$ on [fe80::19b8:3780:49f9:4e2a], exposed through Svr2016.

## User and IP address reconnaissance (SMB)

Medium ● Unknown ● Resolved

Manage alert Export ···

**Alert description**

Mike Ninja on Win10BB enumerated SMB sessions on Svr2016, retrieving recent IP addresses of 2 accounts.

**Alert information**

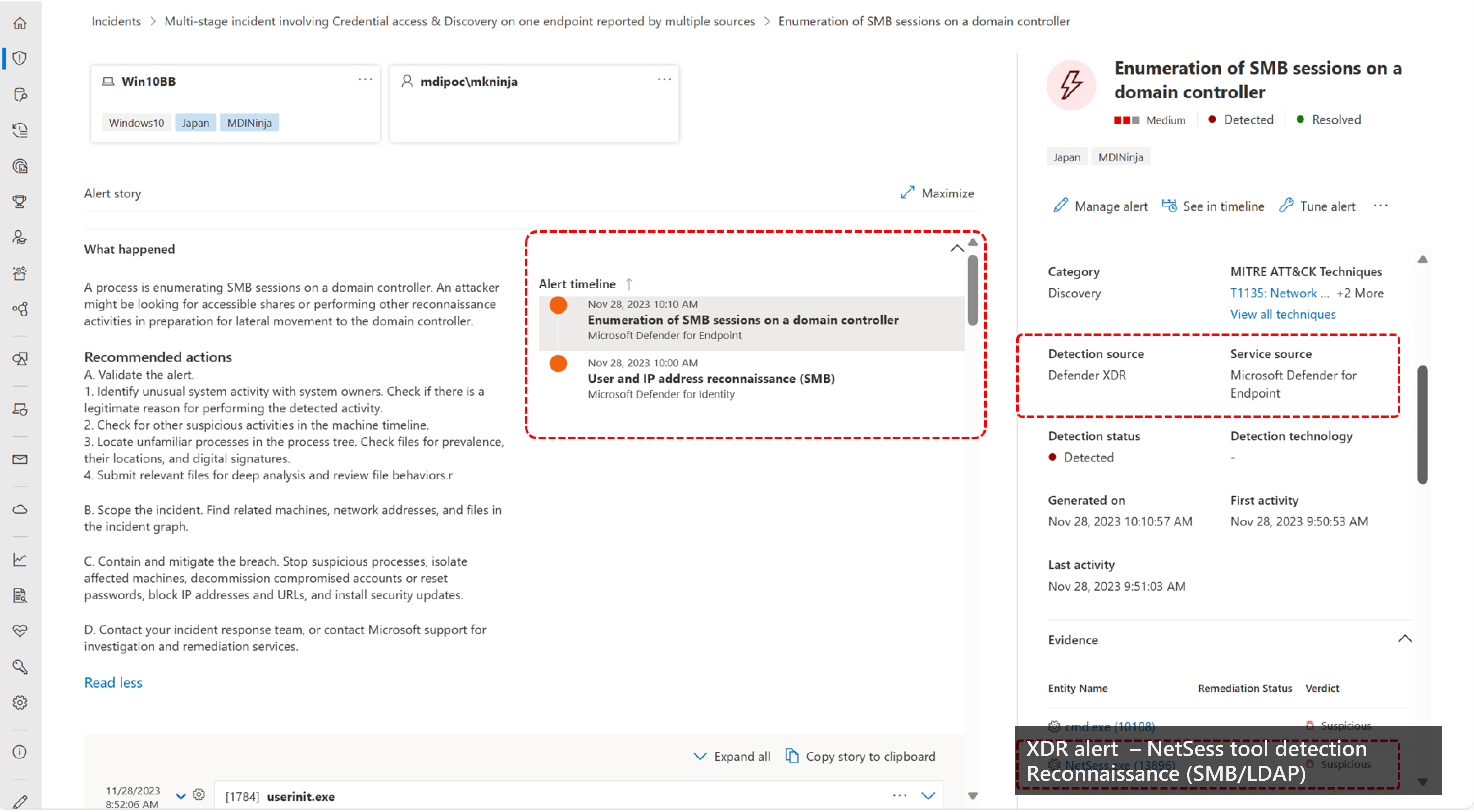
Learn more about this alert type

**Incident details**

| Incident | Incident severity |
|---|---|
| Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources | High |

| Active alerts | Devices | Users | Mailboxes | Apps |
|---|---|---|---|---|
| 0/9 | 2 | 1 | 0 | 0 |

MDI alert – NetSess tool detection Reconnaissance (SMB/LDAP)



Incidents > Multi-stage incident involving Credential access & Discovery on one endpoint reported by multiple sources > Enumeration of SMB sessions on a domain controller

Win10BB ···

Windows10 | Japan | MDINinja

mdipoc\mkninja ···

Alert story

Maximize

What happened

A process is enumerating SMB sessions on a domain controller. An attacker might be looking for accessible shares or performing other reconnaissance activities in preparation for lateral movement to the domain controller.

Recommended actions

A. Validate the alert.
1. Identify unusual system activity with system owners. Check if there is a legitimate reason for performing the detected activity.
2. Check for other suspicious activities in the machine timeline.
3. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.
4. Submit relevant files for deep analysis and review file behaviors.r

B. Scope the incident. Find related machines, network addresses, and files in the incident graph.

C. Contain and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset passwords, block IP addresses and URLs, and install security updates.

D. Contact your incident response team, or contact Microsoft support for investigation and remediation services.

Read less

Alert timeline ↑

- Nov 28, 2023 10:10 AM
  **Enumeration of SMB sessions on a domain controller**
  Microsoft Defender for Endpoint
- Nov 28, 2023 10:00 AM
  **User and IP address reconnaissance (SMB)**
  Microsoft Defender for Identity

Expand all | Copy story to clipboard

11/28/2023 8:52:06 AM | [1784] **userinit.exe** ···

## Enumeration of SMB sessions on a domain controller

Medium | ● Detected | ● Resolved

Japan | MDINinja

Manage alert | See in timeline | Tune alert | ···

| | |
|---|---|
| **Category**<br>Discovery | **MITRE ATT&CK Techniques**<br>T1135: Network ... +2 More<br>View all techniques |
| **Detection source**<br>Defender XDR | **Service source**<br>Microsoft Defender for Endpoint |
| **Detection status**<br>● Detected | **Detection technology**<br>- |
| **Generated on**<br>Nov 28, 2023 10:10:57 AM | **First activity**<br>Nov 28, 2023 9:50:53 AM |
| **Last activity**<br>Nov 28, 2023 9:51:03 AM | |

Evidence

| Entity Name | Remediation Status | Verdict |
|---|---|---|
| cmd.exe (10108) | | Suspicious |
| NetSess.exe (13896) | | Suspicious |

XDR alert – NetSess tool detection Reconnaissance (SMB/LDAP)

# Advanced hunting

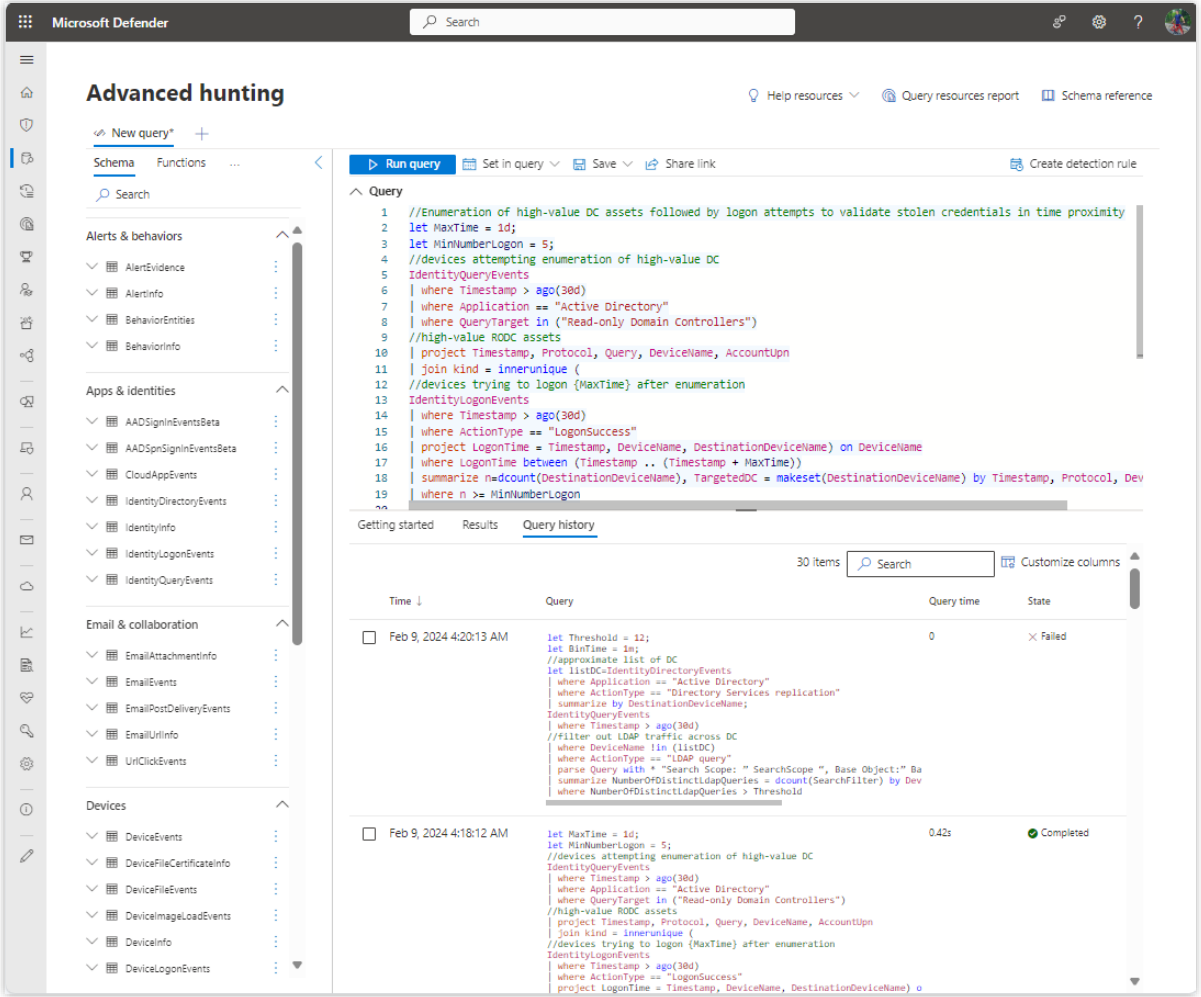
A query-based threat hunting tool that lets you explore up to 30 days of raw data.

### Enrich existing information

- Understand the impact of existing alerts
- Get more information on entities and IOCs

### Proactive hunting

- Proactive and interactive search for threats
- The power of knowing the network
- Not all threat scenarios begin with an alert



```
//Enumeration of high-value DC assets followed by logon attempts to validate stolen credentials in time proximity
let MaxTime = 1d;
let MinNumberLogon = 5;
//devices attempting enumeration of high-value DC
IdentityQueryEvents
| where Timestamp > ago(30d)
| where Application == "Active Directory"
| where QueryTarget in ("Read-only Domain Controllers")
//high-value RODC assets
| project Timestamp, Protocol, Query, DeviceName, AccountUpn
| join kind = innerunique (
//devices trying to logon {MaxTime} after enumeration
IdentityLogonEvents
| where Timestamp > ago(30d)
| where ActionType == "LogonSuccess"
| project LogonTime = Timestamp, DeviceName, DestinationDeviceName) on DeviceName
| where LogonTime between (Timestamp .. (Timestamp + MaxTime))
| summarize n=dcount(DestinationDeviceName), TargetedDC = makeset(DestinationDeviceName) by Timestamp, Protocol, Dev
| where n >= MinNumberLogon
```

| | Time ↓ | Query | Query time | State |
|---|---|---|---|---|
| □ | Feb 9, 2024 4:20:13 AM | (see below) | 0 | ✕ Failed |
| □ | Feb 9, 2024 4:18:12 AM | (see below) | 0.42s | ● Completed |

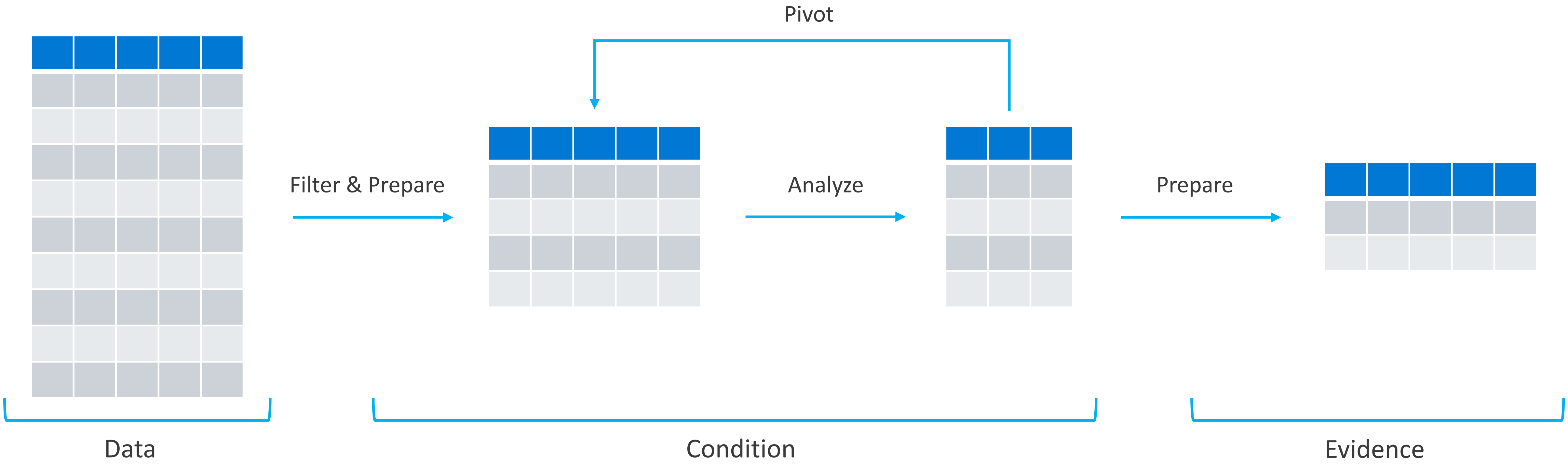
```
let Threshold = 12;
let BinTime = 1m;
//approximate list of DC
let listDC=IdentityDirectoryEvents
| where Application == "Active Directory"
| where ActionType == "Directory Services replication"
| summarize by DestinationDeviceName;
IdentityQueryEvents
| where Timestamp > ago(30d)
//filter out LDAP traffic across DC
| where DeviceName !in (listDC)
| where ActionType == "LDAP query"
| parse Query with * "Search Scope: " SearchScope ", Base Object:" Ba
| summarize NumberOfDistinctLdapQueries = dcount(SearchFilter) by Dev
| where NumberOfDistinctLdapQueries > Threshold
```

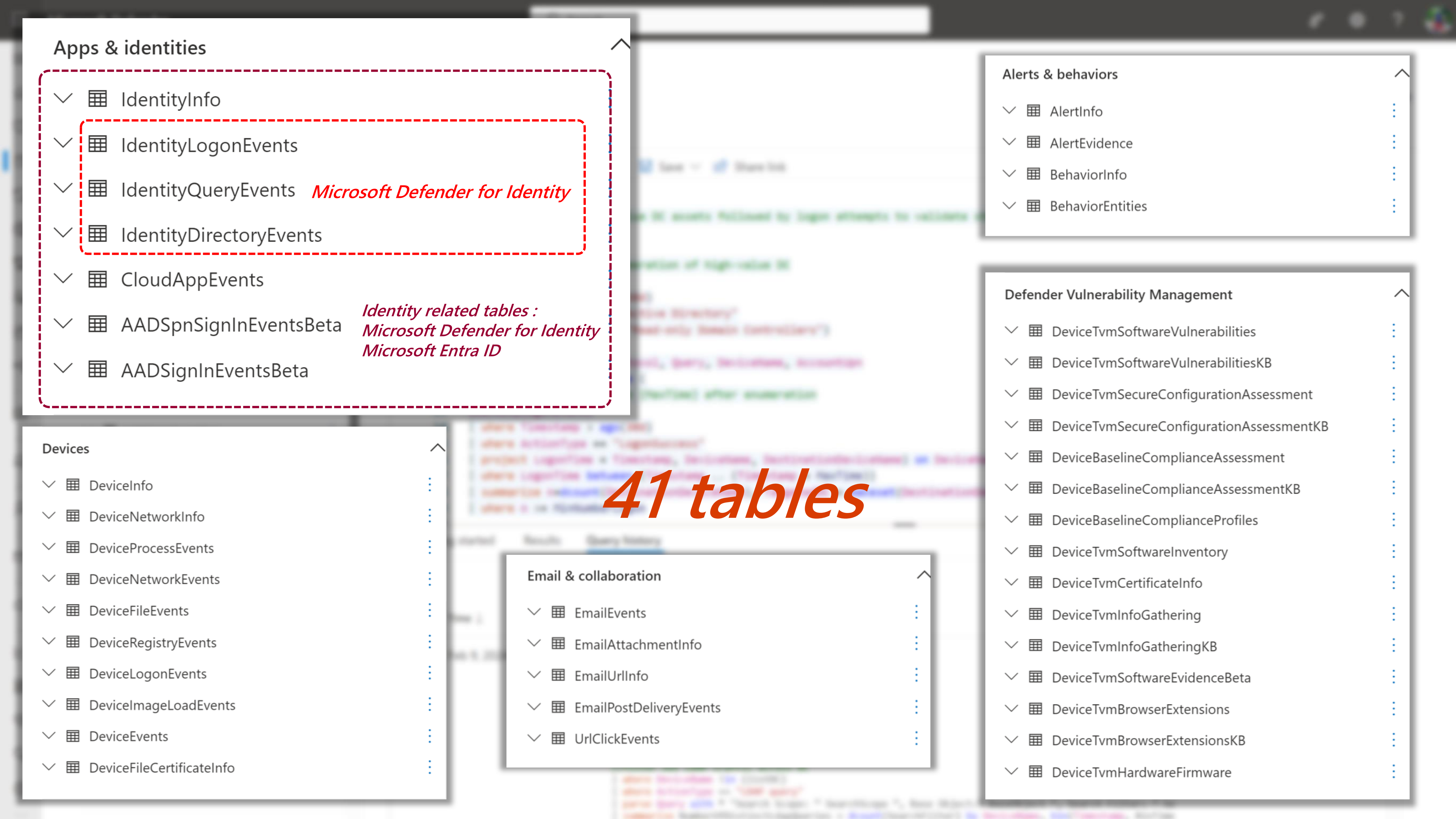
```
let MaxTime = 1d;
let MinNumberLogon = 5;
//devices attempting enumeration of high-value DC
IdentityQueryEvents
| where Timestamp > ago(30d)
| where Application == "Active Directory"
| where QueryTarget in ("Read-only Domain Controllers")
//high-value RODC assets
| project Timestamp, Protocol, Query, DeviceName, AccountUpn
| join kind = innerunique (
//devices trying to logon {MaxTime} after enumeration
IdentityLogonEvents
| where Timestamp > ago(30d)
| where ActionType == "LogonSuccess"
| project LogonTime = Timestamp, DeviceName, DestinationDeviceName) o
```

# KQL

KQL is a powerful language for hunting specific activities and data. For example, threat hunters use KQL to find suspicious activities in Advanced Hunting, Microsoft 365 Defender and Microsoft Sentinel.

```
DeviceEvents | where ActionType == "AntivirusDetection" | summarize count() by DeviceName | limit 3
```





Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

*Microsoft Defender for Identity*

*Identity related tables :*
*Microsoft Defender for Identity*
*Microsoft Entra ID*

Alerts & behaviors

- AlertInfo
- AlertEvidence
- BehaviorInfo
- BehaviorEntities

Defender Vulnerability Management

- DeviceTvmSoftwareVulnerabilities
- DeviceTvmSoftwareVulnerabilitiesKB
- DeviceTvmSecureConfigurationAssessment
- DeviceTvmSecureConfigurationAssessmentKB
- DeviceBaselineComplianceAssessment
- DeviceBaselineComplianceAssessmentKB
- DeviceBaselineComplianceProfiles
- DeviceTvmSoftwareInventory
- DeviceTvmCertificateInfo
- DeviceTvmInfoGathering
- DeviceTvmInfoGatheringKB
- DeviceTvmSoftwareEvidenceBeta
- DeviceTvmBrowserExtensions
- DeviceTvmBrowserExtensionsKB
- DeviceTvmHardwareFirmware

Devices

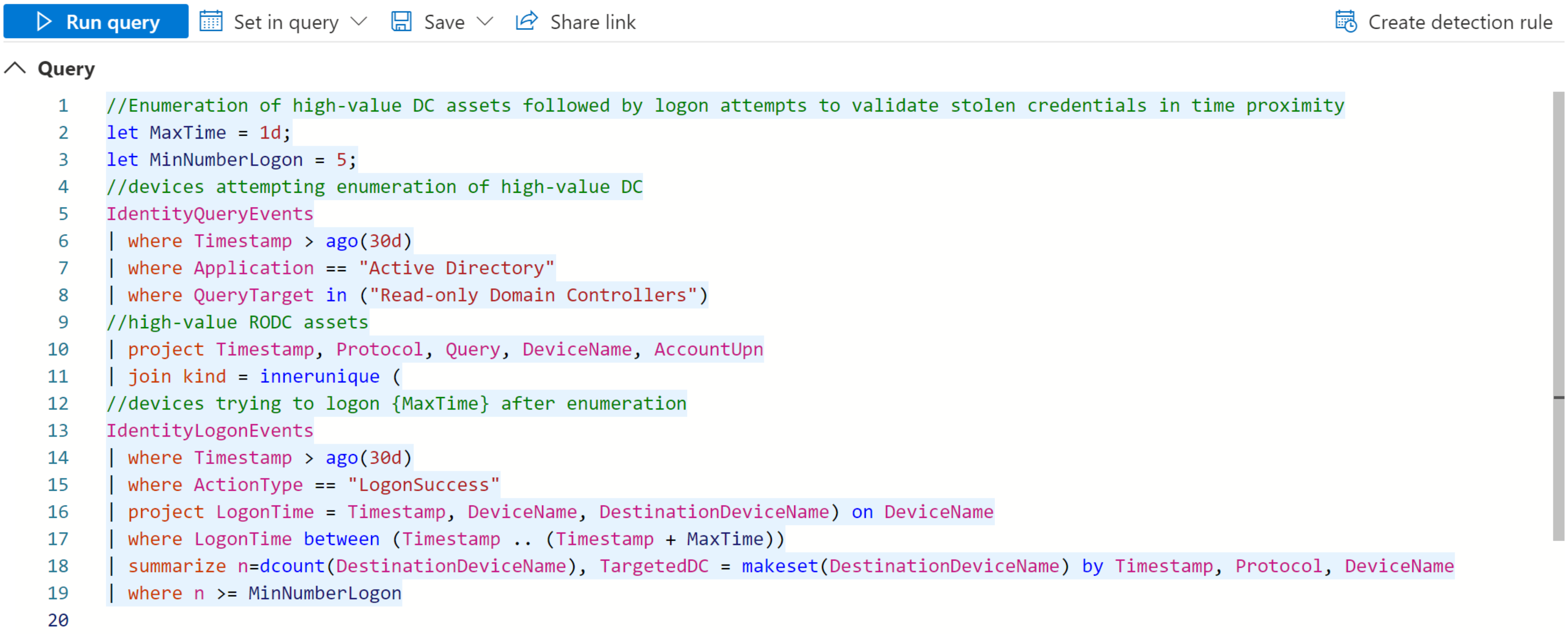
- DeviceInfo
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceRegistryEvents
- DeviceLogonEvents
- DeviceImageLoadEvents
- DeviceEvents
- DeviceFileCertificateInfo

Email & collaboration

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
- UrlClickEvents

*41 tables*

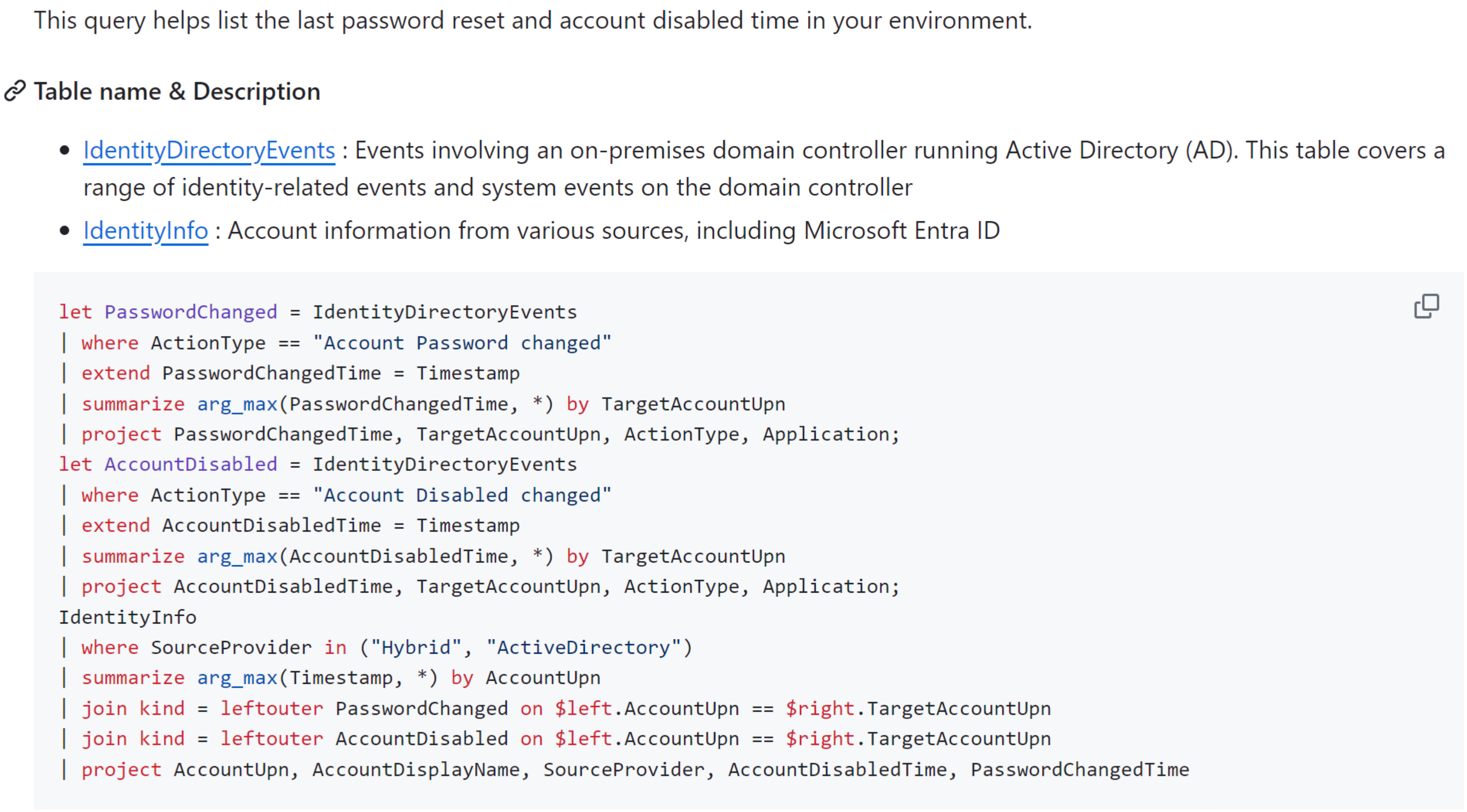
# e.g. solorigate (Midnight blizzard)



```
//Enumeration of high-value DC assets followed by logon attempts to validate stolen credentials in time proximity
let MaxTime = 1d;
let MinNumberLogon = 5;
//devices attempting enumeration of high-value DC
IdentityQueryEvents
| where Timestamp > ago(30d)
| where Application == "Active Directory"
| where QueryTarget in ("Read-only Domain Controllers")
//high-value RODC assets
| project Timestamp, Protocol, Query, DeviceName, AccountUpn
| join kind = innerunique (
//devices trying to logon {MaxTime} after enumeration
IdentityLogonEvents
| where Timestamp > ago(30d)
| where ActionType == "LogonSuccess"
| project LogonTime = Timestamp, DeviceName, DestinationDeviceName) on DeviceName
| where LogonTime between (Timestamp .. (Timestamp + MaxTime))
| summarize n=dcount(DestinationDeviceName), TargetedDC = makeset(DestinationDeviceName) by Timestamp, Protocol, DeviceName
| where n >= MinNumberLogon
```

https://www.microsoft.com/en-us/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

# e.g. Last Password Reset & Account Disabled Time List



This query helps list the last password reset and account disabled time in your environment.

### Table name & Description

- IdentityDirectoryEvents : Events involving an on-premises domain controller running Active Directory (AD). This table covers a range of identity-related events and system events on the domain controller
- IdentityInfo : Account information from various sources, including Microsoft Entra ID

```
let PasswordChanged = IdentityDirectoryEvents
| where ActionType == "Account Password changed"
| extend PasswordChangedTime = Timestamp
| summarize arg_max(PasswordChangedTime, *) by TargetAccountUpn
| project PasswordChangedTime, TargetAccountUpn, ActionType, Application;
let AccountDisabled = IdentityDirectoryEvents
| where ActionType == "Account Disabled changed"
| extend AccountDisabledTime = Timestamp
| summarize arg_max(AccountDisabledTime, *) by TargetAccountUpn
| project AccountDisabledTime, TargetAccountUpn, ActionType, Application;
IdentityInfo
| where SourceProvider in ("Hybrid", "ActiveDirectory")
| summarize arg_max(Timestamp, *) by AccountUpn
| join kind = leftouter PasswordChanged on $left.AccountUpn == $right.TargetAccountUpn
| join kind = leftouter AccountDisabled on $left.AccountUpn == $right.TargetAccountUpn
| project AccountUpn, AccountDisplayName, SourceProvider, AccountDisabledTime, PasswordChangedTime
```

https://github.com/LearningKijo/KQL/blob/main/KQL-XDR-Hunting/Identity-Microsoft-Defender-for-Identity/MDI-Query-Repository/03-Last-PasswordReset-AccountDisabled-TimeList.md

# Out-of-the-box KQL queries

*Microsoft kql queries*

- Threat analytics, Microsoft Defender XDR
- Microsoft Security Blog
- Azure-Sentinel/Hunting Queries at master · Azure/Azure-Sentinel

*GitHub (Not official queries from Microsoft)*

- reprise99/Sentinel-Queries
- FalconForceTeam/FalconFriday
- LearningKijo/KQL
- Bert-JanP/Hunting-Queries-Detection-Rules
- cyb3rmik3/KQL-threat-hunting-queries
- DanielpFR/MDI

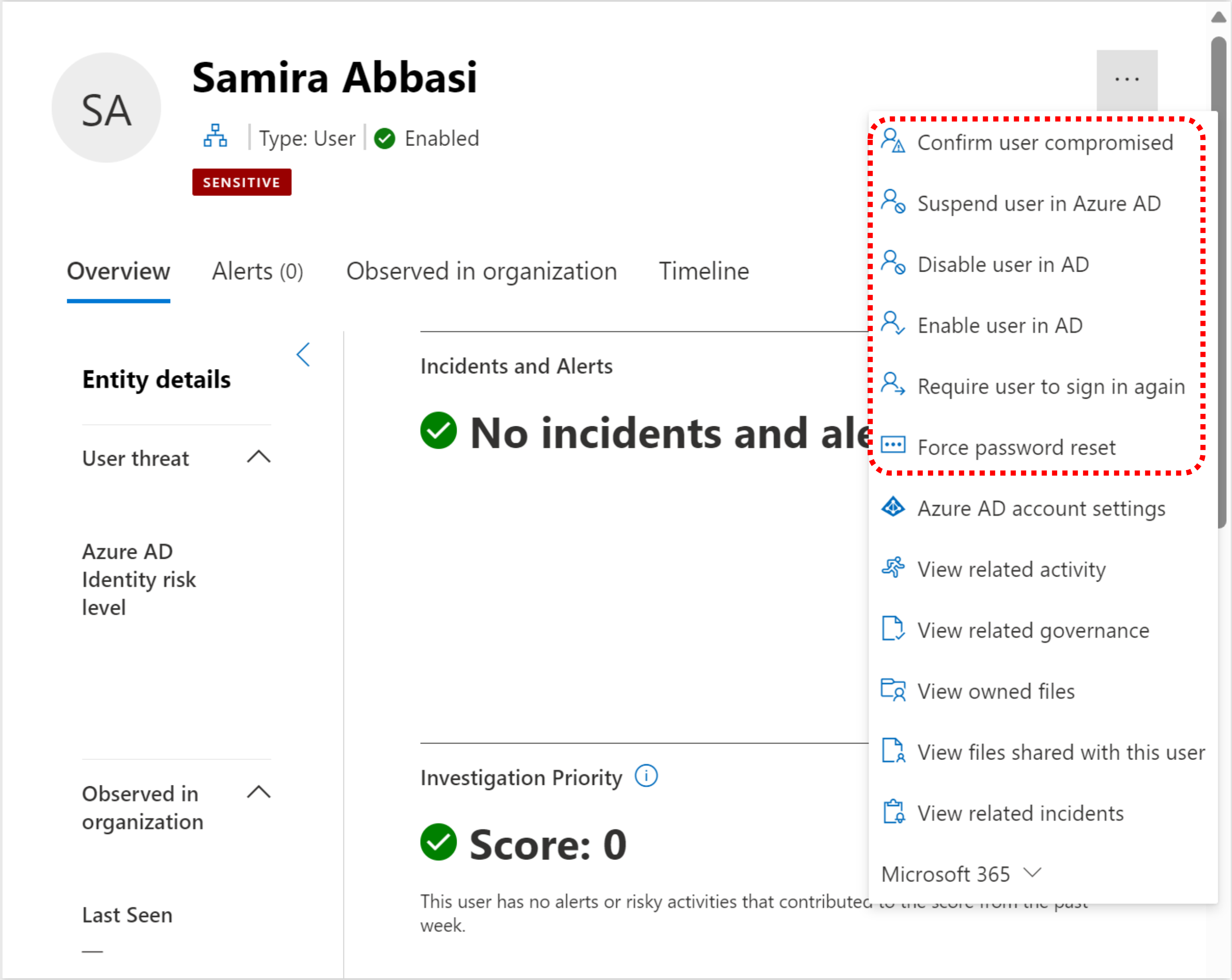
*Do you have* ***Identity-based response actions*** *for on-premise?*

MDI user response actions

- Disable/Enable user in Active Directory
- Reset user password

Other actions

- Suspend user in Azure AD (Entra ID)
- Require user to sign in again
- Confirm user compromised



# Samira Abbasi

SA

Type: User | ✓ Enabled

SENSITIVE

Overview | Alerts (0) | Observed in organization | Timeline

**Entity details**

User threat

Azure AD Identity risk level

Observed in organization

Last Seen

—

Incidents and Alerts

✓ No incidents and ale

Investigation Priority

✓ Score: 0

This user has no alerts or risky activities that contributed to the score from the past week.

# Automatic attack disruption

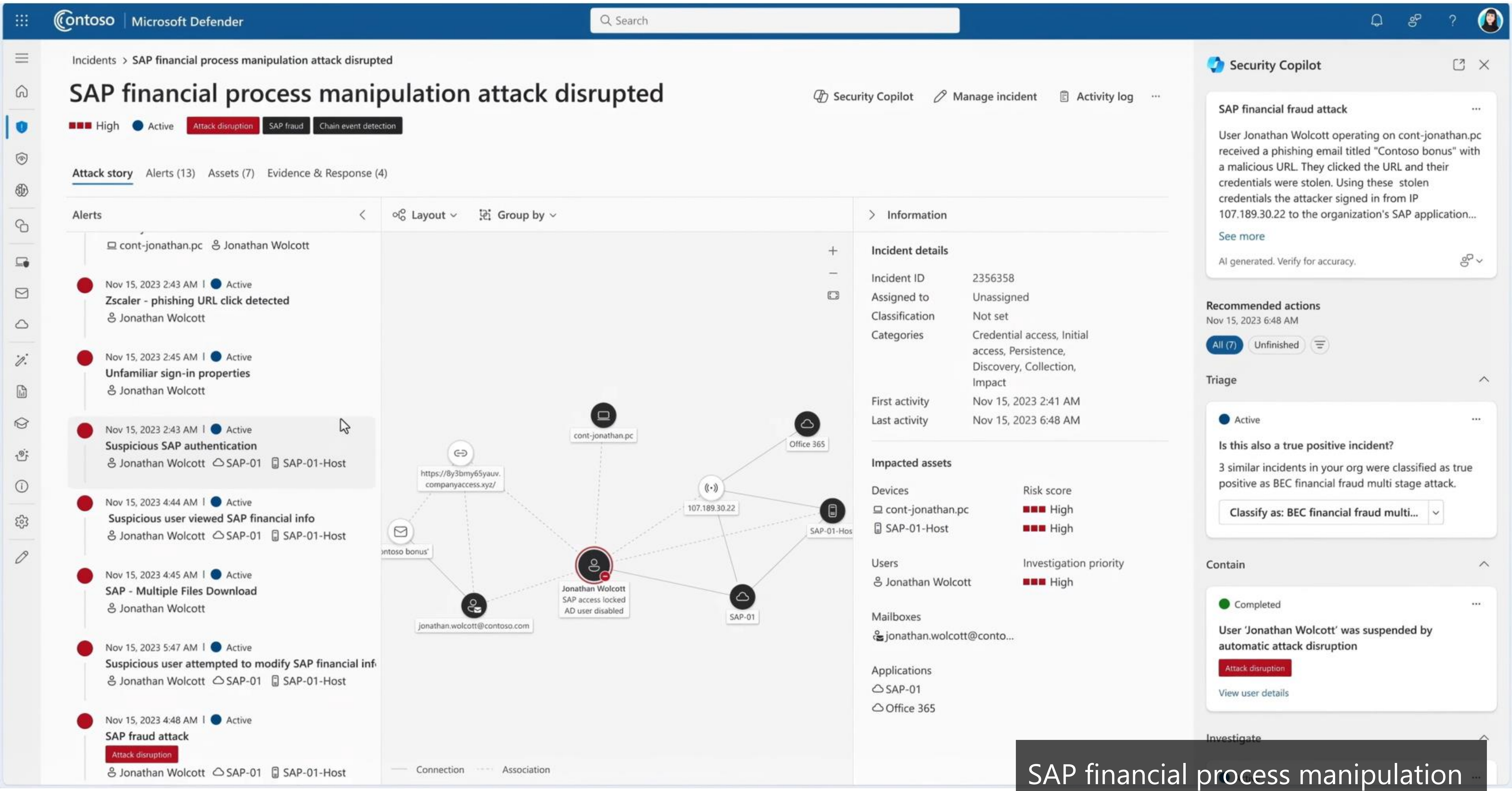
Automatic attack disruption in Microsoft Defender XDR uses XDR signals from different sources (endpoints, email, identity, data) to automatically contain compromised assets and stop ongoing cyber attacks, minimizing their impact on organizations.

## Here are Automated response actions

| Source | Action |
|---|---|
| **Microsoft Defender for Identity** | **- Disable user in Active Directory** |
| Microsoft Defender for Endpoint | - Contain devices from the network<br>- Contain user from the network |

## Here are supported attacks

| Advanced attack | Microsoft Security blog |
|---|---|
| Adversary-in-the-middle attacks (AiTM) | Automatically disrupt adversary-in-the-middle (AiTM) attacks with XDR |
| Business email compromise (BEC) | XDR attack disruption in action – Defending against a recent BEC attack |
| Human-operated ransomware attacks | Automatic disruption of Ransomware and BEC attacks with Microsoft 365 Defender |
| SAP financial process manipulation<br>*(NEW : Private Preview)* | Gaining control of SAP applications security and automatic attack disruption |



# SAP financial process manipulation attack disrupted

High · Active · Attack disruption · SAP fraud · Chain event detection

**Alerts**

cont-jonathan.pc · Jonathan Wolcott

Nov 15, 2023 2:43 AM | Active
**Zscaler - phishing URL click detected**
Jonathan Wolcott

Nov 15, 2023 2:45 AM | Active
**Unfamiliar sign-in properties**
Jonathan Wolcott

Nov 15, 2023 2:43 AM | Active
**Suspicious SAP authentication**
Jonathan Wolcott · SAP-01 · SAP-01-Host

Nov 15, 2023 4:44 AM | Active
**Suspicious user viewed SAP financial info**
Jonathan Wolcott · SAP-01 · SAP-01-Host

Nov 15, 2023 4:45 AM | Active
**SAP - Multiple Files Download**
Jonathan Wolcott

Nov 15, 2023 5:47 AM | Active
**Suspicious user attempted to modify SAP financial inf**
Jonathan Wolcott · SAP-01 · SAP-01-Host

Nov 15, 2023 4:48 AM | Active
**SAP fraud attack**
Attack disruption
Jonathan Wolcott · SAP-01 · SAP-01-Host

**Incident details**

| | |
|---|---|
| Incident ID | 2356358 |
| Assigned to | Unassigned |
| Classification | Not set |
| Categories | Credential access, Initial access, Persistence, Discovery, Collection, Impact |
| First activity | Nov 15, 2023 2:41 AM |
| Last activity | Nov 15, 2023 6:48 AM |

**Impacted assets**

| Devices | Risk score |
|---|---|
| cont-jonathan.pc | High |
| SAP-01-Host | High |

| Users | Investigation priority |
|---|---|
| Jonathan Wolcott | High |

Mailboxes
jonathan.wolcott@conto...

Applications
SAP-01
Office 365

**Security Copilot**

**SAP financial fraud attack**

User Jonathan Wolcott operating on cont-jonathan.pc received a phishing email titled "Contoso bonus" with a malicious URL. They clicked the URL and their credentials were stolen. Using these stolen credentials the attacker signed in from IP 107.189.30.22 to the organization's SAP application...

See more

AI generated. Verify for accuracy.

**Recommended actions**
Nov 15, 2023 6:48 AM
All (7) · Unfinished

Triage

Active
Is this also a true positive incident?
3 similar incidents in your org were classified as true positive as BEC financial fraud multi stage attack.
Classify as: BEC financial fraud multi...

Contain

Completed
User 'Jonathan Wolcott' was suspended by automatic attack disruption
Attack disruption
View user details

Investigate

## SAP financial process manipulation

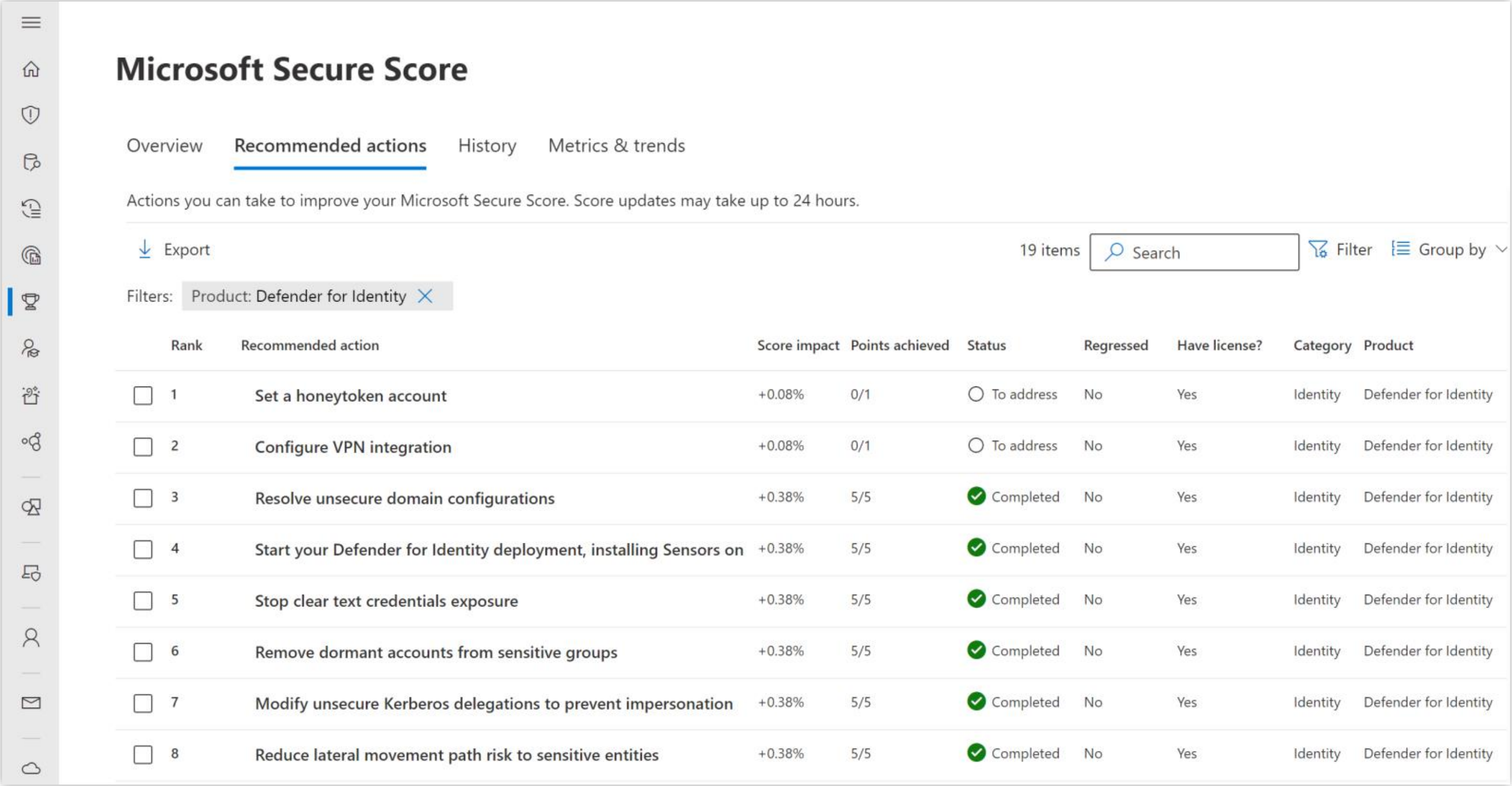
*(NEW : Private Preview)*

Microsoft Defender XDR, Security Copilot & Microsoft Sentinel now in one portal
https://youtu.be/snV2joMnSlc?si=x4bXpKpORj450FTA

# Proactively identify misconfigurations

Microsoft Defender for Endpoint helps identify only endpoint-based vulnerable configuration.

For on-premise, Microsoft Defender for Identity helps discover vulnerable configuration across *ADDC, ADCS and ADFS.*



## Microsoft Secure Score

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Filters: Product: Defender for Identity

| | Rank | Recommended action | Score impact | Points achieved | Status | Regressed | Have license? | Category | Product |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Set a honeytoken account | +0.08% | 0/1 | ○ To address | No | Yes | Identity | Defender for Identity |
| □ | 2 | Configure VPN integration | +0.08% | 0/1 | ○ To address | No | Yes | Identity | Defender for Identity |
| □ | 3 | Resolve unsecure domain configurations | +0.38% | 5/5 | ✓ Completed | No | Yes | Identity | Defender for Identity |
| □ | 4 | Start your Defender for Identity deployment, installing Sensors on | +0.38% | 5/5 | ✓ Completed | No | Yes | Identity | Defender for Identity |
| □ | 5 | Stop clear text credentials exposure | +0.38% | 5/5 | ✓ Completed | No | Yes | Identity | Defender for Identity |
| □ | 6 | Remove dormant accounts from sensitive groups | +0.38% | 5/5 | ✓ Completed | No | Yes | Identity | Defender for Identity |
| □ | 7 | Modify unsecure Kerberos delegations to prevent impersonation | +0.38% | 5/5 | ✓ Completed | No | Yes | Identity | Defender for Identity |
| □ | 8 | Reduce lateral movement path risk to sensitive entities | +0.38% | 5/5 | ✓ Completed | No | Yes | Identity | Defender for Identity |

[Microsoft Defender XDR portal -> Secure Score -> Microsoft Defender for Identity]

https://learn.microsoft.com/en-us/defender-for-identity/security-assessment