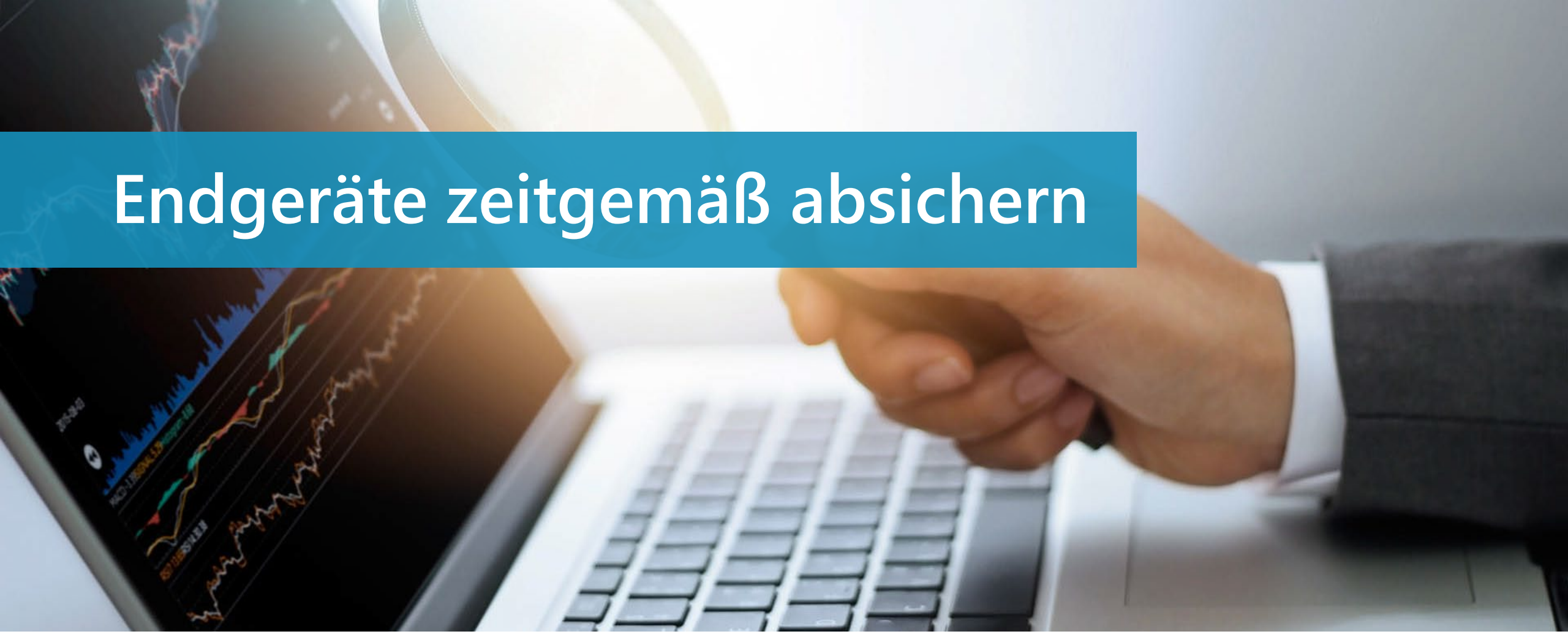
Endgeräte zeitgemäß absichern



Benjamin Strohmaier
benjamin.strohmaier@itelio.com

Raphael Baud
raphael.baud@itelio.com

Agenda

Aktuelle Bedrohungen

Warum Geräteschutz nicht ausreicht

Schutz der Endgeräte

Defender for Endpoint

Schutz der Kommunikation

Defender for Office 365

Schutz der Anwendungen

Defender for Cloud Apps

Schutz der Domäne

Defender for Identity

Zusammenfassung

Microsoft 365 Defender als Ganzes

Aktuelle Bedrohungen

Moderne Angriffsmuster

Eröffnung neuer Angriffsvektoren durch Cloud-Technologie

„Burg-Modell“ keine ausreichende Sicherheitsmaßnahme

Ausgeklügelte Angriffe über lange Zeit

Nutzung aller verfügbaren Einstiegs- und Angriffspunkte

Resultierende Folgen

Erhöhte Anzahl abzusichernder Stellen

Steigender Aufwand für IT-Sicherheit

Überblick kann nicht bewahrt werden

Geräteschutz nicht mehr ausreichend

Schutz der Endgeräte

Microsoft Defender for Endpoint

Endpunkt-Sicherheitsplattform

Erweiterung des klassischen Antivirus um moderne Sicherheitsmechanismen

Unterstützt gängige Client-, Server- und Smartphone-Betriebssysteme

Next-Generation Protection

Mehr als der „klassische“ Windows Defender

Intelligente Antivirus-Funktionalität

Cloudbasierter Schutz vor neuen Gefahren

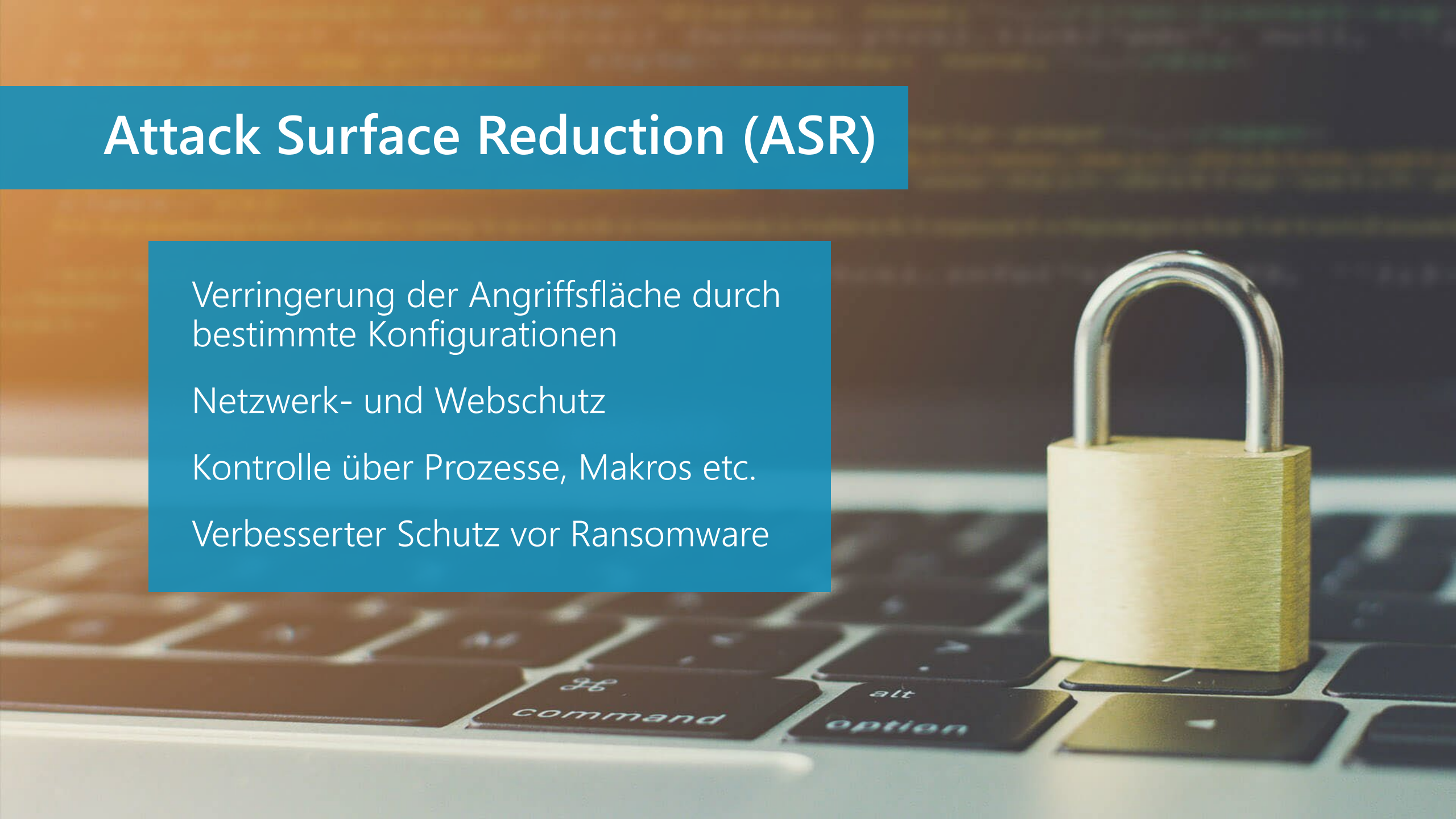
Attack Surface Reduction (ASR)

Verringerung der Angriffsfläche durch bestimmte Konfigurationen

Netzwerk- und Webschutz

Kontrolle über Prozesse, Makros etc.

Verbesserter Schutz vor Ransomware



Automated Investigation and Remediation

Erkennung verdächtiger Aktivitäten auf Endpunkten

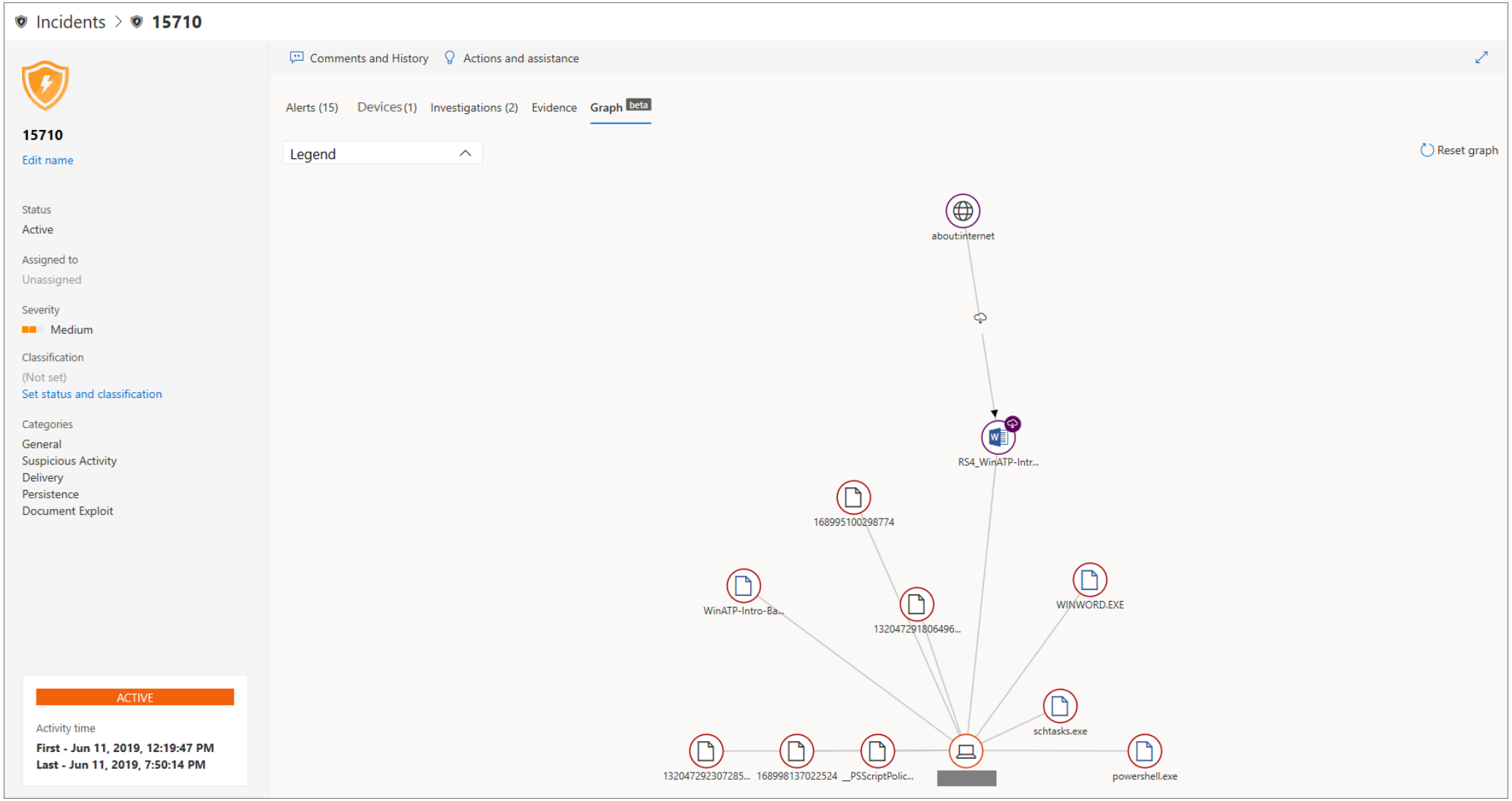
Ermittlung des Bedrohungsgrades

Automatisierungsgrad bestimmt Aktion

Endpoint Detection and Response (EDR)

- Bündelung zusammenhängender Alerts als Incidents
- Kombination sämtlicher MDE-Features
- Nachverfolgung von Angriffen durch grafische Aufarbeitung
- Advanced Hunting für tiefe Analyse

Incidents


Incidents > 15710
Comments and History
Actions and assistance
Alerts (15)
Devices (1)
Investigations (2)
Evidence
Graph beta
Legend
Reset graph
15710
Edit name
Status
Active
Assigned to
Unassigned
Severity
Medium
Classification
(Not set)
Set status and classification
Categories
General
Suspicious Activity
Delivery
Persistence
Document Exploit
ACTIVE
Activity time
First - Jun 11, 2019, 12:19:47 PM
Last - Jun 11, 2019, 7:50:14 PM
about:internet
RS4_WinATP-Intr...
168995100298774
WinATP-Intro-Ba...
132047291806496...
WINWORD.EXE
schtasks.exe
132047292307285...
168998137022524
__PSScriptPolic...
powershell.exe

Onboarding und Konfiguration

Onboarding:

- Intune (Clients und Smartphones)
- GPO/Skript (Clients und Server)
- Azure (Server)

Konfiguration:

- Intune (Clients, Smartphones und Server)
- GPO (Clients und Server)

Schutz der Kommunikation

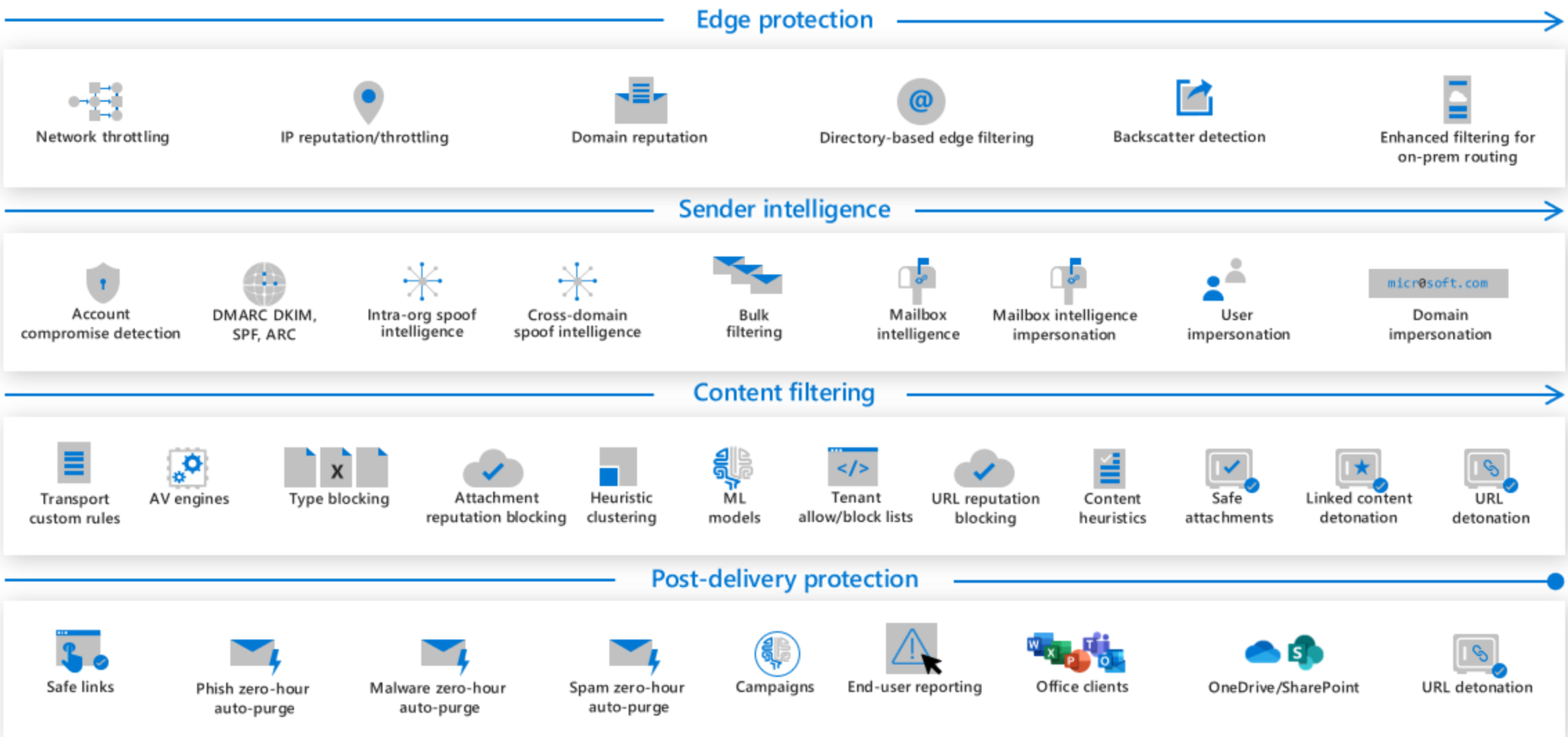
Microsoft Defender for Office 365

Überwachung von Kommunikations- und Kollaborationskanälen (EXO, SPO, Teams)

Schutz vor z.B. Phishing-Mails, Malware und bösartigen Anhängen

Erkennung von Angriffen, Datenlecks und Compliance-Verstößen

Microsoft Defender for Office 365 protection stack



Schutz der Anwendungen

Microsoft Defender for Cloud Apps

- Cloud Access Security Broker (CASB)
- Cloud Discovery zur Erkennung von Schatten-IT
- Anbindung an 3rd-Party-Cloud-Anwendungen
- Echtzeit-Kontrolle über App-Sitzungen

Cloud Discovery

- Auswertung von Netzwerklogs (Defender for Endpoint oder Anbindung der internen Firewall)
- Erkennung genutzter Cloud-Dienste
- Bewertung in vorgefertigtem App-Katalog
- Blockierung ungewünschter Cloud Apps (Defender for Endpoint)

Anbindung weiterer Anwendungen

Verbindung über APIs unterstützter Cloud Apps

Auswertung von Aktivitätslogs, Konten und Inhalten

Erweiterung der Bedrohungserkennung auf diese Apps

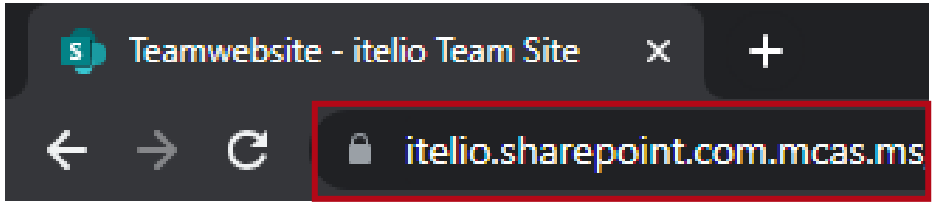
Conditional Access App Control

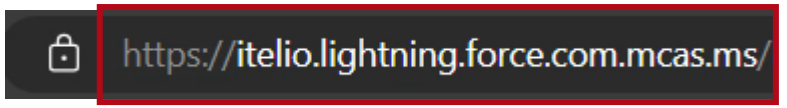
Reverse Proxy für Cloud-Anwendungen

Sitzungen zu konfigurierten Apps werden getunnelt

Steuerung der Zugriffe und Datenflüsse

Conditional Access App Control





Der Zugriff auf Microsoft SharePoint Online wird geschützt

Zur Verbesserung der Sicherheit wird dein Zugriff auf Microsoft SharePoint Online geschützt.

Bei Fragen oder Problemen wende dich bitte an support@itelio.com

☐ Diese Benachrichtigung für alle Apps eine Woche lang nicht anzeigen

Weiter zu Microsoft SharePoint Online

Schutz der Domäne

Microsoft Defender for Identity

Überwachung des lokalen Active Directory

Verhaltensanalysen und Bedrohungserkennung

Integration mit Azure Active Directory

Bedrohungserkennung

Überwachung von Benutzeraktivitäten und -authentifizierungen

Erkennung von Anomalien und ungewöhnlichem Verhalten

Identifizierung potenziell kompromittierter Konten und Insider-Bedrohungen

Funktionsweise

Installation von Sensoren auf Domänencontrollern

Auswertung von Event Logs

Lernzeit für das System

Angriffssimulation zur Validierung

Zusammenfassung

Microsoft 365 Defender

Zusammenführung der Sicherheitslösungen

Verwaltung über zentrale Oberfläche

Ganzheitliche Betrachtung von Incidents

Microsoft | Microsoft 365 Defender | Search

Incidents > MDI Demo Incident - 05/26/2022 - Multi-stage incident involving Privilege escalation on multiple endpoints reported by multiple sources

Manage incident | Consult a threat expert | Comments and history

Summary | Alerts (87) | Devices (20) | Users (20) | Mailboxes (3) | Investigations (14) | Evidence (247)

62/87 active alerts

11 MITRE ATT&CK tactics

1 other alert categories

May 24, 2022, 8:25:29 PM | **New**

Suspicious attachment opened on alexw-pc by user alexwilber

20 impacted devices

20 impacted users

3 impacted mailboxes

Top impacted entities

Entity type	Risk level/investigation priority	Tags
annetteh-pc	High	Demo Machine, Possible Insi
mtp-air-dc01	High	Data sensitivity: High, Domai
janetl-pc	High	Data sensitivity: High, Demo
mdatpglobalreader	1016	Office 365 administrator
pekrebs	701	Quad Copter Enthusiasts
bamorel	90	All Employees, Mark 8 Projec

Incident Information

This incident might be associated with more in...

Associated incidents

Incident ID	Reason	Entity
9437	Same user cr...	mdatpglobal...
9437	Same user cr...	mdatpglobal...

Tags summary

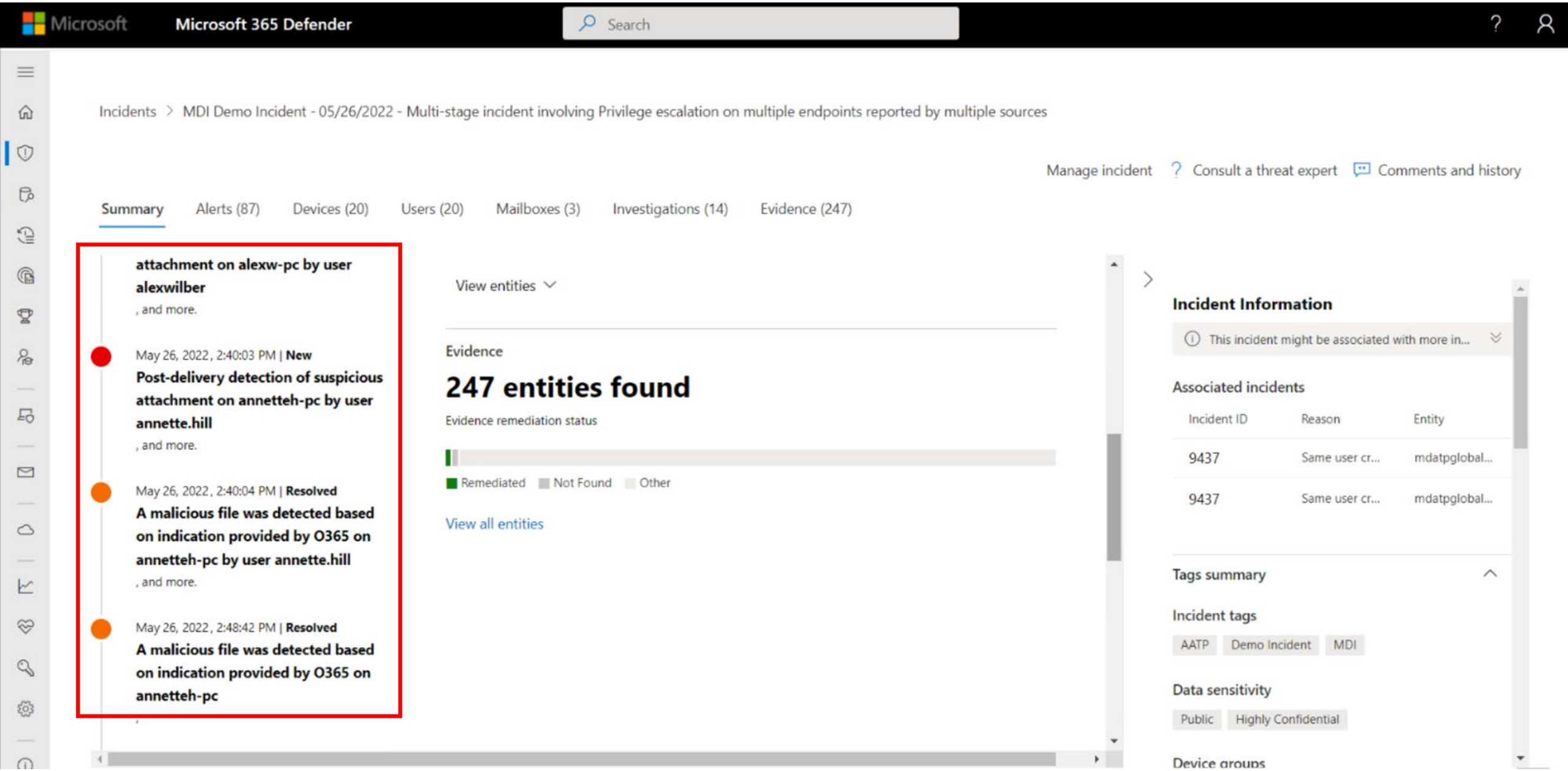
Incident tags

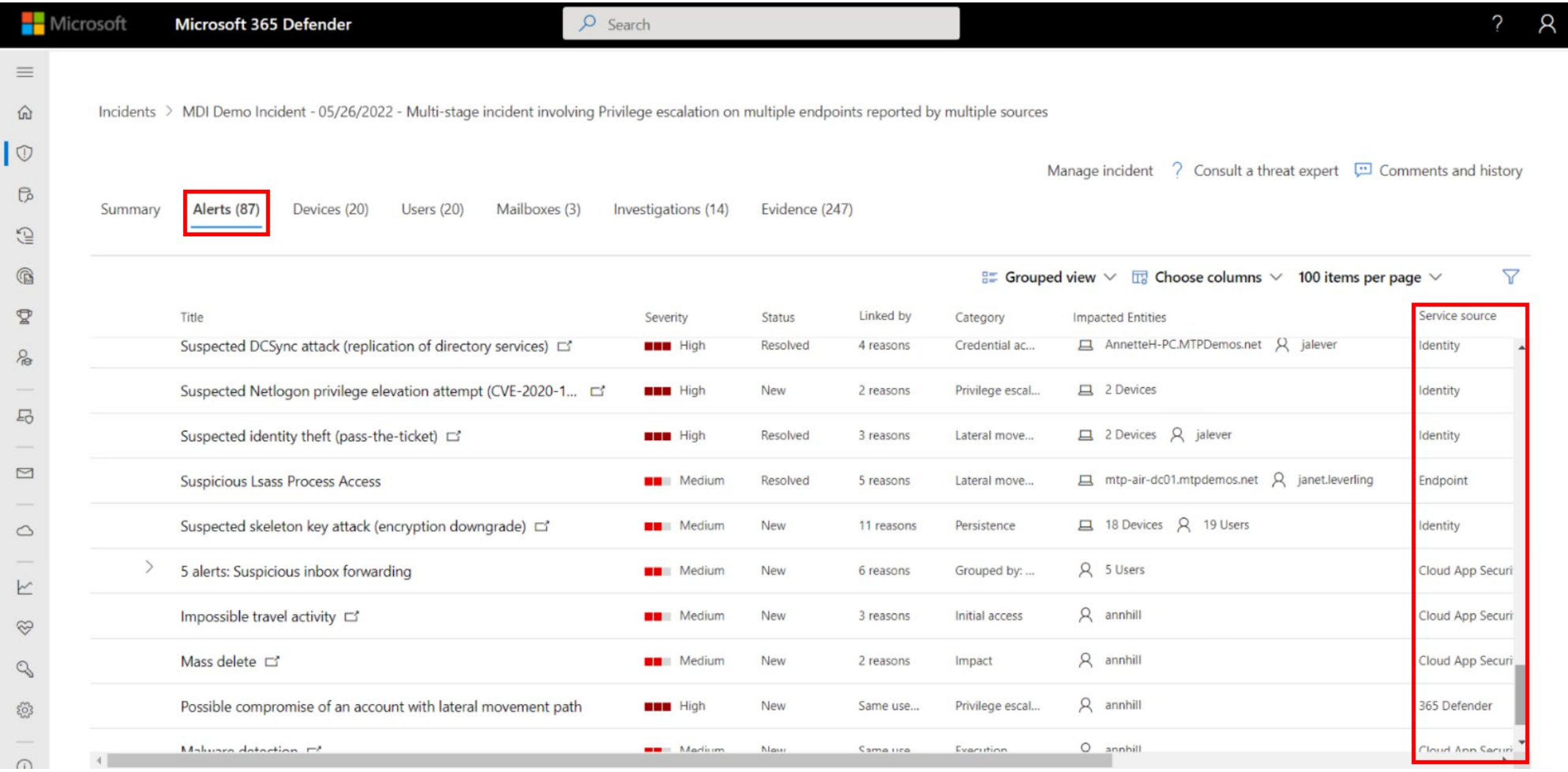
AATP | Demo Incident | MDI

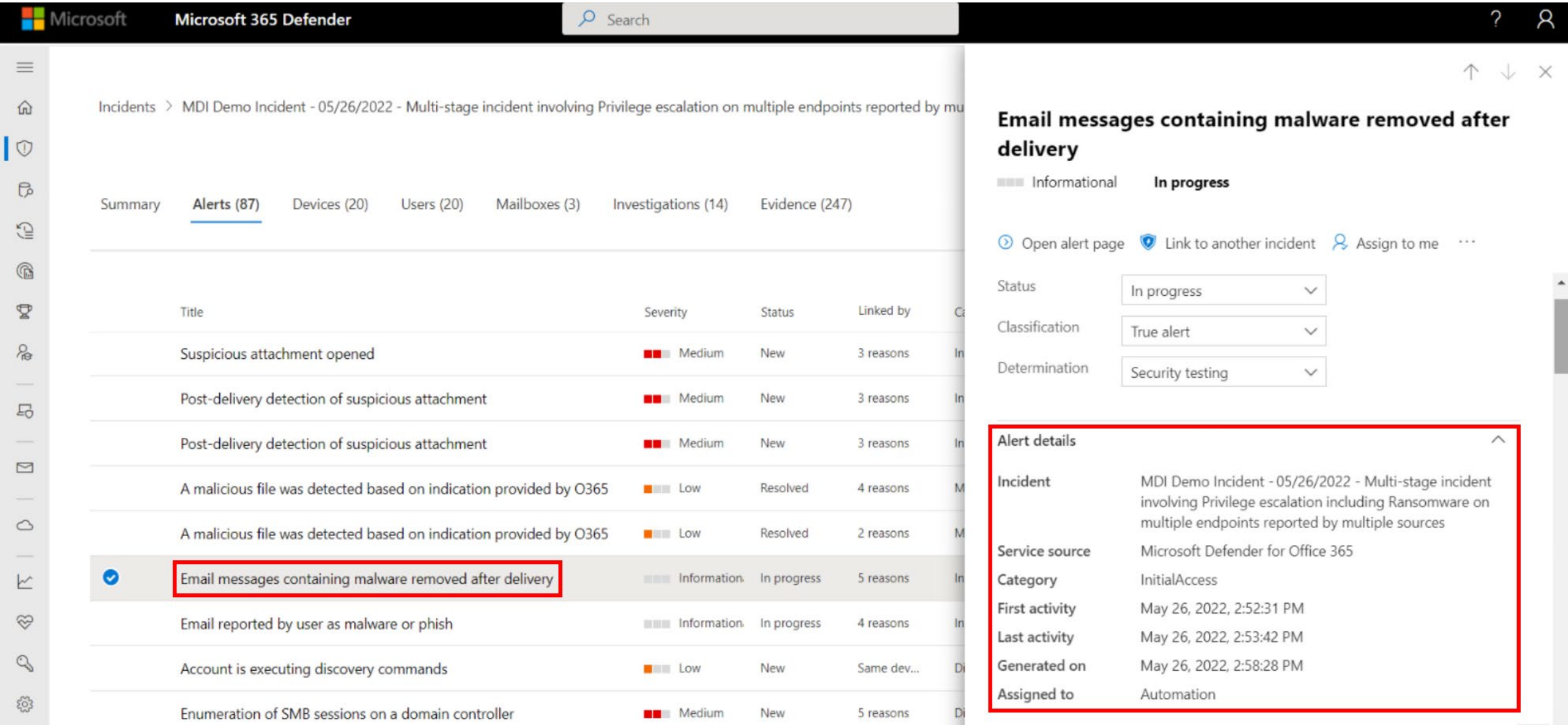
Data sensitivity

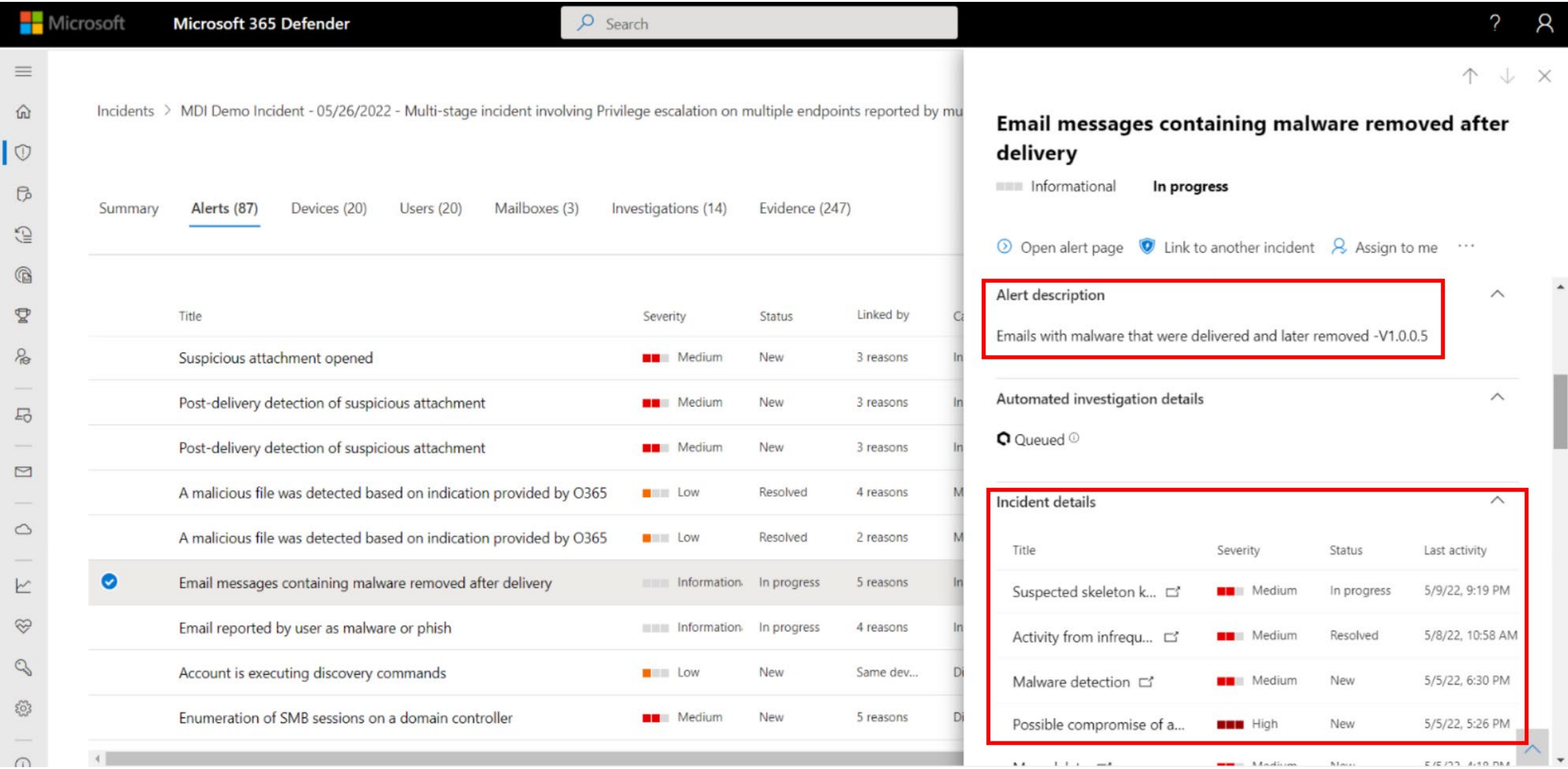
Public | Highly Confidential

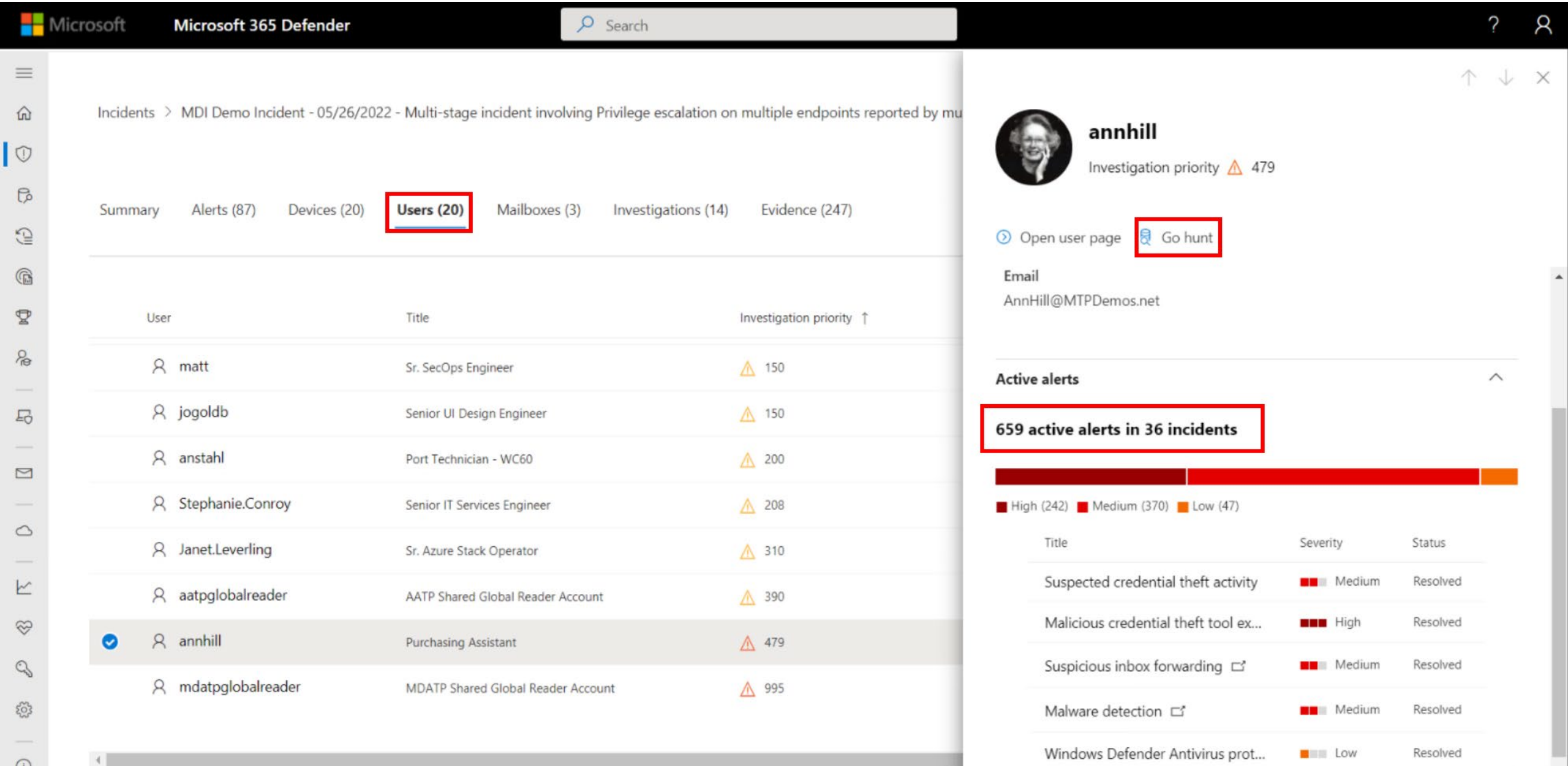
Device groups

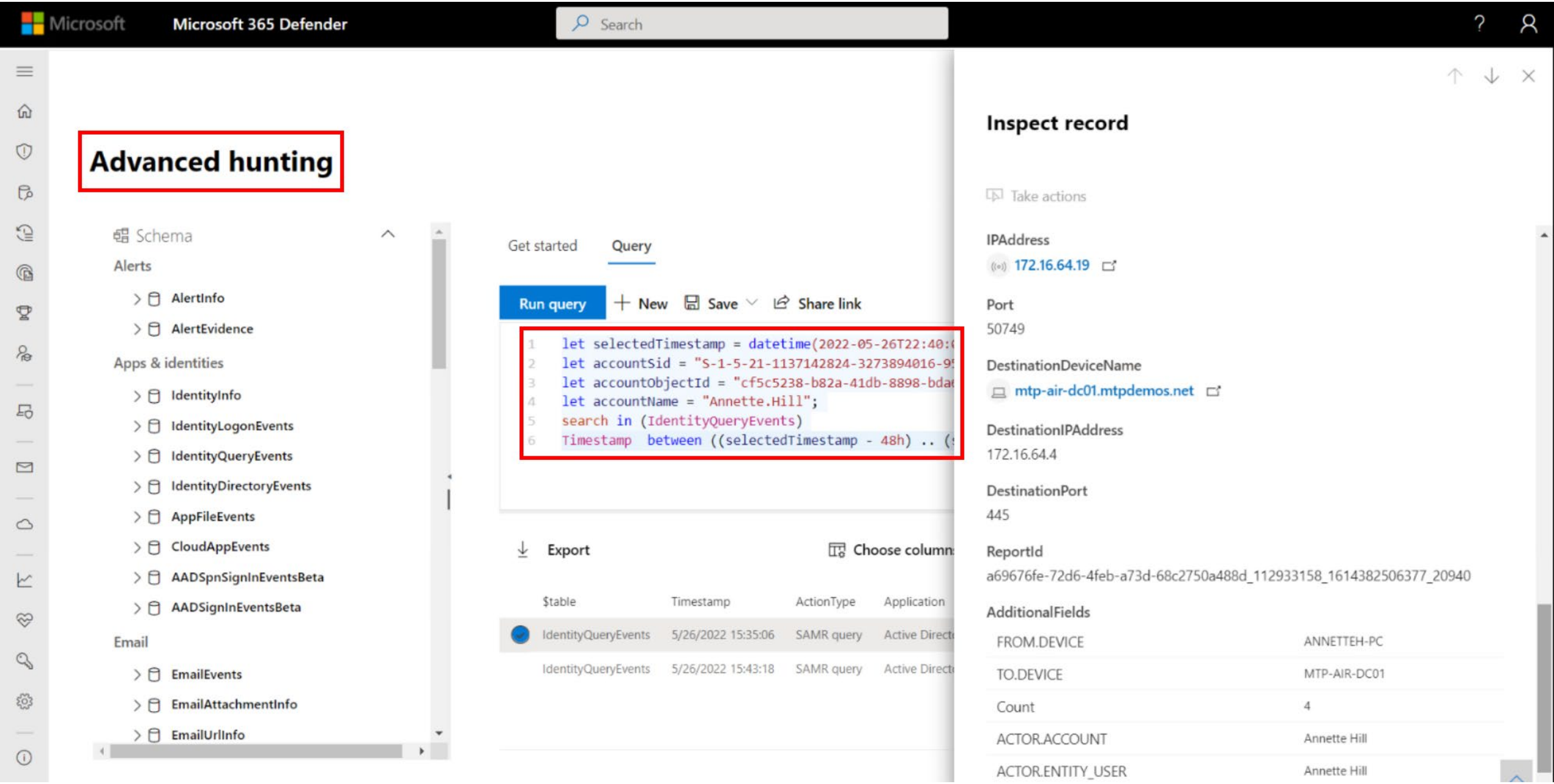

Microsoft
Microsoft 365 Defender
Search
Incidents > MDI Demo Incident - 05/26/2022 - Multi-stage incident involving Privilege escalation on multiple endpoints reported by multiple sources
Manage incident
Consult a threat expert
Comments and history
Summary
Alerts (87)
Devices (20)
Users (20)
Mailboxes (3)
Investigations (14)
Evidence (247)
attachment on alexw-pc by user alexwilber
, and more.
May 26, 2022, 2:40:03 PM | New
Post-delivery detection of suspicious attachment on annetteh-pc by user annette.hill
, and more.
May 26, 2022, 2:40:04 PM | Resolved
A malicious file was detected based on indication provided by O365 on annetteh-pc by user annette.hill
, and more.
May 26, 2022, 2:48:42 PM | Resolved
A malicious file was detected based on indication provided by O365 on annetteh-pc
View entities
Evidence
247 entities found
Evidence remediation status
Remediated
Not Found
Other
View all entities
Incident Information
This incident might be associated with more in...
Associated incidents
Incident ID
Reason
Entity
9437
Same user cr...
mdatpglobal...
9437
Same user cr...
mdatpglobal...
Tags summary
Incident tags
AATP
Demo Incident
MDI
Data sensitivity
Public
Highly Confidential
Device groups


Microsoft
Microsoft 365 Defender
Search
Incidents > MDI Demo Incident - 05/26/2022 - Multi-stage incident involving Privilege escalation on multiple endpoints reported by multiple sources
Manage incident
Consult a threat expert
Comments and history
Summary
Alerts (87)
Devices (20)
Users (20)
Mailboxes (3)
Investigations (14)
Evidence (247)
Grouped view
Choose columns
100 items per page
Title
Severity
Status
Linked by
Category
Impacted Entities
Service source
Suspected DCSync attack (replication of directory services) High Resolved 4 reasons Credential ac... AnnetteH-PC.MTPDemos.net jalever Identity
Suspected Netlogon privilege elevation attempt (CVE-2020-1... High New 2 reasons Privilege escal... 2 Devices Identity
Suspected identity theft (pass-the-ticket) High Resolved 3 reasons Lateral move... 2 Devices jalever Identity
Suspicious Lsass Process Access Medium Resolved 5 reasons Lateral move... mtp-air-dc01.mtpdemos.net janet.leverling Endpoint
Suspected skeleton key attack (encryption downgrade) Medium New 11 reasons Persistence 18 Devices 19 Users Identity
5 alerts: Suspicious inbox forwarding Medium New 6 reasons Grouped by: ... 5 Users Cloud App Securi
Impossible travel activity Medium New 3 reasons Initial access annhill Cloud App Securi
Mass delete Medium New 2 reasons Impact annhill Cloud App Securi
Possible compromise of an account with lateral movement path High New Same use... Privilege escal... annhill 365 Defender


Microsoft
Microsoft 365 Defender
Search
Incidents > MDI Demo Incident - 05/26/2022 - Multi-stage incident involving Privilege escalation on multiple endpoints reported by mu
Summary
Alerts (87)
Devices (20)
Users (20)
Mailboxes (3)
Investigations (14)
Evidence (247)
Title
Severity
Status
Linked by
Suspicious attachment opened
Medium
New
3 reasons
Post-delivery detection of suspicious attachment
Medium
New
3 reasons
Post-delivery detection of suspicious attachment
Medium
New
3 reasons
A malicious file was detected based on indication provided by O365
Low
Resolved
4 reasons
A malicious file was detected based on indication provided by O365
Low
Resolved
2 reasons
Email messages containing malware removed after delivery
Information
In progress
5 reasons
Email reported by user as malware or phish
Information
In progress
4 reasons
Account is executing discovery commands
Low
New
Same dev...
Enumeration of SMB sessions on a domain controller
Medium
New
5 reasons
Email messages containing malware removed after delivery
Informational
In progress
Open alert page
Link to another incident
Assign to me
Status
In progress
Classification
True alert
Determination
Security testing
Alert details
Incident
MDI Demo Incident - 05/26/2022 - Multi-stage incident involving Privilege escalation including Ransomware on multiple endpoints reported by multiple sources
Service source
Microsoft Defender for Office 365
Category
InitialAccess
First activity
May 26, 2022, 2:52:31 PM
Last activity
May 26, 2022, 2:53:42 PM
Generated on
May 26, 2022, 2:58:28 PM
Assigned to
Automation


Microsoft
Microsoft 365 Defender
Search
Incidents > MDI Demo Incident - 05/26/2022 - Multi-stage incident involving Privilege escalation on multiple endpoints reported by mu
Summary
Alerts (87)
Devices (20)
Users (20)
Mailboxes (3)
Investigations (14)
Evidence (247)
Title
Severity
Status
Linked by
Suspicious attachment opened
Medium
New
3 reasons
Post-delivery detection of suspicious attachment
Medium
New
3 reasons
Post-delivery detection of suspicious attachment
Medium
New
3 reasons
A malicious file was detected based on indication provided by O365
Low
Resolved
4 reasons
A malicious file was detected based on indication provided by O365
Low
Resolved
2 reasons
Email messages containing malware removed after delivery
Information
In progress
5 reasons
Email reported by user as malware or phish
Information
In progress
4 reasons
Account is executing discovery commands
Low
New
Same dev...
Enumeration of SMB sessions on a domain controller
Medium
New
5 reasons
Email messages containing malware removed after delivery
Informational
In progress
Open alert page
Link to another incident
Assign to me
Alert description
Emails with malware that were delivered and later removed -V1.0.0.5
Automated investigation details
Queued
Incident details
Title
Severity
Status
Last activity
Suspected skeleton k...
Medium
In progress
5/9/22, 9:19 PM
Activity from infrequ...
Medium
Resolved
5/8/22, 10:58 AM
Malware detection
Medium
New
5/5/22, 6:30 PM
Possible compromise of a...
High
New
5/5/22, 5:26 PM


Microsoft
Microsoft 365 Defender
Search
Incidents > MDI Demo Incident - 05/26/2022 - Multi-stage incident involving Privilege escalation on multiple endpoints reported by mu
Summary
Alerts (87)
Devices (20)
Users (20)
Mailboxes (3)
Investigations (14)
Evidence (247)
User
Title
Investigation priority
matt
Sr. SecOps Engineer
150
jogoldb
Senior UI Design Engineer
150
anstahl
Port Technician - WC60
200
Stephanie.Conroy
Senior IT Services Engineer
208
Janet.Leverling
Sr. Azure Stack Operator
310
aatpglobalreader
AATP Shared Global Reader Account
390
annhill
Purchasing Assistant
479
mdatpglobalreader
MDATP Shared Global Reader Account
995
annhill
Investigation priority 479
Open user page
Go hunt
Email
AnnHill@MTPDemos.net
Active alerts
659 active alerts in 36 incidents
High (242)
Medium (370)
Low (47)
Title
Severity
Status
Suspected credential theft activity
Medium
Resolved
Malicious credential theft tool ex...
High
Resolved
Suspicious inbox forwarding
Medium
Resolved
Malware detection
Medium
Resolved
Windows Defender Antivirus prot...
Low
Resolved


Microsoft
Microsoft 365 Defender
Search
Advanced hunting
Schema
Alerts
AlertInfo
AlertEvidence
Apps & identities
IdentityInfo
IdentityLogonEvents
IdentityQueryEvents
IdentityDirectoryEvents
AppFileEvents
CloudAppEvents
AADSpnSignInEventsBeta
AADSignInEventsBeta
Email
EmailEvents
EmailAttachmentInfo
EmailUrlInfo
Get started
Query
Run query
New
Save
Share link
let selectedTimestamp = datetime(2022-05-26T22:40:
let accountSid = "S-1-5-21-1137142824-3273894016-9
let accountObjectId = "cf5c5238-b82a-41db-8898-bda
let accountName = "Annette.Hill";
search in (IdentityQueryEvents)
Timestamp between ((selectedTimestamp - 48h) ..
Export
Choose column
$table
Timestamp
ActionType
Application
IdentityQueryEvents
5/26/2022 15:35:06
SAMR query
IdentityQueryEvents
5/26/2022 15:43:18
SAMR query
Inspect record
Take actions
IPAddress
172.16.64.19
Port
50749
DestinationDeviceName
mtp-air-dc01.mtpdemos.net
DestinationIPAddress
172.16.64.4
DestinationPort
445
ReportId
a69676fe-72d6-4feb-a73d-68c2750a488d_112933158_1614382506377_20940
AdditionalFields
FROM.DEVICE
ANNETTEH-PC
TO.DEVICE
MTP-AIR-DC01
Count
4
ACTOR.ACCOUNT
Annette Hill
ACTOR.ENTITY_USER
Annette Hill

Microsoft | Microsoft 365 Defender | Search

Annette Hill
Purchasing Assistant
Purchasing

DOMAIN ADMIN

User threat

Open incidents	Investigation prio...
3	479
Active alerts	**Identity risk level**
40	High
Sensitive users at risk	
2	

User exposure

First seen	Last seen
Sep 7, 2021	Jun 2, 2022
Accounts	**Devices**
3	22
Logon Types	**Locations**
3	7
Matched files	
15	

Investigation priority score

Score is based on the last 7 days How do we score?

479

- Alerts Score: 470
- Risky activities Score: 9

User's score compared to the organization 91%

User score in the last two weeks

Top 90% in your organization

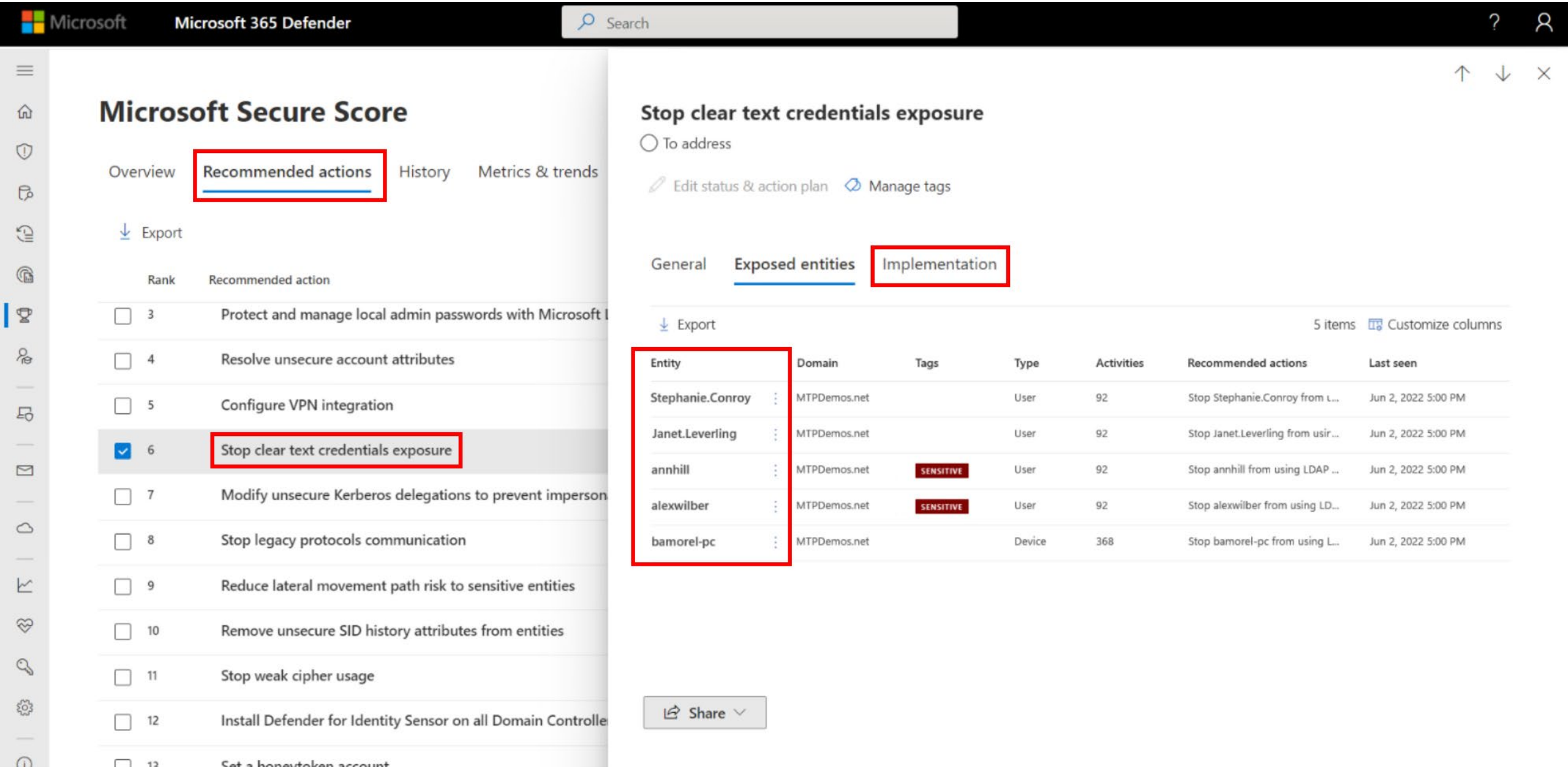
Alerts and risky activities that contributed to the score (last 7 days) View all user alerts (40)

Today

+30 6/2/22, 11:17:09 AM
Suspected skeleton key attack (encryption downgrade)

+50 6/2/22, 5:08:03 AM
Logon from a risky IP address

+50 6/2/22, 1:51:28 AM
Logon from a risky IP address


Microsoft
Microsoft 365 Defender
Search
Microsoft Secure Score
Overview
Recommended actions
History
Metrics & trends
Export
Rank
Recommended action
3 Protect and manage local admin passwords with Microsoft
4 Resolve unsecure account attributes
5 Configure VPN integration
6 Stop clear text credentials exposure
7 Modify unsecure Kerberos delegations to prevent imperson
8 Stop legacy protocols communication
9 Reduce lateral movement path risk to sensitive entities
10 Remove unsecure SID history attributes from entities
11 Stop weak cipher usage
12 Install Defender for Identity Sensor on all Domain Controlle
Stop clear text credentials exposure
To address
Edit status & action plan
Manage tags
General
Exposed entities
Implementation
Export
5 items
Customize columns
Entity
Domain
Tags
Type
Activities
Recommended actions
Last seen
Stephanie.Conroy
MTPDemos.net
User
92
Stop Stephanie.Conroy from ...
Jun 2, 2022 5:00 PM
Janet.Leverling
MTPDemos.net
User
92
Stop Janet.Leverling from usir...
Jun 2, 2022 5:00 PM
annhill
MTPDemos.net
SENSITIVE
User
92
Stop annhill from using LDAP ...
Jun 2, 2022 5:00 PM
alexwilber
MTPDemos.net
SENSITIVE
User
92
Stop alexwilber from using LD...
Jun 2, 2022 5:00 PM
bamorel-pc
MTPDemos.net
Device
368
Stop bamorel-pc from using L...
Jun 2, 2022 5:00 PM
Share

Noch Fragen?