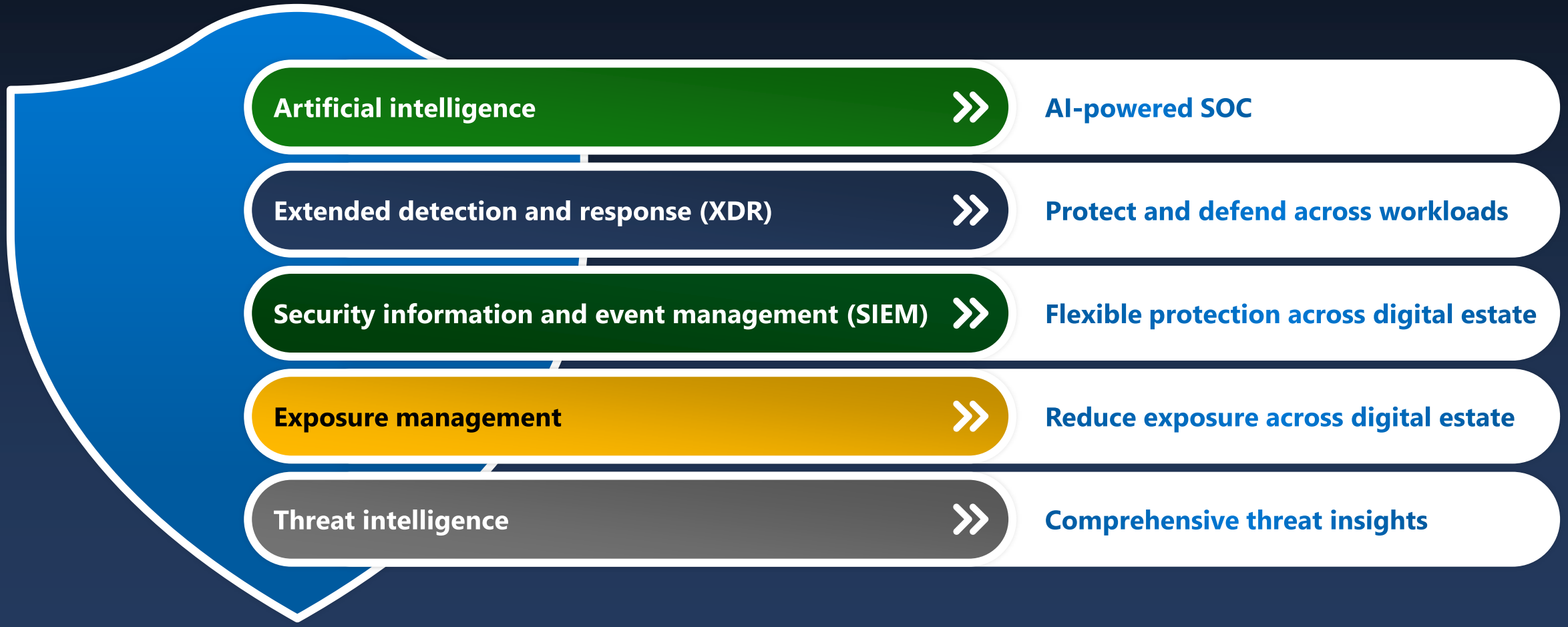
Microsoft Security

# Microsoft's Unified Security Operations Platform

August 2024

Jeff Beckitt
Security Technology Specialist

# Microsoft's unified security operations platform



News Zero Trust Microsoft Entra · 9 min read

# Simplified Zero Trust security with the Microsoft Entra Suite and unified security operations platform, now generally available

By Vasu Jakkal, Corporate Vice President, Security, Compliance, Identity, and Management
Joy Chik, President, Identity & Network Access

July 11, 2024

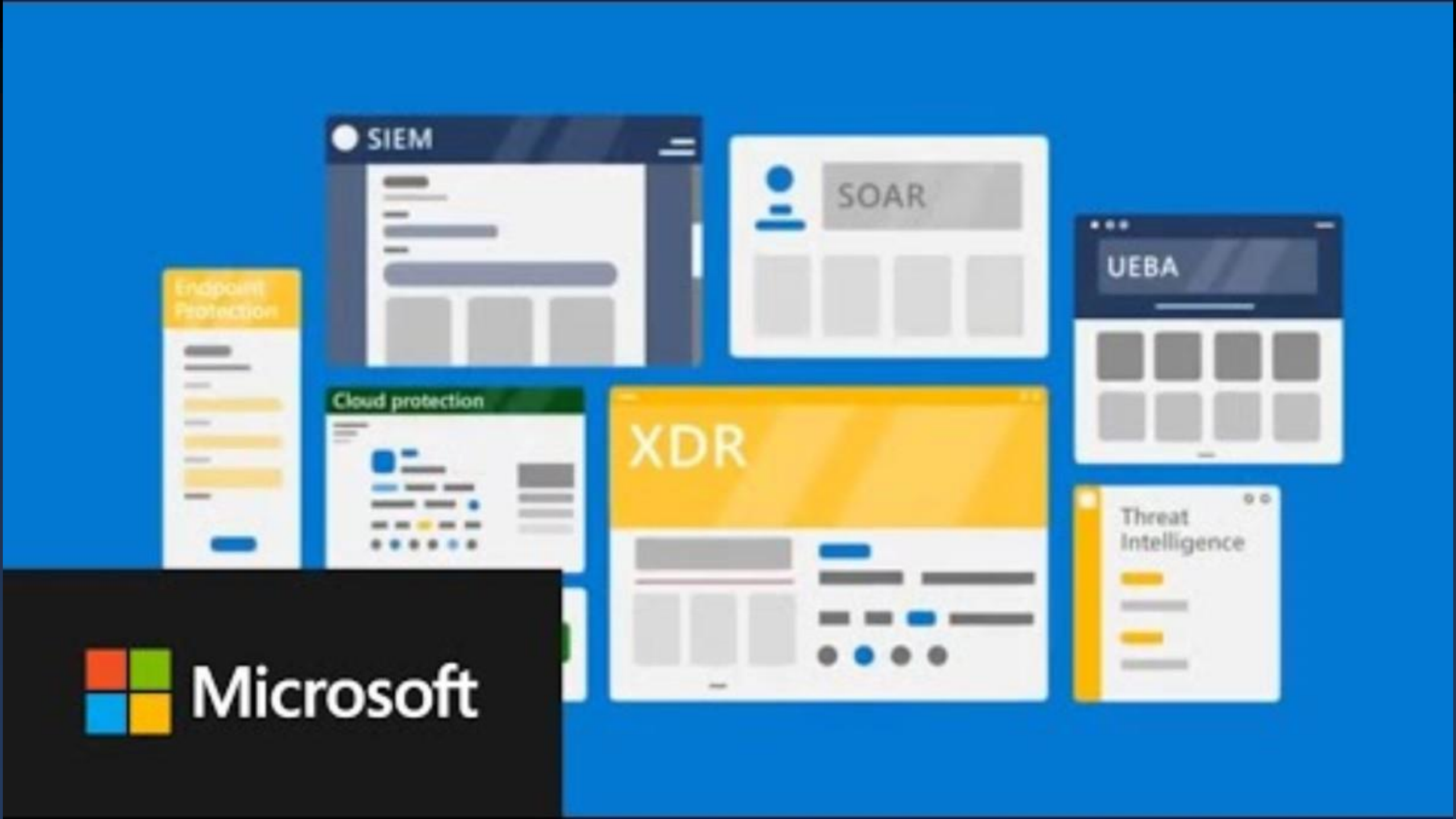
Microsoft Defender

Microsoft Defender XDR

Microsoft Entra ID Governance

more

We're announcing new capabilities to help accelerate your transition to a Zero Trust security model with the general availability of the Microsoft Entra Suite, the industry's most comprehensive secure access solution for the workforce, and the general availability of Microsoft Sentinel within the Microsoft unified security operations platform, which delivers unified threat protection and posture management. These innovations make it easier to secure access, identify and close critical security gaps, detect cyberthreats, reduce response times, and streamline operations.


SIEM
SOAR
UEBA
Endpoint Protection
Cloud protection
XDR
Threat Intelligence
Microsoft

# What is Microsoft's unified security operations platform?

| It is | It's not |
| --- | --- |
| A single experience for SIEM, XDR, XSPM, TI and Copilot for security | A product |
| Unification of features across SIEM and XDR | A new SKU |
| A differentiator that will help attach SIEM to XDR customers | An upsell |

# Pricing Isn’t changing.

## Two SKUs

- Customers purchase SIEM and XDR separately. Defender XDR continues to be licensed based, Microsoft Sentinel continues to be consumption based

## Cost savings

- Customers do not need to ingest Defender XDR data into Microsoft Sentinel for hunting or investigations, potentially resulting in cost savings
- Ingestion still required for extended retention

# What is happening to Microsoft Sentinel?

- The experience is going to be available in the Defender portal
- Customers can continue to access in Azure, even after onboarding
- Customers need to opt in to the single experience
- We continue to invest in innovation to Microsoft Sentinel

# Unified security operations platform in the Defender Portal

## Microsoft Copilot for Security

- Step-by-step, incident-specific remediation guidance
- Incident and event summary reports
- Natural language translation to KQL
- Script analysis
- Knowledge transfer

## Defender Experts

- Managed detection and response
- Incident response support
- Proactive threat hunting

## Analyst experience

- Unified incidents and investigation
- Unified response actions
- Unified advanced hunting
- Attack path modeling
- Attack surface management
- Critical asset protection
- SOC optimization
- Case management
- Global search

## Defense at machine speed

- Automatic attack disruption
- Deception technology
- Automated self-healing

## Security analytics

- Correlation and normalization
- UEBA
- Unified data model
- Customizable automation
- Threat intelligence platform and analytics
- Entity profiles

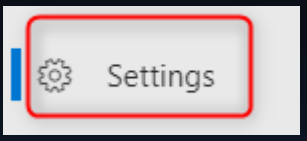
## Data

300+ third-party solutions

CHECK POINT · SAP · ORACLE · CROWDSTRIKE · paloalto NETWORKS

- Business applications
- Microsoft integrations
- Modern workplace
- Industry standards
- Cloud workloads
- Users
- Devices
- Data storage
- Infrastructure

# Connecting the Sentinel workspace (1 of 2)







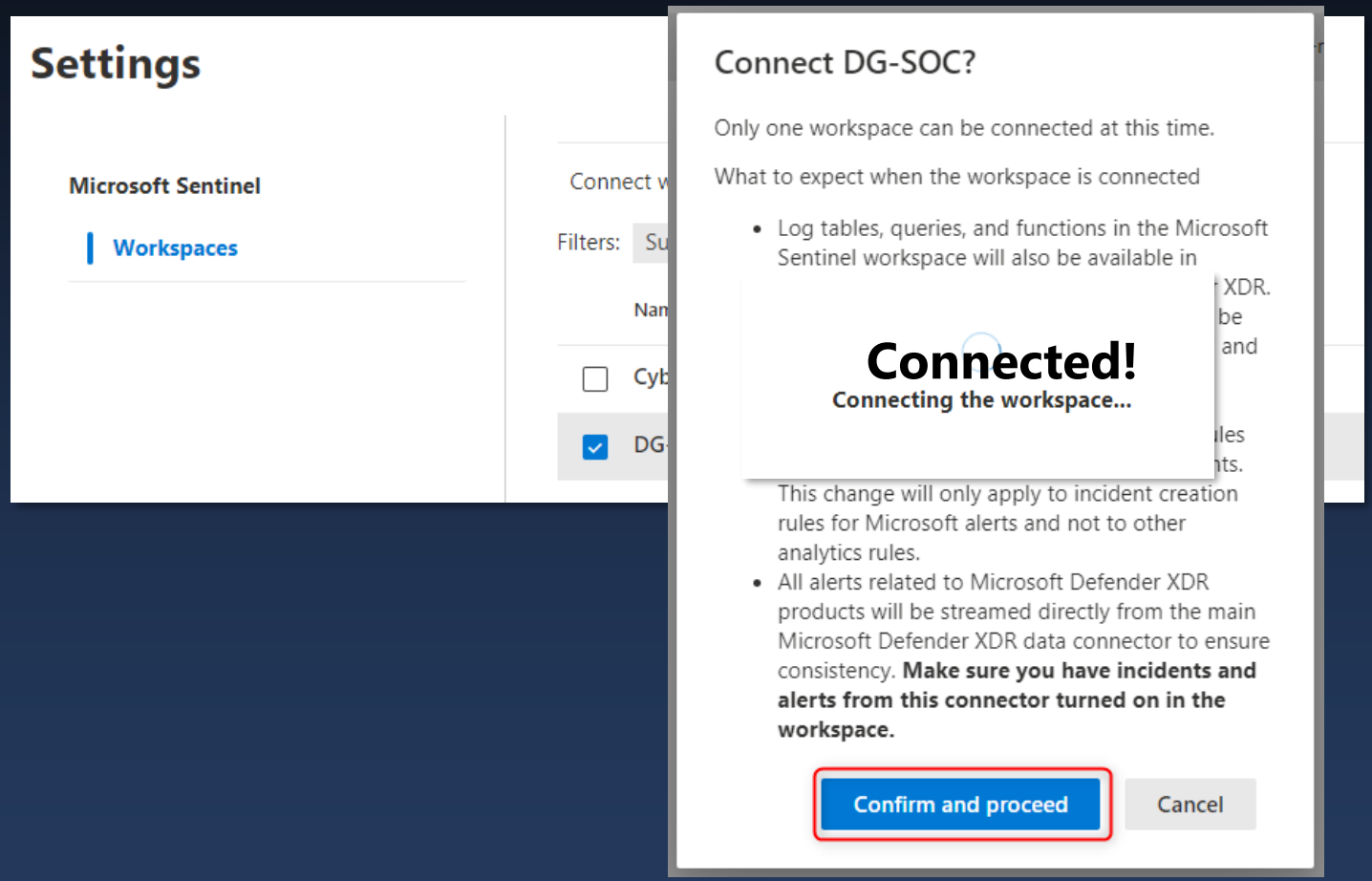
[Required Azure permissions to connect/disconnect:]

Subscription owner *or* User Access Administrator *and* Sentinel Contributor

*Scope*: Subscription, resource group, or workspace resource for Microsoft Sentinel Contributor

# Connecting the Sentinel workspace (2 of 2)

## Prerequisites and permissions are in place



Work | Incidents - Microsoft Defender

https://security.microsoft.com/incidents?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb

Import favorites | Defender | Sentinel | Defender for Cloud | Demo Access

Microsoft Defender

Search

u221

U

- Home
- Exposure management
- Investigation & response
- Incidents & alerts
  - Incidents
  - Alerts
- Hunting
- Actions & submissions
- Partner catalog
- Threat intelligence
- Assets
- Microsoft Sentinel
- Identities
- Endpoints
- Email & collaboration

# Incidents

10 pending file quarantine actions need approval

Snooze for 1 hour

The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, see inci

## Most recent incidents and alerts

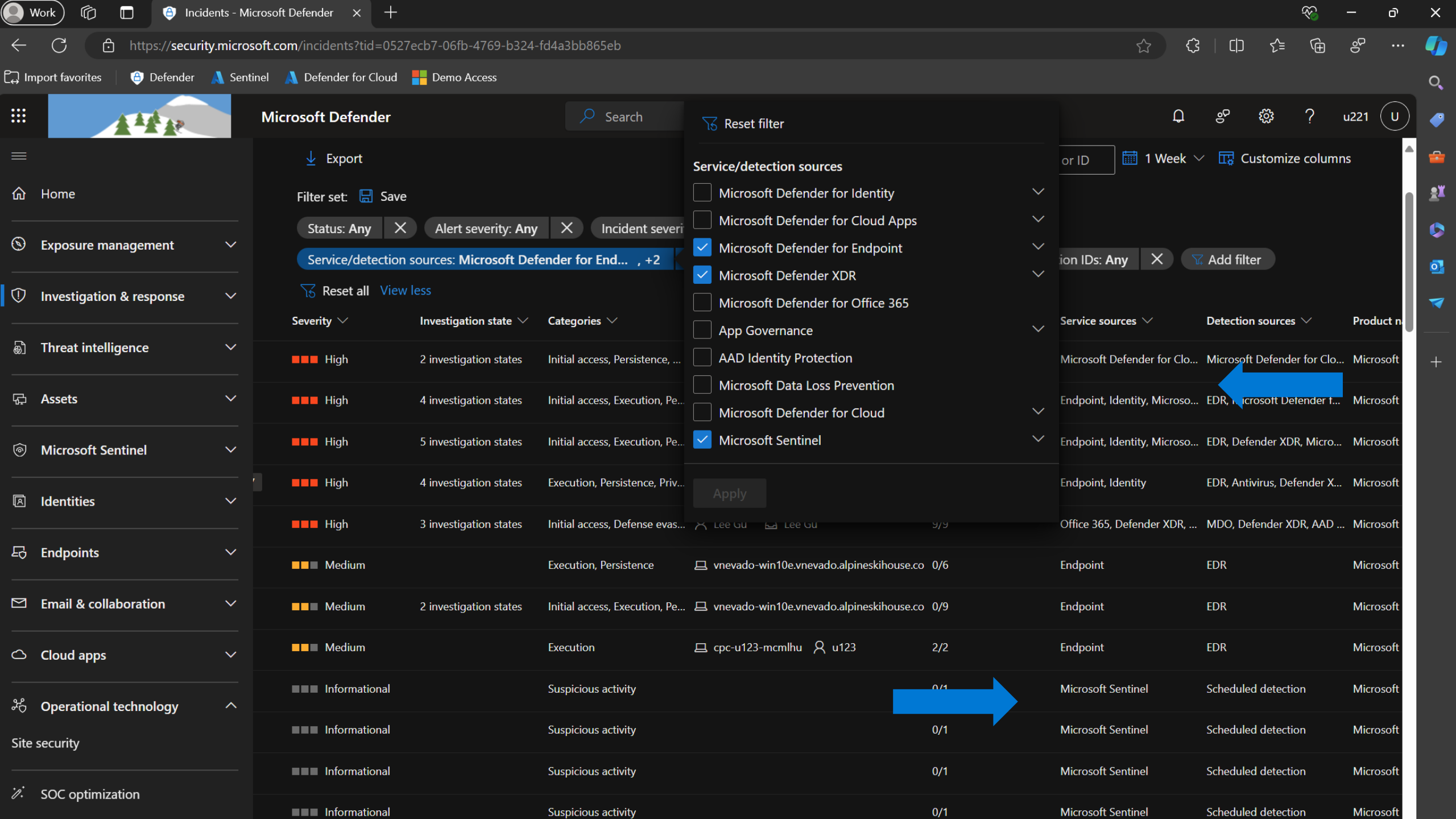
Export | Search for name or ID | 1 Week | Customize columns

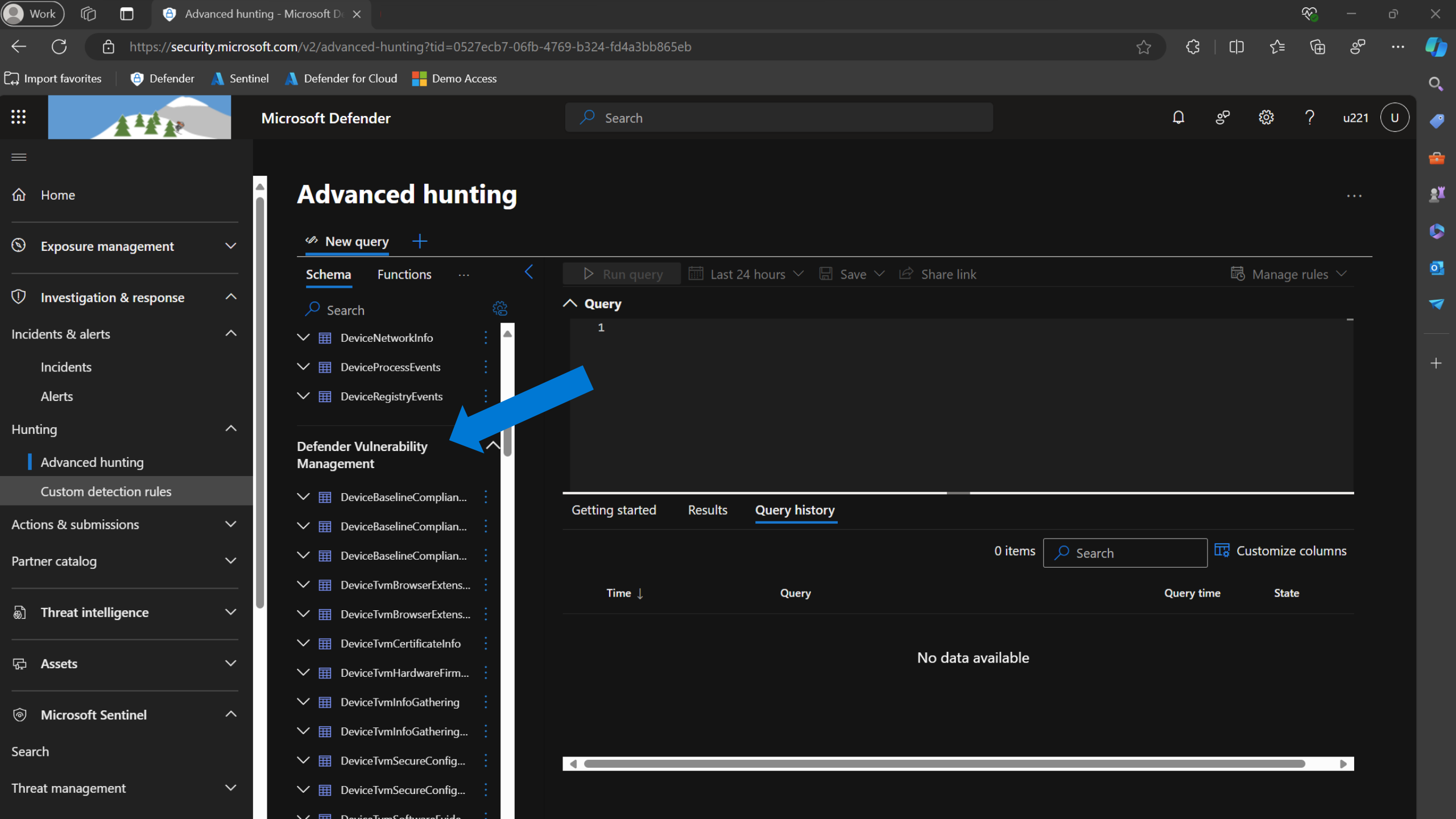
Filter set: Save

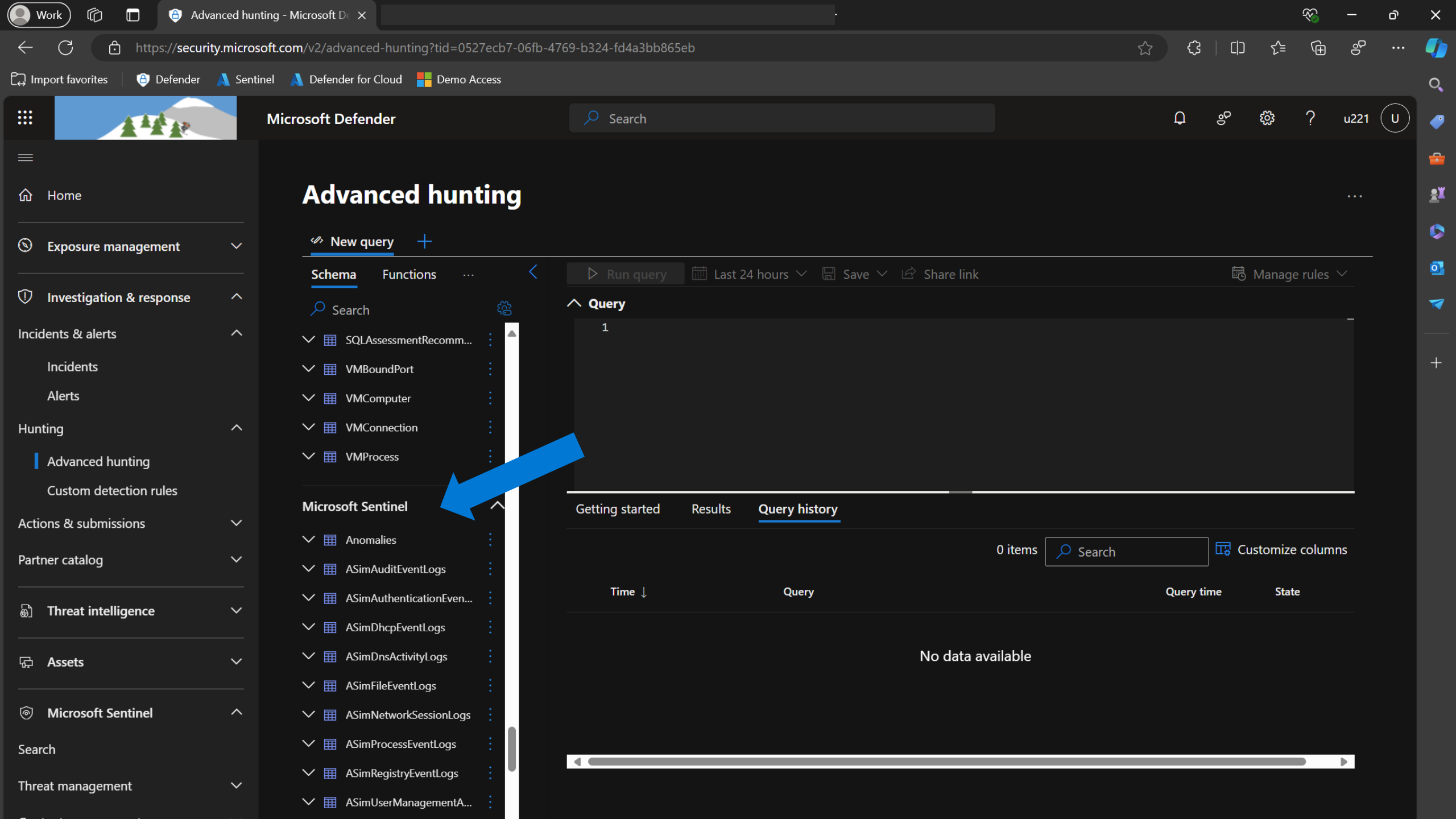
Status: Active, In Progress | Alert severity: High, Medium | Incident severity: High, Medium | Incident assignment: Any | Tags: Any

Entities: Any | Alert subscription IDs: Any | Add filter | Reset all | View less

| Incident name | Incident Id | Tags | Severity | Investigation state | Categories | Impacte |
|---|---|---|---|---|---|---|
| SAP financial process manipulation (attack disrup... | 529 | BEC Fraud +3 | High | 2 investigation states | Initial access, Persistence, ... | Can |
| Suspicious authentication activity on one endpoint | 851 | | Medium | | Initial access | woo |
| Multi-stage incident involving Initial access & Lat... | 551 | Critical asset +5 | High | 5 investigation states | Initial access, Execution, Pe... | 3 D |
| Multi-stage incident involving Privilege escalation... | 751 | Brass Typhoon +7 | High | 4 investigation states | Execution, Persistence, Priv... | 3 D |
| BEC financial fraud attack was launched from a co... | 483 | BEC Fraud +4 | High | 3 investigation states | Initial access, Defense evas... | Lee |
| Multi-stage incident involving Initial access & Dis... | 466 | Backdoor +2 | Medium | 2 investigation states | Initial access, Execution, Pe... | vne |
| Suspicious scheduled task on one endpoint | 848 | | Medium | | Execution | cpc |
| Suspicious authentication activity on one endpoint | 849 | | Medium | | Initial access | alpi |


Work
Incidents - Microsoft Defender
https://security.microsoft.com/incidents?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb
Import favorites
Defender
Sentinel
Defender for Cloud
Demo Access
Microsoft Defender
Search
u221
Export
Filter set:
Save
Status: Any
Alert severity: Any
Incident severi
Service/detection sources: Microsoft Defender for End... , +2
Reset all
View less
Reset filter
Service/detection sources
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender XDR
Microsoft Defender for Office 365
App Governance
AAD Identity Protection
Microsoft Data Loss Prevention
Microsoft Defender for Cloud
Microsoft Sentinel
Apply
or ID
1 Week
Customize columns
ion IDs: Any
Add filter
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Operational technology
Site security
SOC optimization
Severity
Investigation state
Categories
Service sources
Detection sources
Product n
High
2 investigation states
Initial access, Persistence, ...
Microsoft Defender for Clo...
Microsoft Defender for Clo...
Microsoft
High
4 investigation states
Initial access, Execution, Pe...
Endpoint, Identity, Microso...
Microsoft
High
5 investigation states
Initial access, Execution, Pe...
Endpoint, Identity, Microso...
EDR, Defender XDR, Micro...
Microsoft
High
4 investigation states
Execution, Persistence, Priv...
Endpoint, Identity
EDR, Antivirus, Defender X...
Microsoft
High
3 investigation states
Initial access, Defense evas...
Office 365, Defender XDR, ...
MDO, Defender XDR, AAD ...
Microsoft
Medium
Execution, Persistence
vnevado-win10e.vnevado.alpineskihouse.co
0/6
Endpoint
EDR
Microsoft
Medium
2 investigation states
Initial access, Execution, Pe...
vnevado-win10e.vnevado.alpineskihouse.co
0/9
Endpoint
EDR
Microsoft
Medium
Execution
cpc-u123-mcmlhu
u123
2/2
Endpoint
EDR
Microsoft
Informational
Suspicious activity
Microsoft Sentinel
Scheduled detection
Microsoft
Informational
Suspicious activity
0/1
Microsoft Sentinel
Scheduled detection
Microsoft
Informational
Suspicious activity
0/1
Microsoft Sentinel
Scheduled detection
Microsoft
Informational
Suspicious activity
0/1
Microsoft Sentinel
Scheduled detection
Microsoft


Work
Advanced hunting - Microsoft D
https://security.microsoft.com/v2/advanced-hunting?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb
Import favorites
Defender
Sentinel
Defender for Cloud
Demo Access
Microsoft Defender
Search
u221
Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Search
Threat management
Advanced hunting
New query
Schema
Functions
Search
DeviceNetworkInfo
DeviceProcessEvents
DeviceRegistryEvents
Defender Vulnerability Management
DeviceBaselineComplian...
DeviceBaselineComplian...
DeviceBaselineComplian...
DeviceTvmBrowserExtens...
DeviceTvmBrowserExtens...
DeviceTvmCertificateInfo
DeviceTvmHardwareFirm...
DeviceTvmInfoGathering
DeviceTvmInfoGathering...
DeviceTvmSecureConfig...
DeviceTvmSecureConfig...
Run query
Last 24 hours
Save
Share link
Manage rules
Query
1
Getting started
Results
Query history
0 items
Search
Customize columns
Time
Query
Query time
State
No data available


Work
Advanced hunting - Microsoft D
https://security.microsoft.com/v2/advanced-hunting?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb
Import favorites
Defender
Sentinel
Defender for Cloud
Demo Access
Microsoft Defender
Search
u221
U
Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Search
Threat management
Advanced hunting
New query
Schema
Functions
Search
SQLAssessmentRecomm...
VMBoundPort
VMComputer
VMConnection
VMProcess
Microsoft Sentinel
Anomalies
ASimAuditEventLogs
ASimAuthenticationEven...
ASimDhcpEventLogs
ASimDnsActivityLogs
ASimFileEventLogs
ASimNetworkSessionLogs
ASimProcessEventLogs
ASimRegistryEventLogs
ASimUserManagementA...
Run query
Last 24 hours
Save
Share link
Manage rules
Query
1
Getting started
Results
Query history
0 items
Search
Customize columns
Time
Query
Query time
State
No data available

Work | Workbooks - Microsoft Defender

https://security.microsoft.com/sentinel/99005f96-e572-4035-b476-836fd9d83d64/cybersoc/CyberSOC/workbooks?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb

Import favorites | Defender | Sentinel | Defender for Cloud | Demo Access

Microsoft Defender

Search

u221

U

Microsoft Sentinel

Search

Threat management

- Workbooks
- Hunting
- Notebooks
- Threat intelligence
- MITRE ATT&CK

Content management

- Content hub
- Repositories
- Community

Configuration

- Data connectors
- Analytics
- Summary Rules
- Watchlist
- Automation

Identities

# Workbooks

Refresh | Guides

| My workbooks | Templates | Updates | More content at |
|---|---|---|---|
| 4 | 27 | 0 | Content hub |

My workbooks | Templates

Add Workbook

Search | Add filter

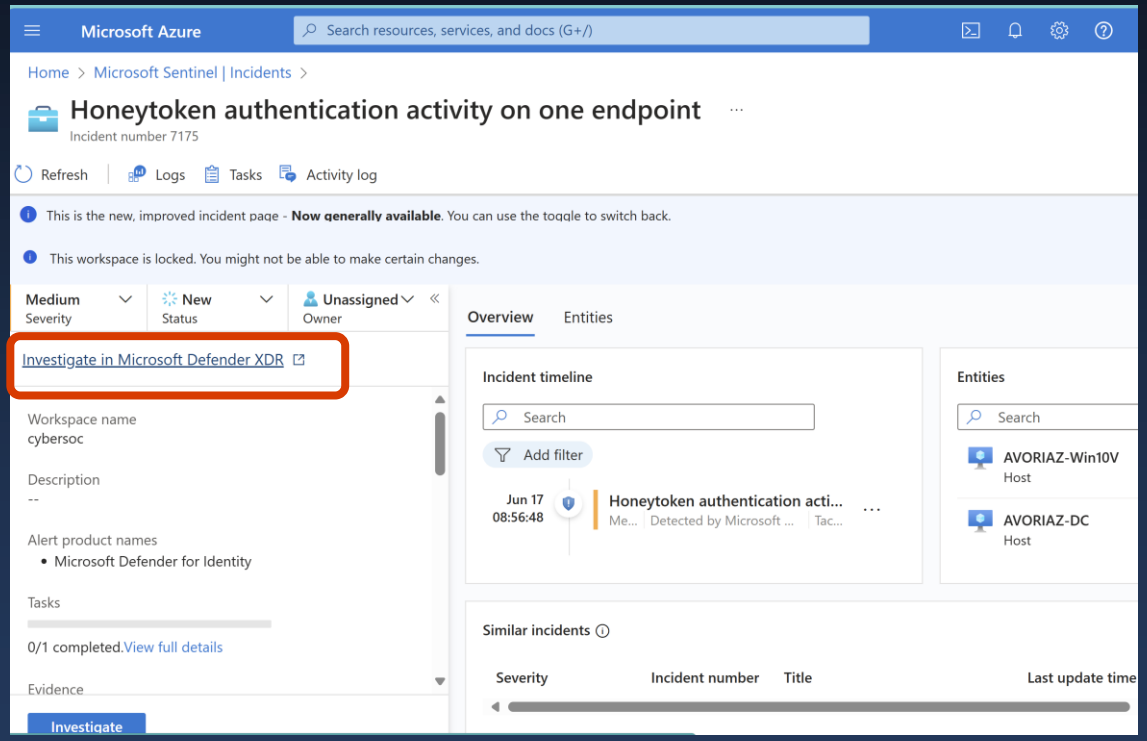
| Name | Content source | Source name |
|---|---|---|
| Azure DDoS Protection Workbook | Content hub | Azure DDoS Prot... |
| Azure Firewall Structured Logs | Content hub | Azure Firewall |
| Microsoft Web Application Firewall (WAF) - Azure WAF | Content hub | Azure Web Appli... |
| Web Session Essentials Workbook | Content hub | Web Session Ess... |

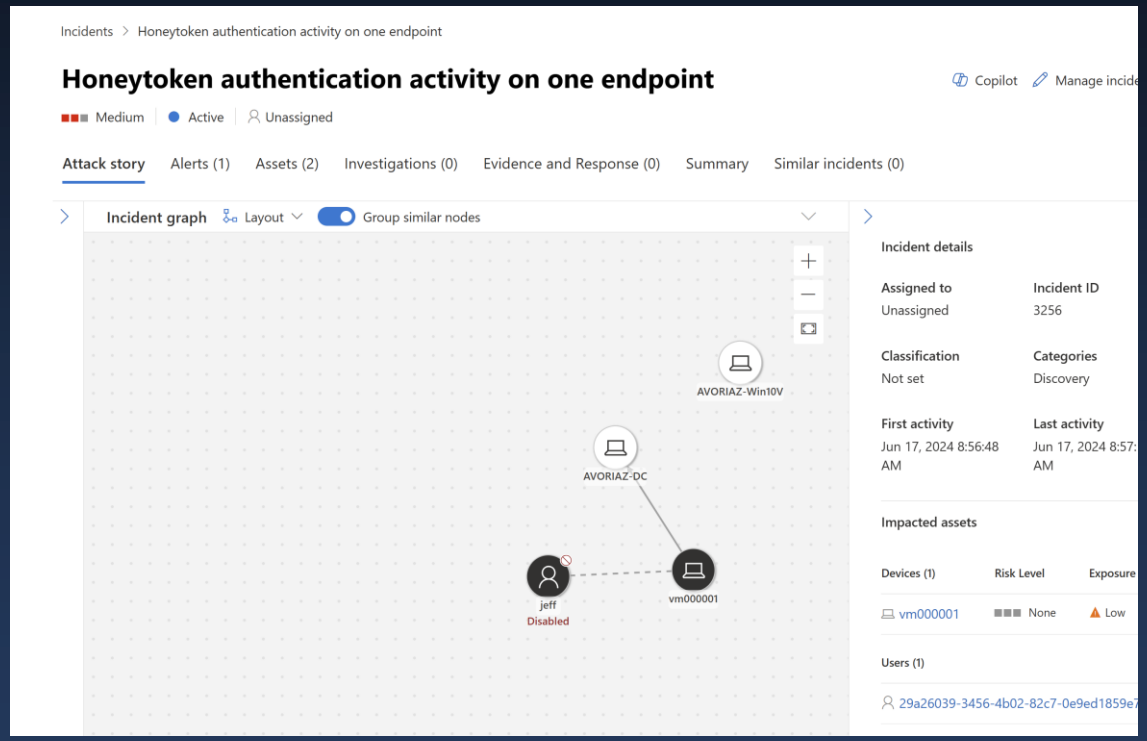
**No workbook selected**
Select workbook to view more details

# What's in it for customers?

| More manageable products | Better hunting capabilities | Improve response and protection |
|---|---|---|
| Microsoft Sentinel has a new home in Defender Portal, resulting in one place to manage all their SOC products. | Customers benefit from one place to create queries and search across their data | Automatic attack disruption expanded to 3rd parties, starting with SAP, more comprehensive incident experience |
| **Cost savings** | **Analyst experience** | **Reduction in incident queue** |
| Customers do not need to ingest their Defender XDR data into Microsoft Sentinel to correlate alerts or hunt | Less portal switching, better incident correlation | Improvement in how Defender XDR data is correlated with Sentinel logs reduces the incident queue and delivers more robust insights. |

# Before: investigations often required two portals



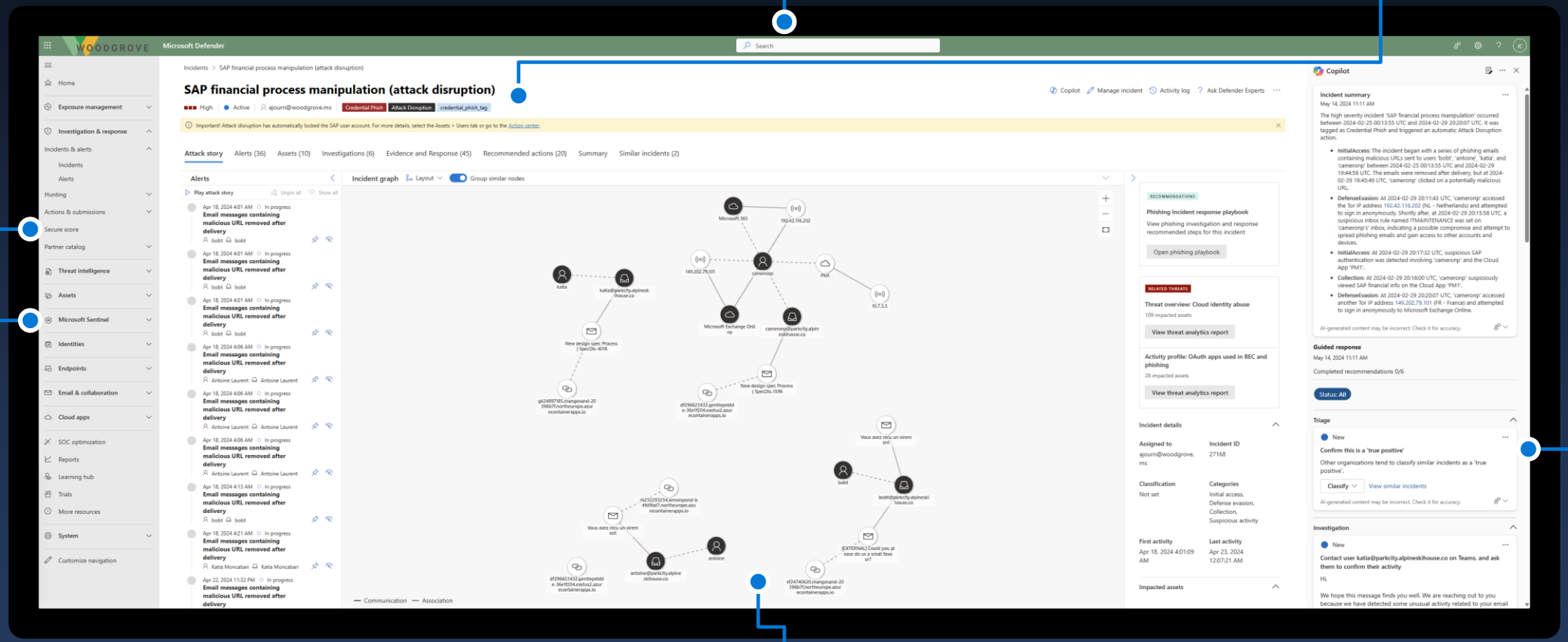



# Now: A single view

**Exposure management**

**Comprehensive incident view**

**Microsoft Sentinel data**




**SIEM and XDR workloads**

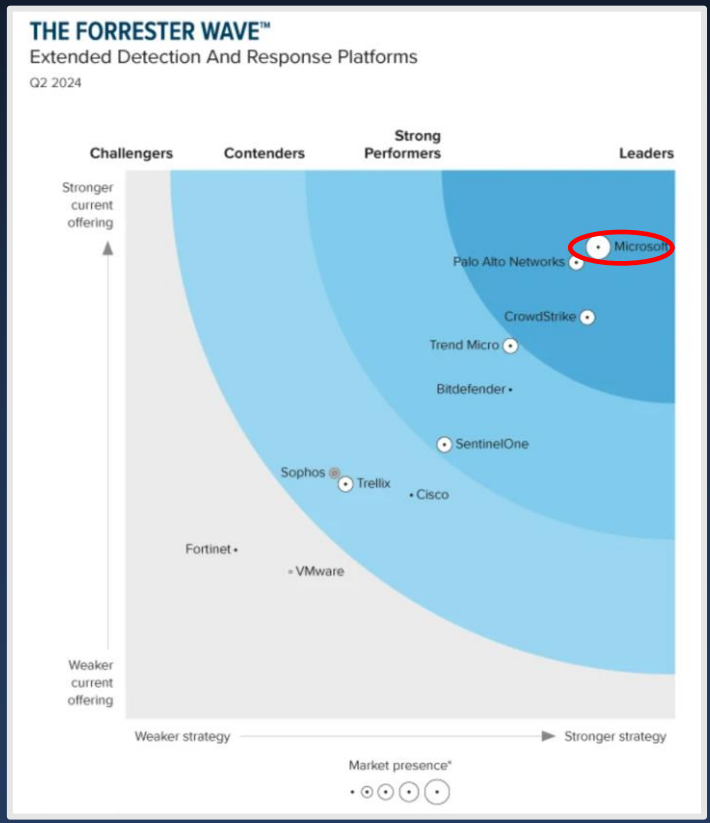
**Single attack map**

**Embedded GenAI**

# Microsoft is the only vendor with leading SIEM+XDR

## Microsoft is named as a Leader in the 2024 Gartner SIEM MQ


## Microsoft is again named a leader in the Forrester Wave for XDR CY2024, Q2




[Microsoft is a Leader in the 2024 Gartner® Magic Quadrant™ for Security Information and Event Management | Microsoft Security Blog]
[Microsoft a Leader in the Forrester Wave for XDR | Microsoft Security Blog]

# Who else claims to have a security operations platform?

## Cisco | Splunk

**Core Components**
SIEM, XDR, GenAI

**Current offering:**
Cisco plans to further integrate XDR, SIEM & GenAI to provide a unified platform for customers. This is a short to mid-term strategy that Cisco is working on and it's currently immature. Cisco is attempting to package natural language search in it's products with Cisco AI Assist.

**Areas Microsoft differentiates:**
- Mature XDR and recognized leader over Cisco XDR and several individual categories
- Leading in AI and innovation
- Cisco has low market penetration for XDR

## Google Cloud

**Core Components**
SIEM, Cloud Security, TI, GenAI

**Current offering:**
Ties together SIEM, SOAR, TI, and cloud security powered by AI into a unified experience. Google lacks an XDR and tries to compensate for this leveraging Mandiant services.

**Areas Microsoft differentiates:**
- Microsoft has an industry leading XDR experience in our unified platform.
- Google does not have an XDR.

## Palo Alto Networks

**Core Components**
SIEM, XDR, Cloud Security, Network, GenAI

**Current offering:**
Palo Alto Networks is attempting to bring together the Strata, Prisma, and Cortex into a single experience and powering this with generative AI.
Currently the 3 platforms are still separate and requires context switching even within 1st party.

**Areas Microsoft differentiates:**
- Microsoft has built a 1st party platform with strong integration. Palo Alto Networks has acquired many of its capabilities and still working on integration experience

## CrowdStrike

**Core Components**
SIEM, XDR, Data Security, TI, Cloud Security, ITDR, GenAI

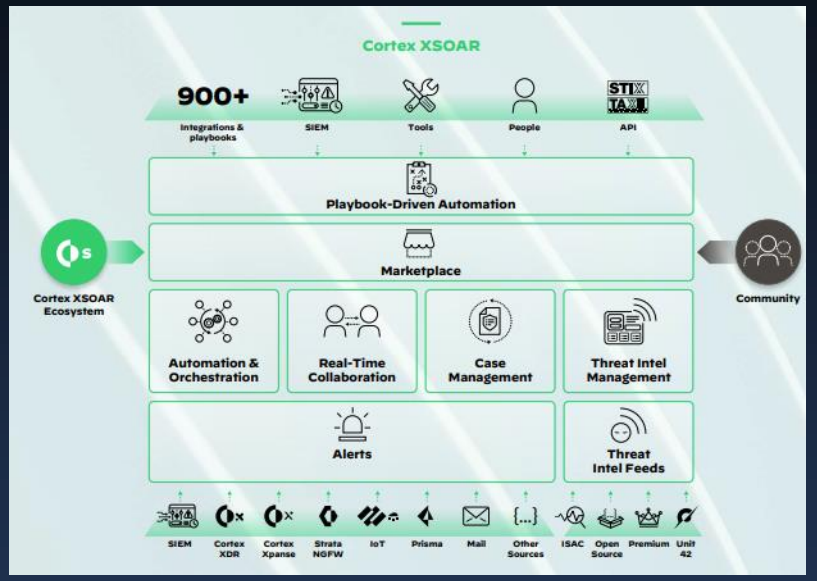
**Current offering**:
CrowdStrike tells customers it's the unified platform with a single agent. Although CrowdStrike competes across several categories across security, endpoint is still it's core offering but is investing in identity, data protection, cloud security, SIEM, and generative AI.

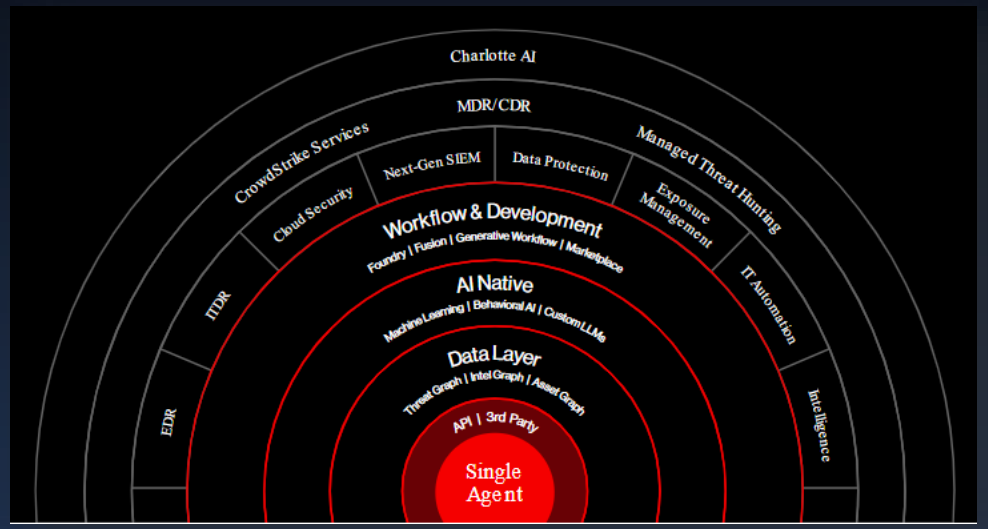
**Areas Microsoft differentiates:**
- Microsoft's XDR is viewed by Forrester as a stronger strategy and larger market penetration.
- Microsoft is a leader across several protection categories within XDR. Including endpoint

- Microsoft is forcing the market to change through increased investments or purchasing/merging with other companies in efforts to catch-up.
- Microsoft is the only company on the list that has built it's platform natively, as opposed to attempting to stitch individual acquisitions together into the ecosystem

# Competitor Platform View

paloalto NETWORKS




CROWDSTRIKE

Chronicle


Sources: SOC Transformation Infographic (paloaltonetworks.com), Chronicle | Suite | Overview, The CrowdStrike Falcon® platform

# Available Material

- GA Announcement Blog published July 11 :https://aka.ms/ZeroTrustBlog-July2024
- MS Learn Documentation: https://aka.ms/onboard-microsoft-sentinel
- Microsoft Mechanics video: Microsoft Defender XDR, Copilot for Security & Microsoft Sentinel now in one portal
- AMA: Microsoft SIEM & XDR: unified security operations
- Webinar: What's New in Microsoft Sentinel & Unified Portal Enhancements
- Virtual Ninja Training - Unifying SIEM & XDR: a new era in SecOps
- Get started with the general availability of Microsoft Sentinel in the Defender Portal with some helpful FAQs.
- Manually deploy playbooks in the unified experience.

# SOC Optimisation







## SOC optimization: unlock the power of precision-driven security management

By Michal Shechter
Published May 06 2024 09:07 AM


Security operations center (SOC) teams actively look for opportunities to optimize both processes and outcomes. Every organization is unique, with its own security challenges. Teams must regularly adjust security controls to keep up with changing threat landscape and business priorities, while balancing investment (cost, SOC resources, time) and security coverage.

Today, we're happy to announce the public preview of a new experience and API – Microsoft Sentinel's SOC Optimization, designed to empower security teams with precision-driven management capabilities. SOC optimization offers **actionable tailored recommendations** that adapt daily to the organization's environment – starting with gaps in data utilization and detection of different types of attacks . These aren't generic tips; they're personalized strategies backed

Co-Authors
MichalShechter

Version history

**Last update:** May 06 2024 01:02 AM
**Updated by:** MichalShechter

Share

Work | SOC Optimization - Microsoft De | https://security.microsoft.com/sentinel/precision?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb

Import favorites | Defender | Sentinel | Defender for Cloud | Demo Access

Microsoft Defender | Search | u221

- Data connectors
- Analytics
- Summary Rules
- Watchlist
- Automation
- Identities
- Endpoints
- Email & collaboration
- Cloud apps
- Operational technology
- Site security
- SOC optimization
- Reports
- Learning hub
- Trials
- More resources

# SOC optimization

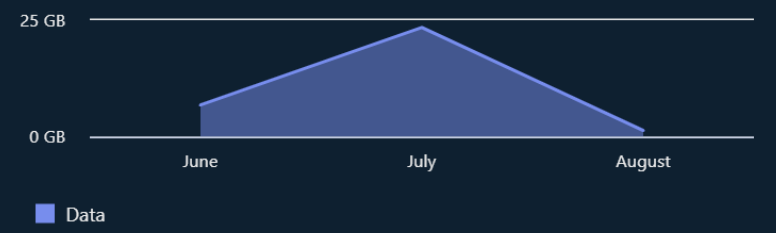
Overview | Completed | Dismissed

## Your optimizations data

**Recent optimizations value**

Utilized SquidProxy_CL table and improved your SOC coverage.

**Data ingested**




**Threat-based coverage optimizations**

**AiTM (Adversary in the Middle)**
Medium | 39/64 Recommended detections

**BEC (Financial Fraud)**
High | 40/52 Recommended detections

**BEC (Mass Credential Harvest)**
High | 75/97 Recommended detections

View all threat scenarios

**Optimizations status**

| Active | In progress | Completed | Dismissed |
|---|---|---|---|
| 32 | 0 | 5 | 0 |

Data connectors
Analytics
Summary Rules
Watchlist
Automation
Identities
Endpoints
Email & collaboration
Cloud apps
Operational technology
Site security
SOC optimization
Reports
Learning hub
Trials
More resources

# Your Optimizations

Filters: Optimization type: All

32 items | Search

Active

**Coverage improvement against AiTM (Adversary i...**
Creation date May 22, 2024 10:37 PM
We discovered that you can improve your coverage against AiTM (Adversary in the Middle).

**Value**
Improve your coverage against AiTM (Adversary in the Middle) attacks from Medium to High.

Coverage | CyberSOC

View full details

Active

**Coverage improvement against BEC (Financial Fra...**
Creation date May 22, 2024 10:37 PM
We discovered that you can improve your coverage against BEC (Financial Fraud).

**Value**
Improve your coverage against BEC (Financial Fraud) attacks.

Coverage | CyberSOC

View full details

Active

**Coverage improvement against BEC (Mass Creden...**
Creation date May 22, 2024 10:37 PM
We discovered that you can improve your coverage against BEC (Mass Credential Harvest).

**Value**
Improve your coverage against BEC (Mass Credential Harvest) attacks.

Coverage | CyberSOC

View full details

Active

**Coverage improvement against ERP (SAP) Financi...**
Creation date May 22, 2024 10:37 PM
We discovered that you can improve your coverage against ERP (SAP) Financial Process Manipulation.

**Value**
Improve your coverage against ERP (SAP) Financial Process Manipulation attacks from Medium to High.

Coverage | CyberSOC

Active

**Coverage improvement against Human Operated ...**
Creation date May 22, 2024 10:37 PM
We discovered that you can improve your coverage against Human Operated Ransomware.

**Value**
Improve your coverage against Human Operated Ransomware attacks from Medium to High.

Coverage | CyberSOC

Active

**Coverage improvement against IaaS Resource Theft**
Creation date May 22, 2024 10:37 PM
We discovered that you can improve your coverage against IaaS Resource Theft.

**Value**
Improve your coverage against IaaS Resource Theft attacks from Low to High.

Coverage | CyberSOC

Microsoft Security

# Questions

For a copy of today's slides, go to this link
https://aka.ms/snackables-unified-soc