THAILAND Cyber Security

Microsoft Security

Cloud

SECURITY

Intensive

Security Operations 2

XDR +

SIEM

AntiVirus
Endpoint DR
eXtended DR

SC-900

SECURITY
COMPLIANCE
IDENTITY

365 Defender

for Identities

- Prevent Cred./**Password Leak**
- Signal from **On-Prim AD DS**
- Enable **MFA on risk level**

for Endpoint (MDE)

- Auto Investigate/Remediate
- Atk surface reduction
- 1st line of defense = Net Protect
- Windows **(VM)**, macOS, Linux, **Android**, iOS, and network devices

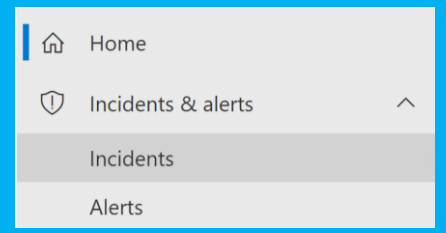
for Office 365

- Data on 365 Cloud
  - SharePoint/OneDrive
  - Outlook (Exchange)

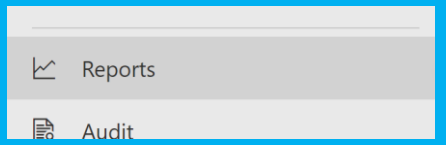
for Cloud Apps

- Cloud Apps Sec (MCAS)
- Control **Access via Cond.Access**

365 Defender Portal
security.microsoft.com



- Incidents
  - = **Aggregated** Alert
  - Affected **Devices**



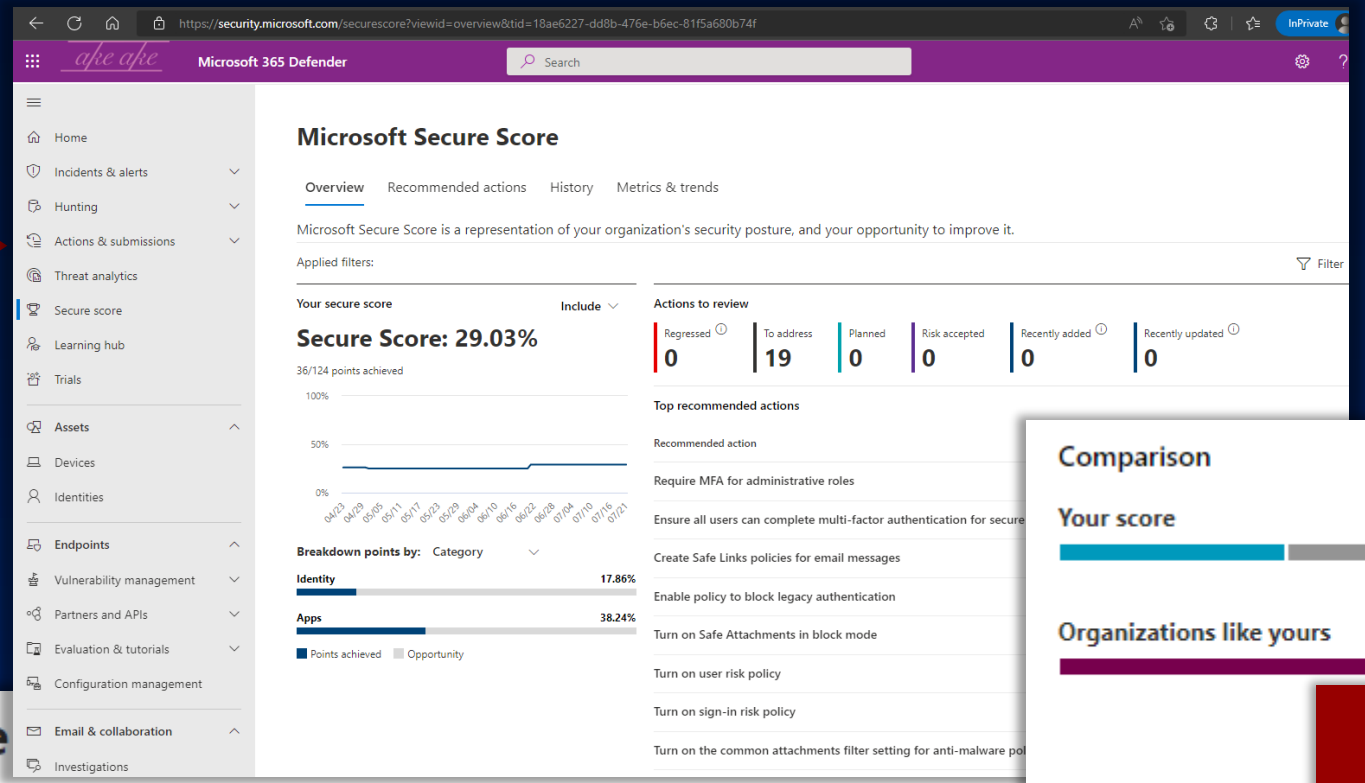
- Report > Trend + Status

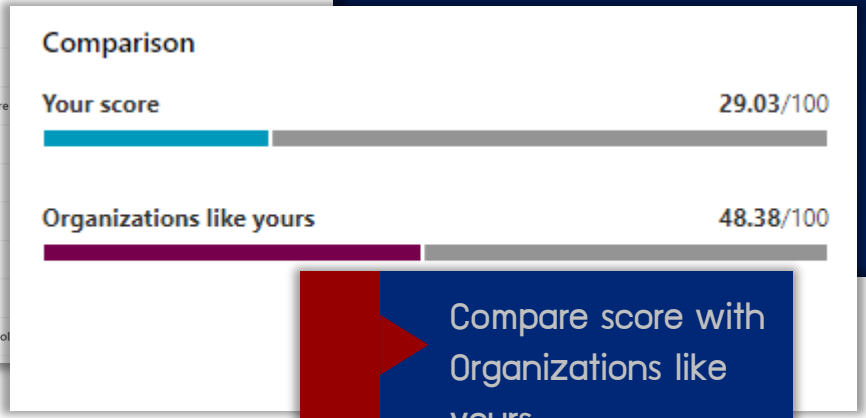
THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS





Compare score with Organizations like yours

Microsoft Secure Score can provide recommendations for MCAS

Can get points even use 3rd party app/software to improve

Microsoft Secure Score

Overview | Recommended actions | History | Metrics & trends

SaaS Security Posture Management for non-Microsoft applications is currently in public preview for every customer with Defe... licensing of this capability may be changed

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

Applied filters:

Export | 1 item | cloud app | Filter | Group by

Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product	Las
12	Create an app discovery policy to identify new and trending c...	+2.42%	0/3	To address	No	Yes	Apps	Microsoft Defender for Clou...	7/1

SC-900

SECURITY
COMPLIANCE
IDENTITY

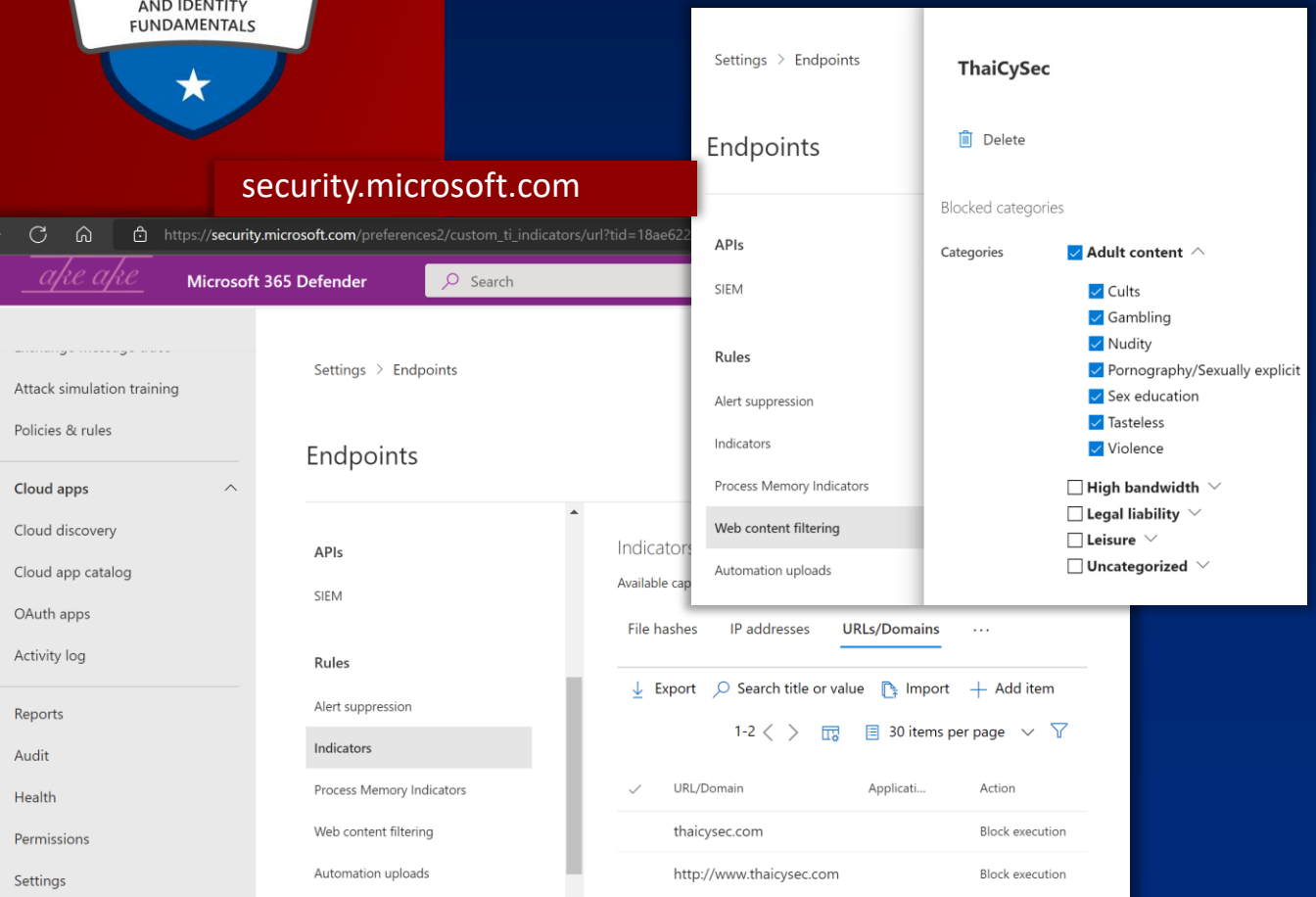
Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

Network Protection

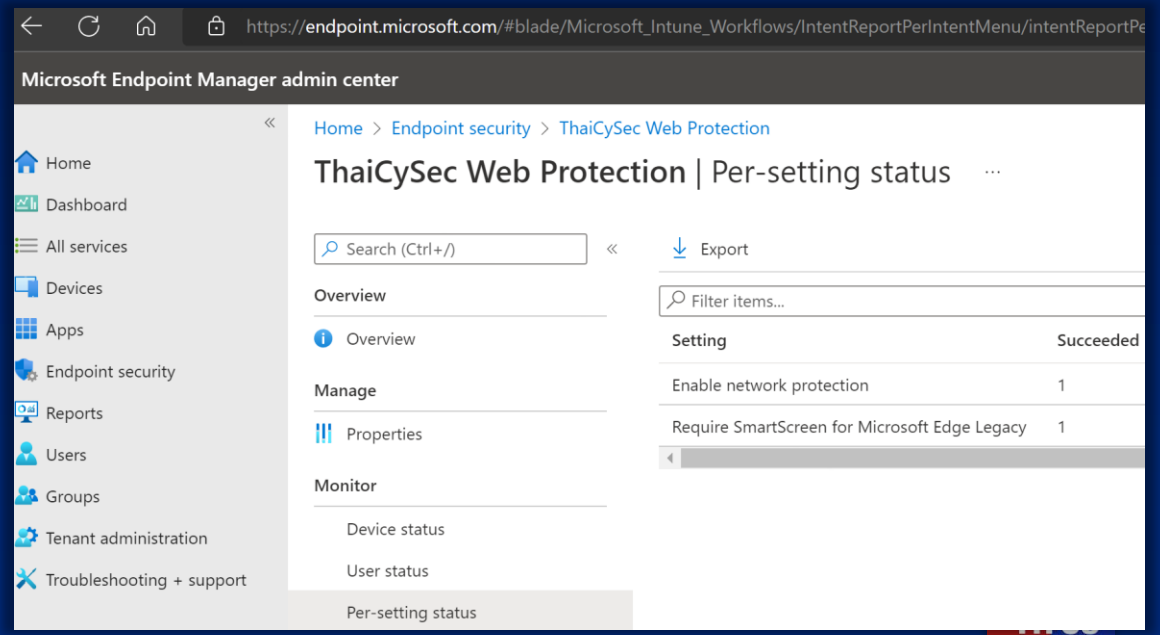
(MDE feature + Intune ASR Policy)

Reducing attack surface as 1st line of defense by preventing access to dangerous/unwanted URL

security.microsoft.com



endpoint.microsoft.com



Defender for Endpoint (MDE)

Admin roles

"Global" "Admin"	Security "Admin"	Security "Operator"	Security "Reader"
View (esp. reports)			
Investigate			
Respond			
Manage Sec Policies			
Assign roles			

💣 Cautions! Some Qs do not ask for "Least priviledge" so any capable role in choices can be the answer.

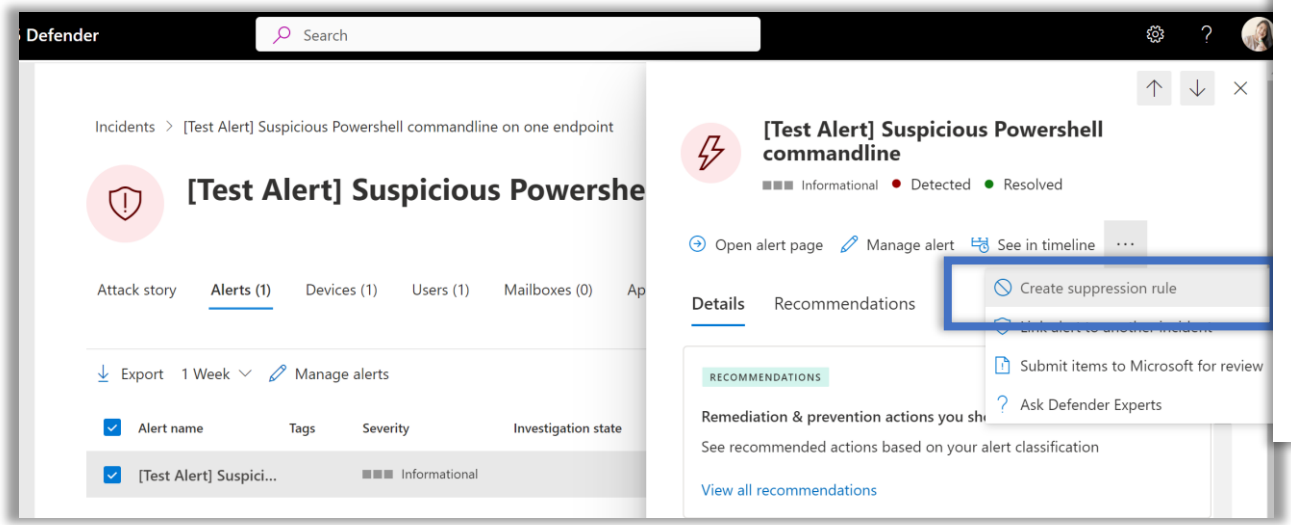
"Global" "Reader" is the read-only version of Global Admin, so they can read anything, esp. outside security portal.

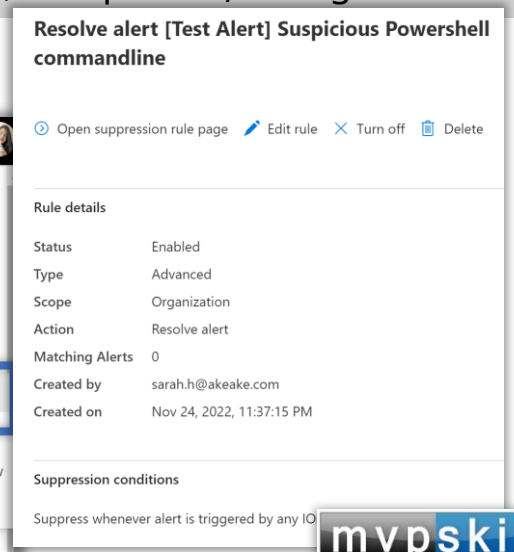
Defender for Endpoint (MDE)

Getting Start

Instruction for Starter

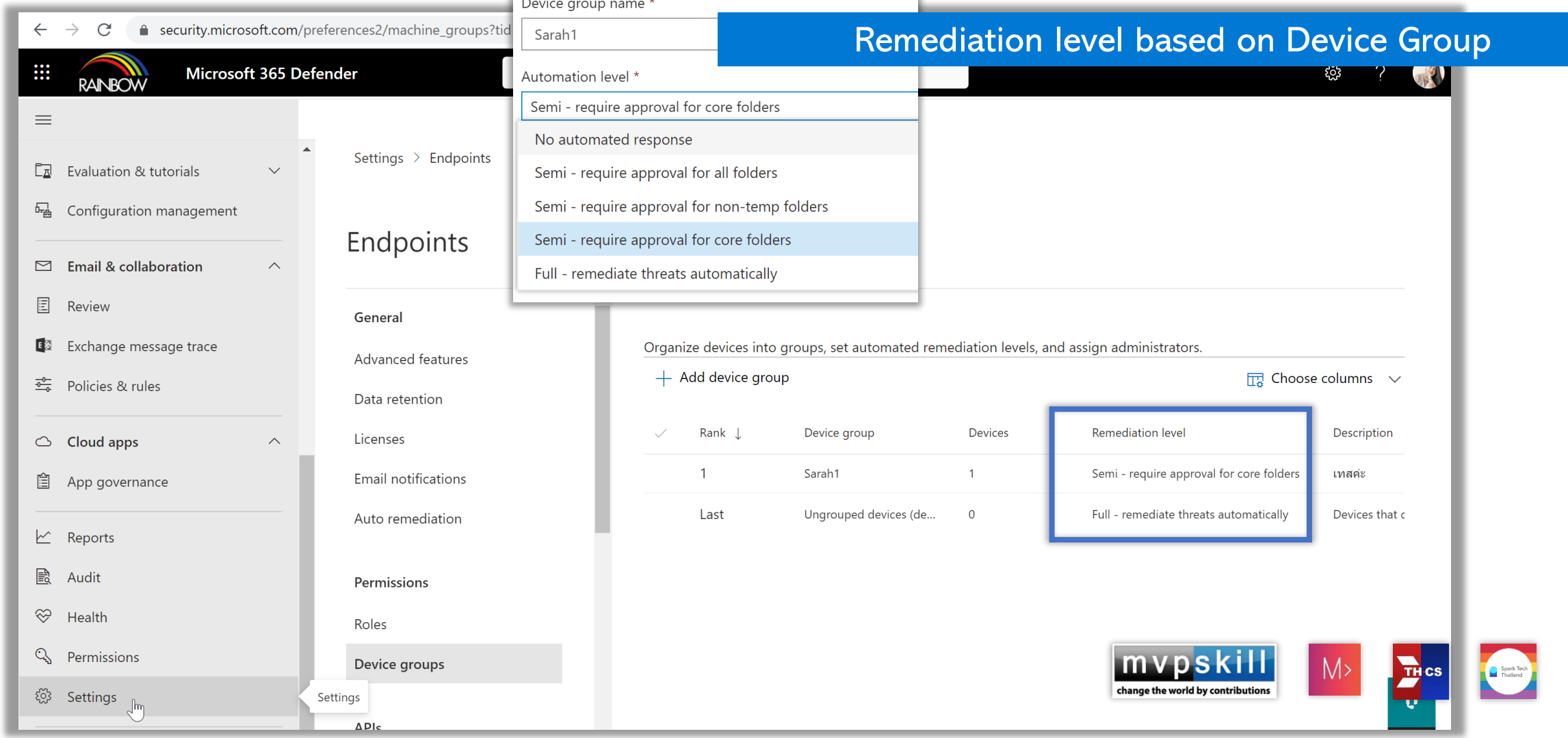
- Get Licenses (P1/P2 or incl. in M365 E3/E5)
- Onboard devices
- Create/Assign to Device Groups (optional) and assign Remediation level (to full?) to each group
- Deploy Security Policies via Intune/GPO (optional) Ex. ASR, EDR (AV), Compliance/Configuration
- Tune/Suppress Alert Levels to reduce noise





Defender for Endpoint (MDE)

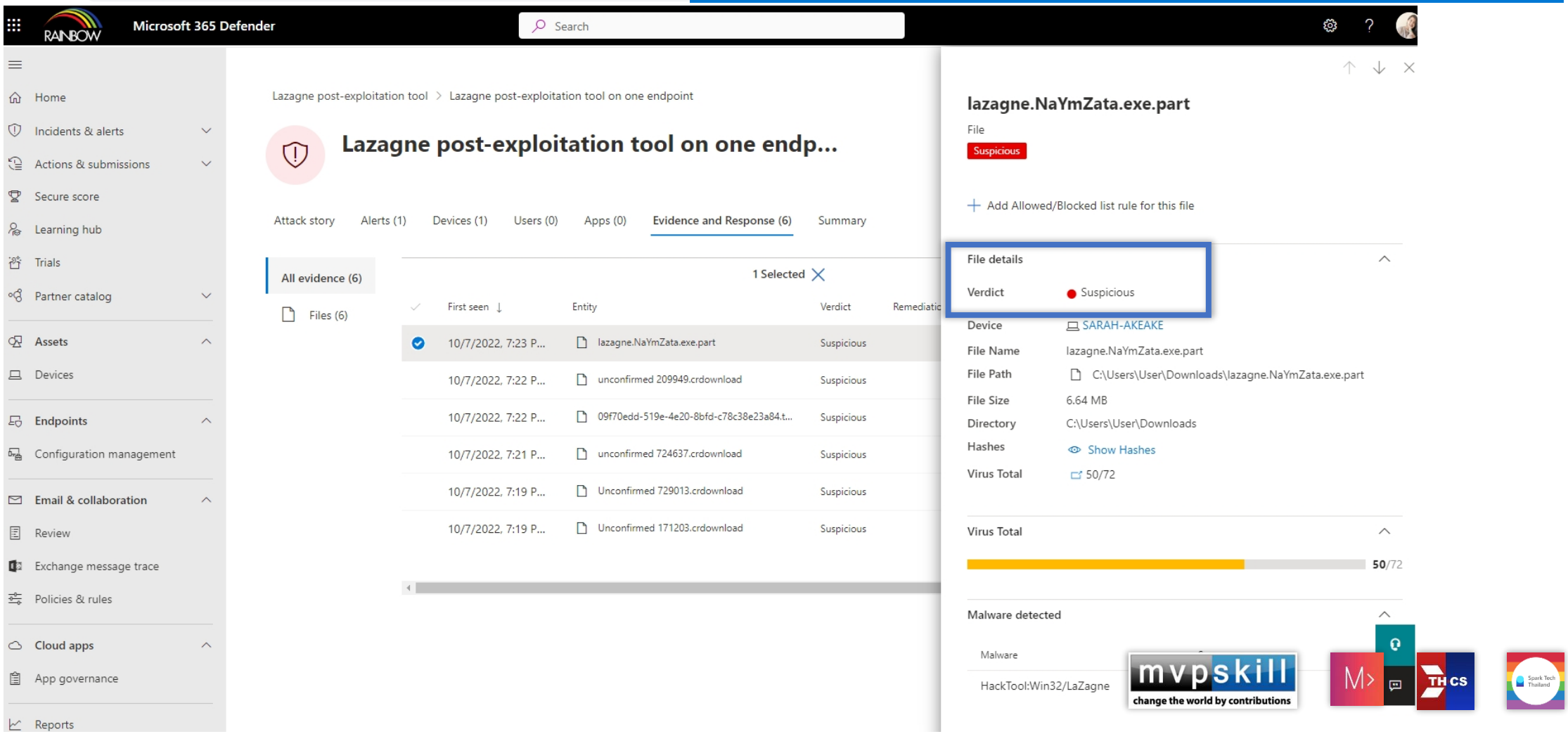
Remediation for Files



Defender for Endpoint (MDE)

Remediation for Files

File Verdict



Defender for Endpoint (MDE)

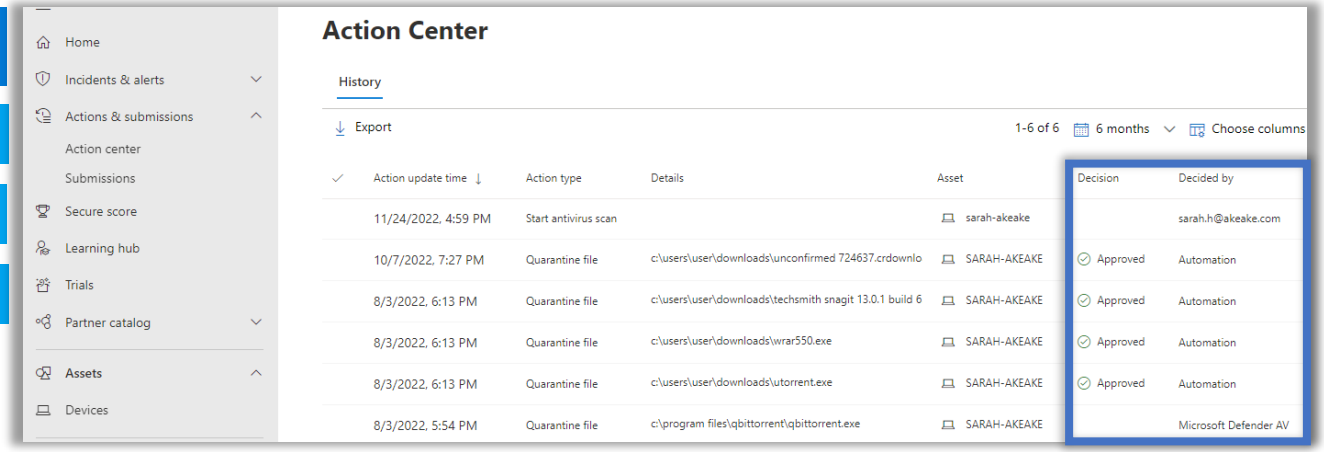
Remediation for Files

Depends on

File Verdicts	Malicious	Suspicious	No threats found	
Device Group Automation Level	full	Semi	Semi-Core Folders	Semi-Non Temp	No Auto Resp
Type of Threat ??? (follow MITRE?)				

Auto-remediate if:

- Full + Malicious
- Semi-Core Folders + Malicious + Not in OS folders
- Semi-Non Temp + Malicious + in Temp* folders

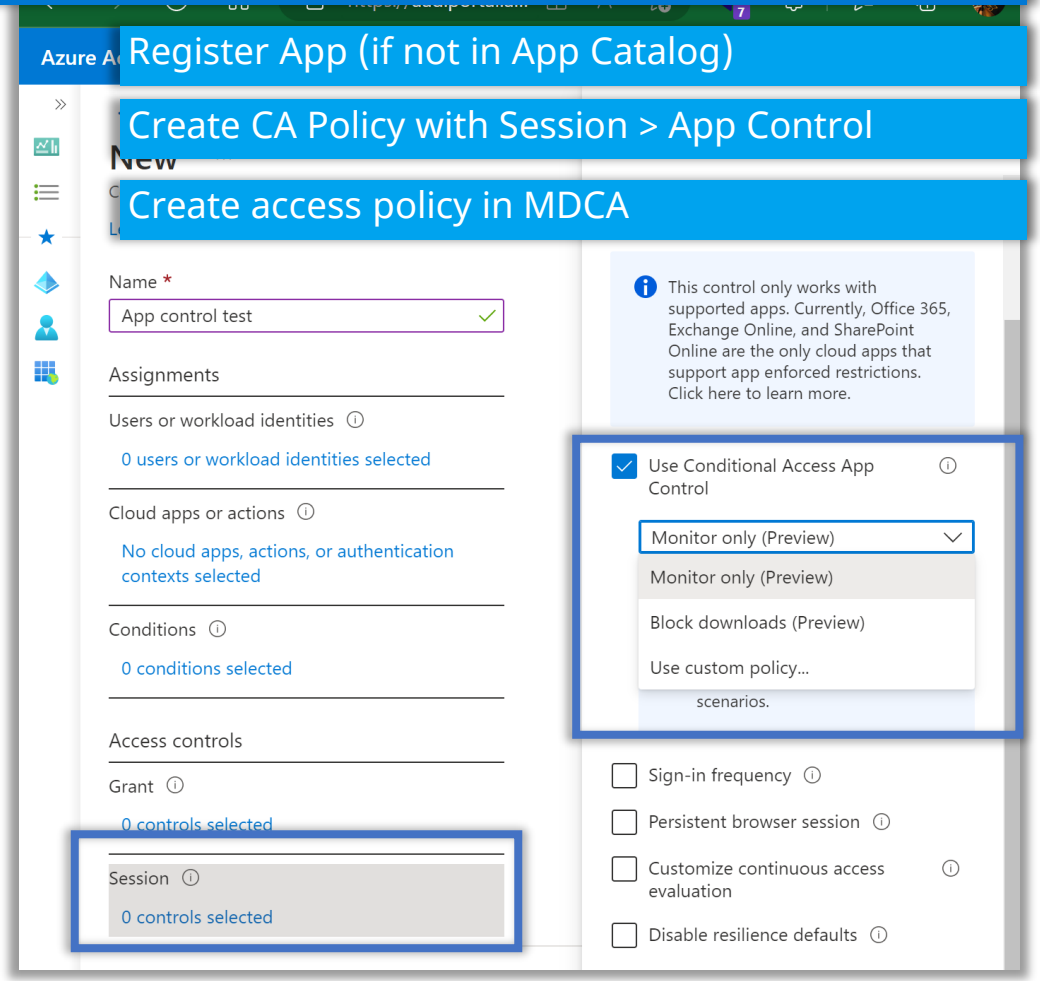


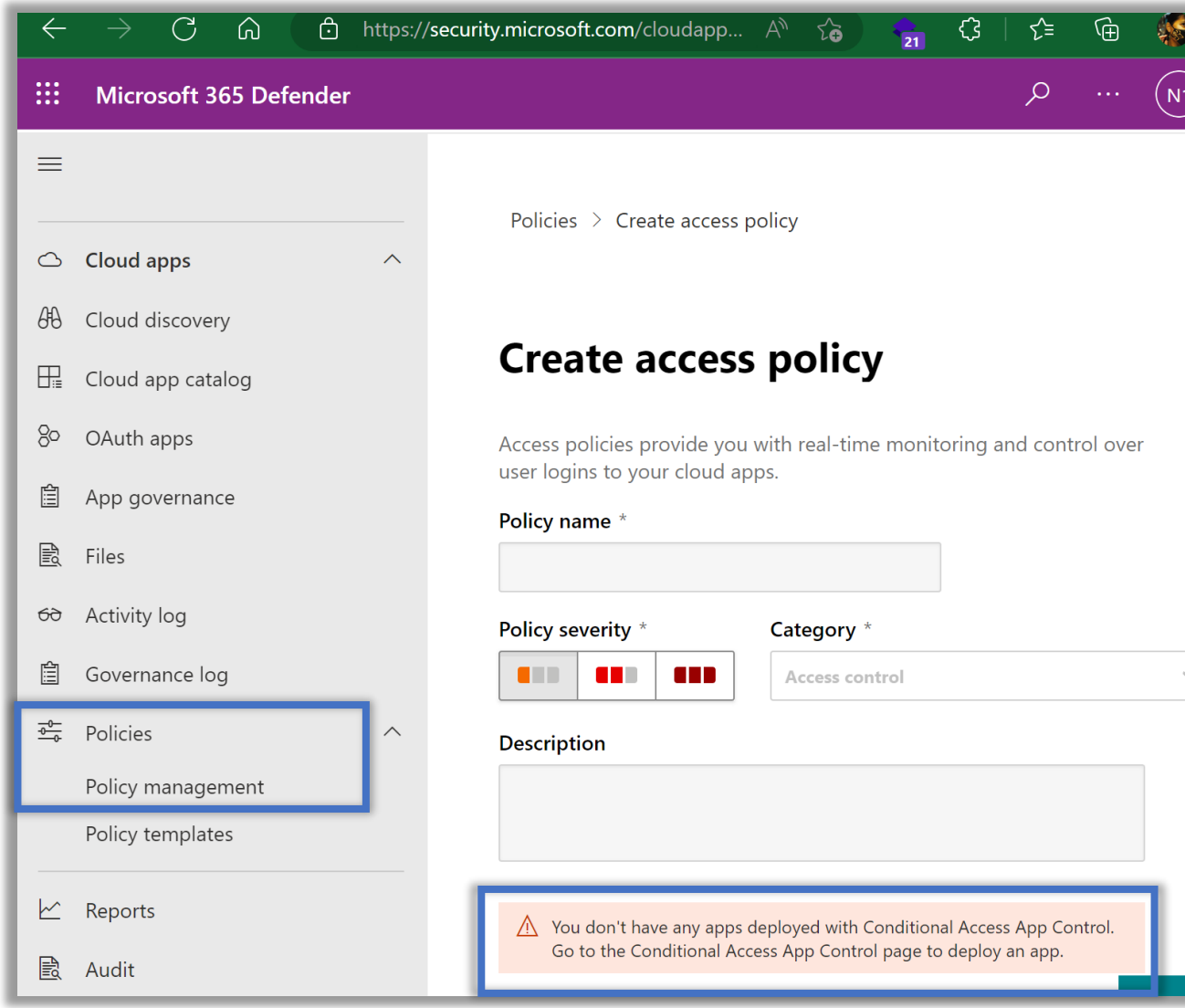
Defender for Cloud Apps

Access Policy

Instruction to review sessions in real-time:

- Register App (if not in App Catalog)
- Create CA Policy with Session > App Control
- Create access policy in MDCA





Defender for Office 365

Connect to MDE

Integrate with MDE

To share info, esp. about endpoints

Turn on Connect to MDE, in MDE Settings on Explorer page

Then turn on “Office 365 Threat Intelligence connection” in Settings > Endpoints > Adv Feat.

Microsoft Defender for Endpoint connection

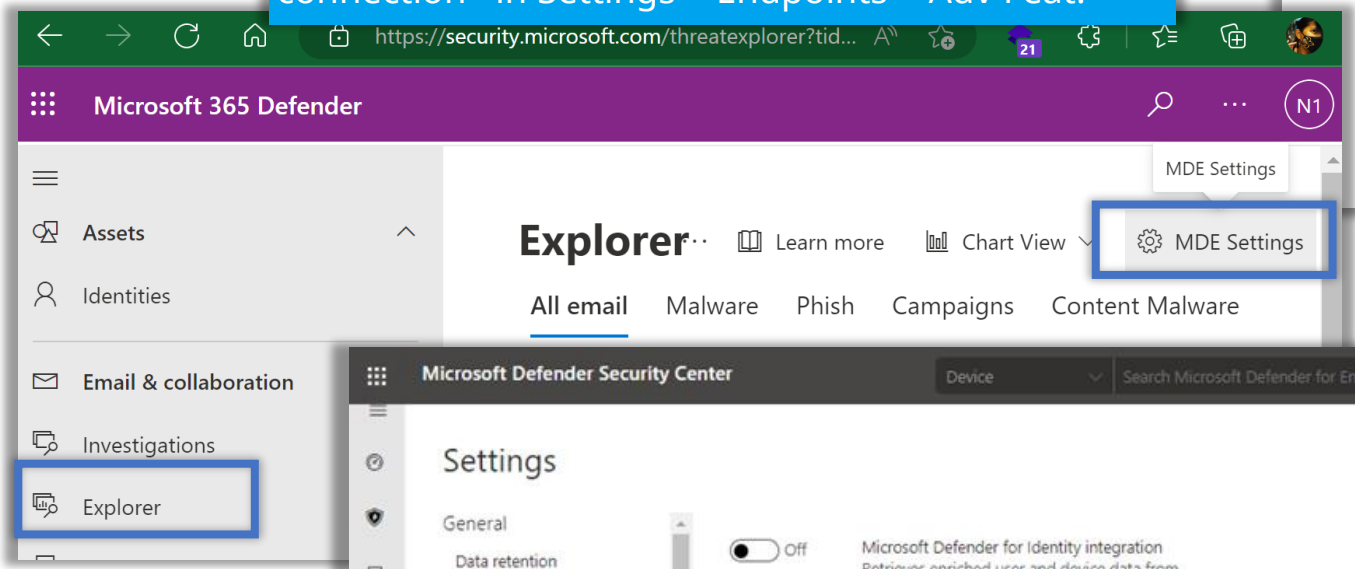
Connect to Defender for Endpoint On

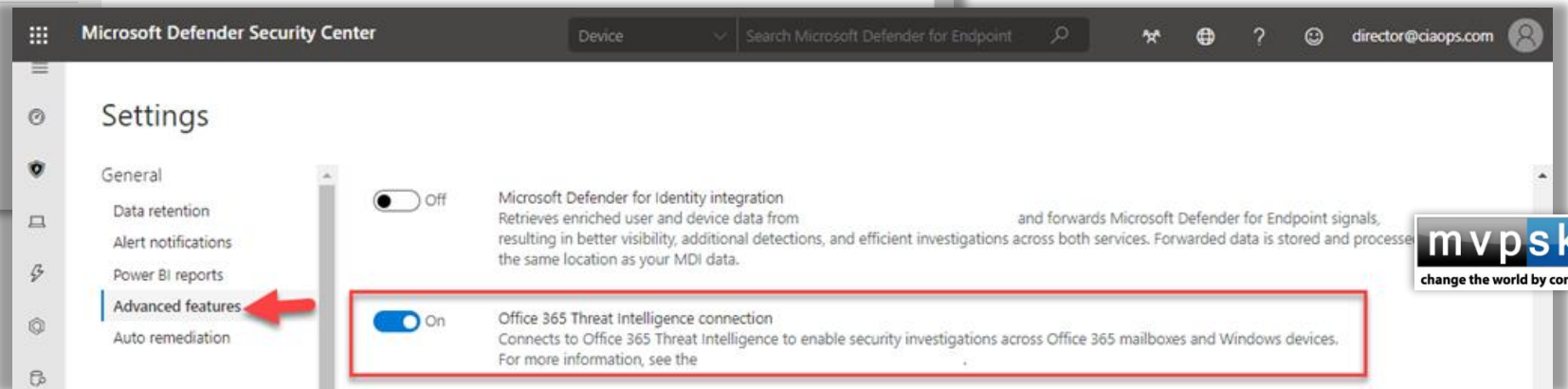
Use this feature to investigate threats between Office 365 and windows devices. When you turn this on:

- You will be able to view device details and Microsoft Defender for Endpoint alerts from the Threat Explorer.
- Microsoft Defender for Endpoint will be able to query Office 365 for email data in your organization and show links back to filtered views in the Threat Explorer.

Note: To turn on this connection, your organization must have a Microsoft Defender for Endpoint subscription and security analysts must have access to Defender for Office 365 P2 and Microsoft Defender for Endpoint.
Learn more about Microsoft Defender for Endpoint

ⓘ After enabling this feature in Office 365, enable the connection from the Windows Security Center.



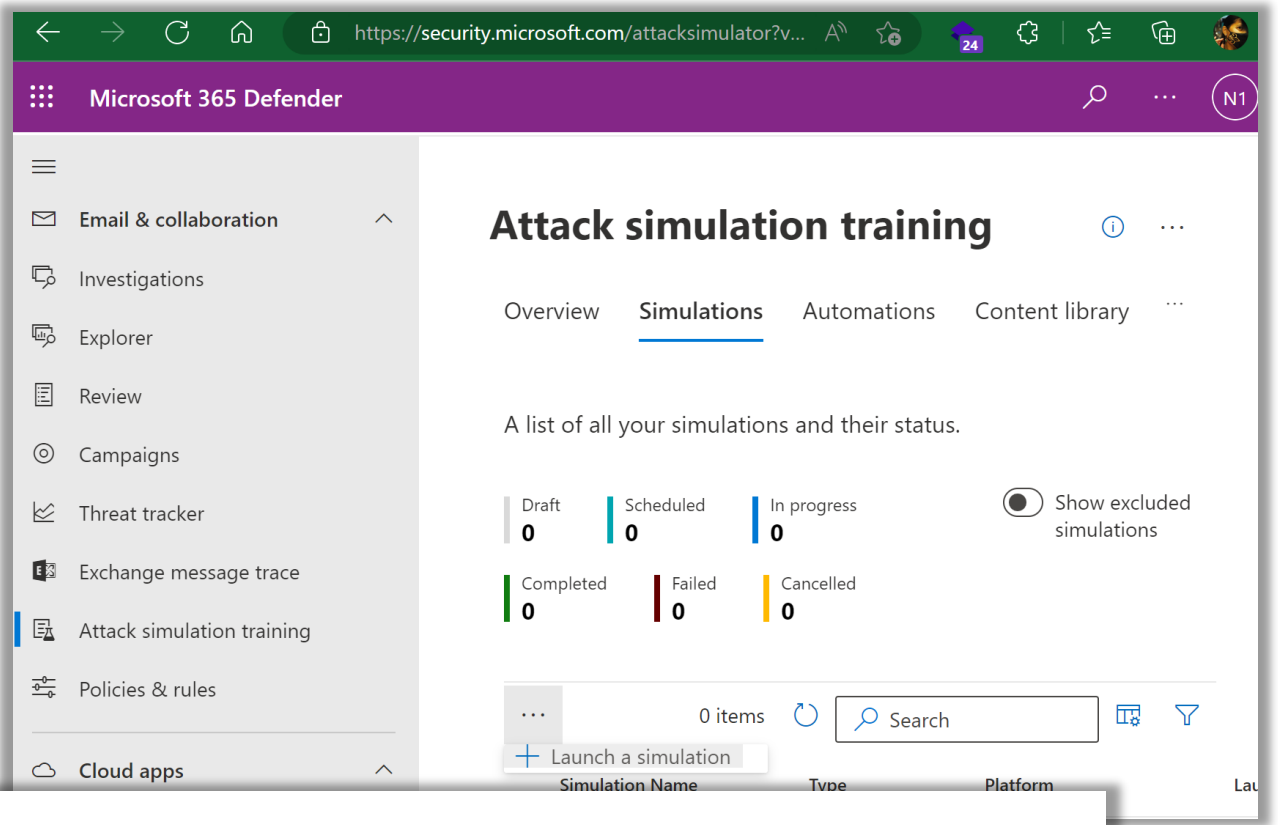


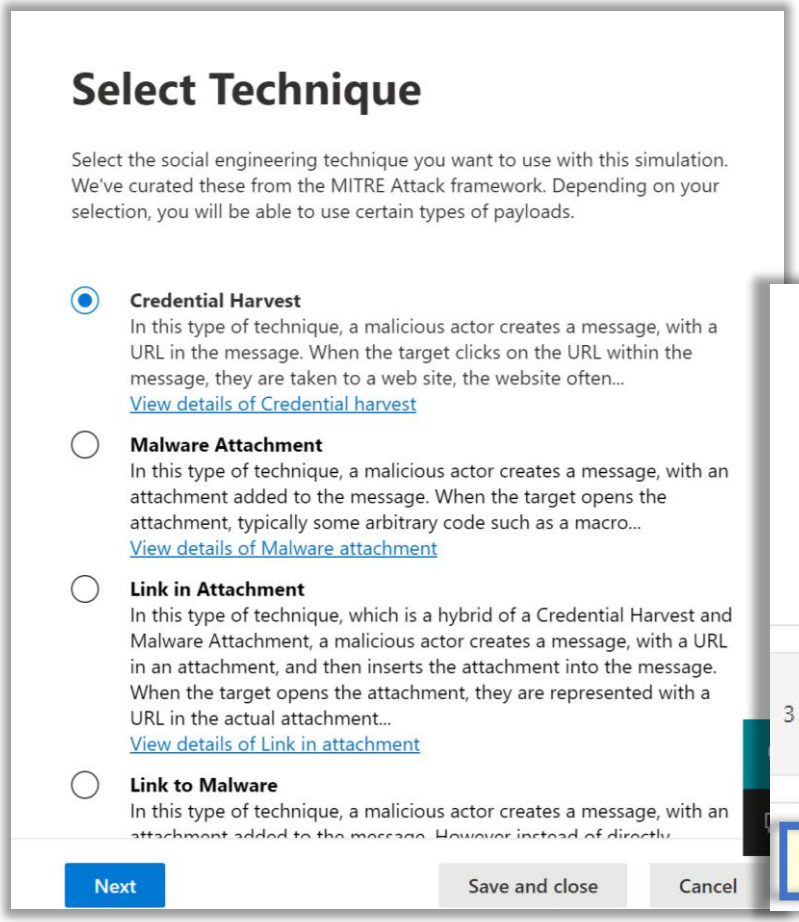
Defender for Office 365

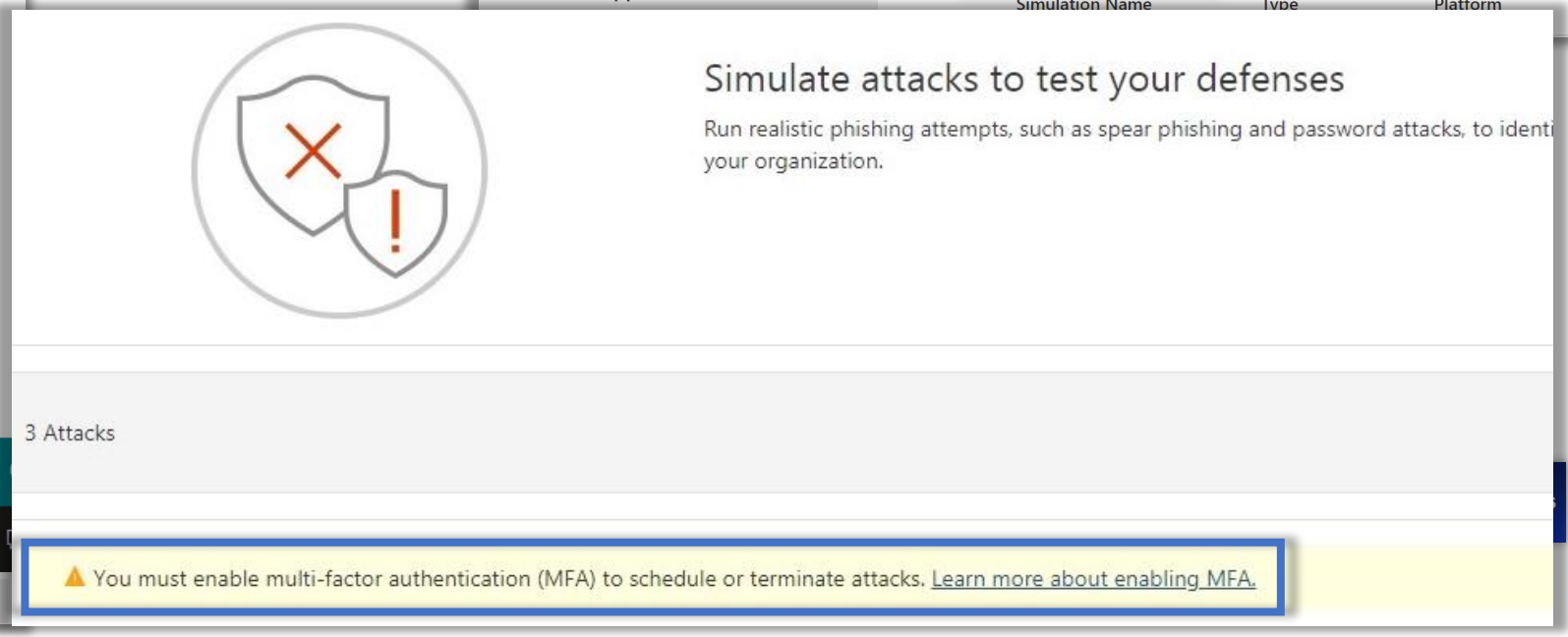
Attack Simulation

Target mailbox must be on-cloud: Exchange Online

Org.Mgmt/Sec Admin/Attack Admin “who launch” the attack have to enable MFA for security.

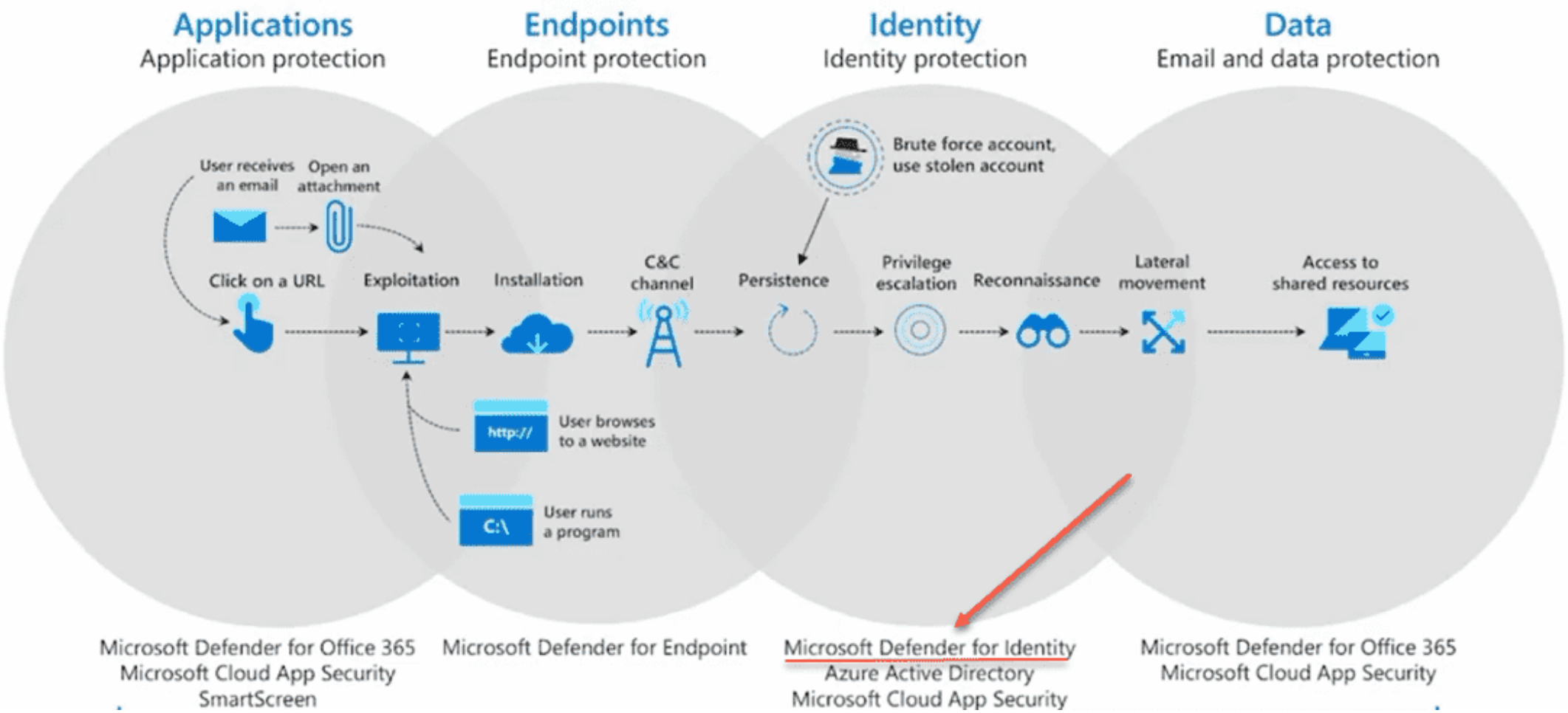






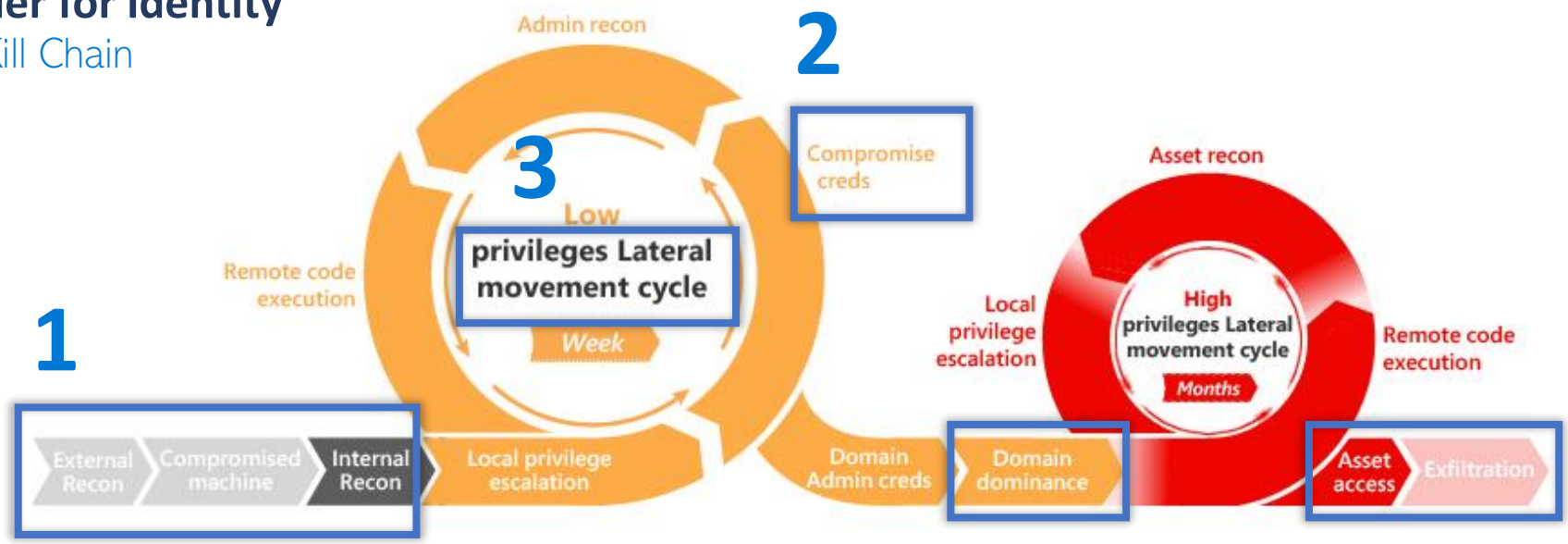
Defender for Identity

Defense Stack



Defender for Identity

Attack Kill Chain



1: Recon

Acc.Enum, AD Recon, NetMap, User-Group-IP

2: Compromise Credentials

SAM, Brute, Kerberos Expose, Netlogon Privesc

3: Lateral Movement

Exploits, PTH, NTLM relay

4: Domain Dominance

DCShadow, DCSync, Golden Ticket, Skeleton Key

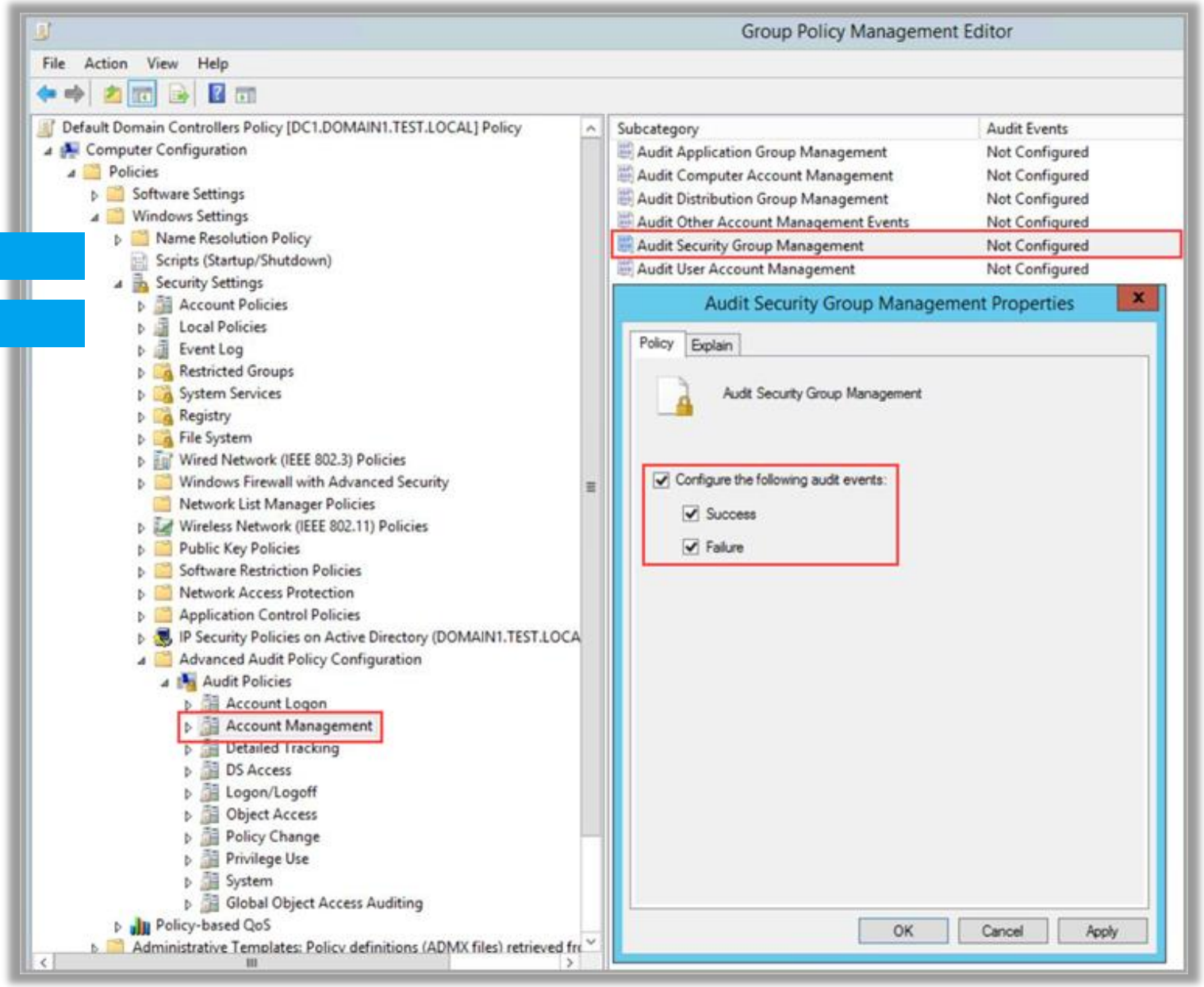
5: Exfiltration

Exfil over SMB, DNS

Defender for Identity
Windows Event Collection

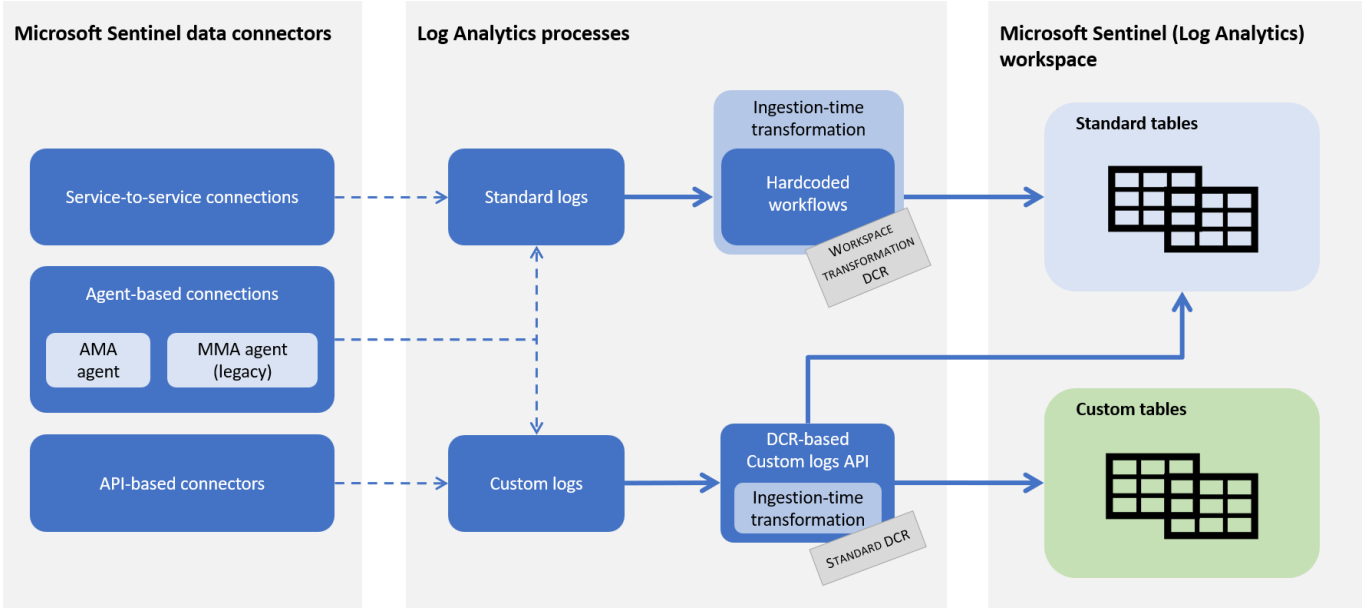
Some requires configure “Advance Audit Policy” in DC

Such as “NTLM” logon



MS Sentinel
Getting Start

- Create Log Analytic Workspace: as datalake from connectors
- Create MS Sentinel on that Workspace
- Connect to Connectors
- Create/Enable Analytic Rules to get Alerts (optional)
- Create Workbook to visualize/ see statistic data from Connectors (opt.)
- Create Playbook (Logic App) for automation, ex. When rules trigger. (optional)



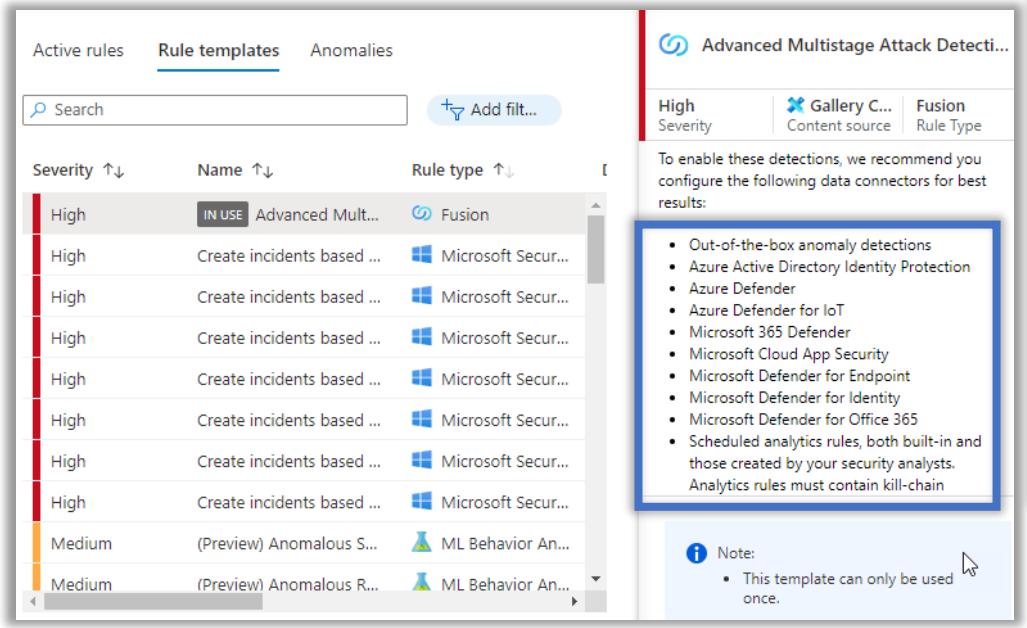
MS Sentinel
Analytic Rules

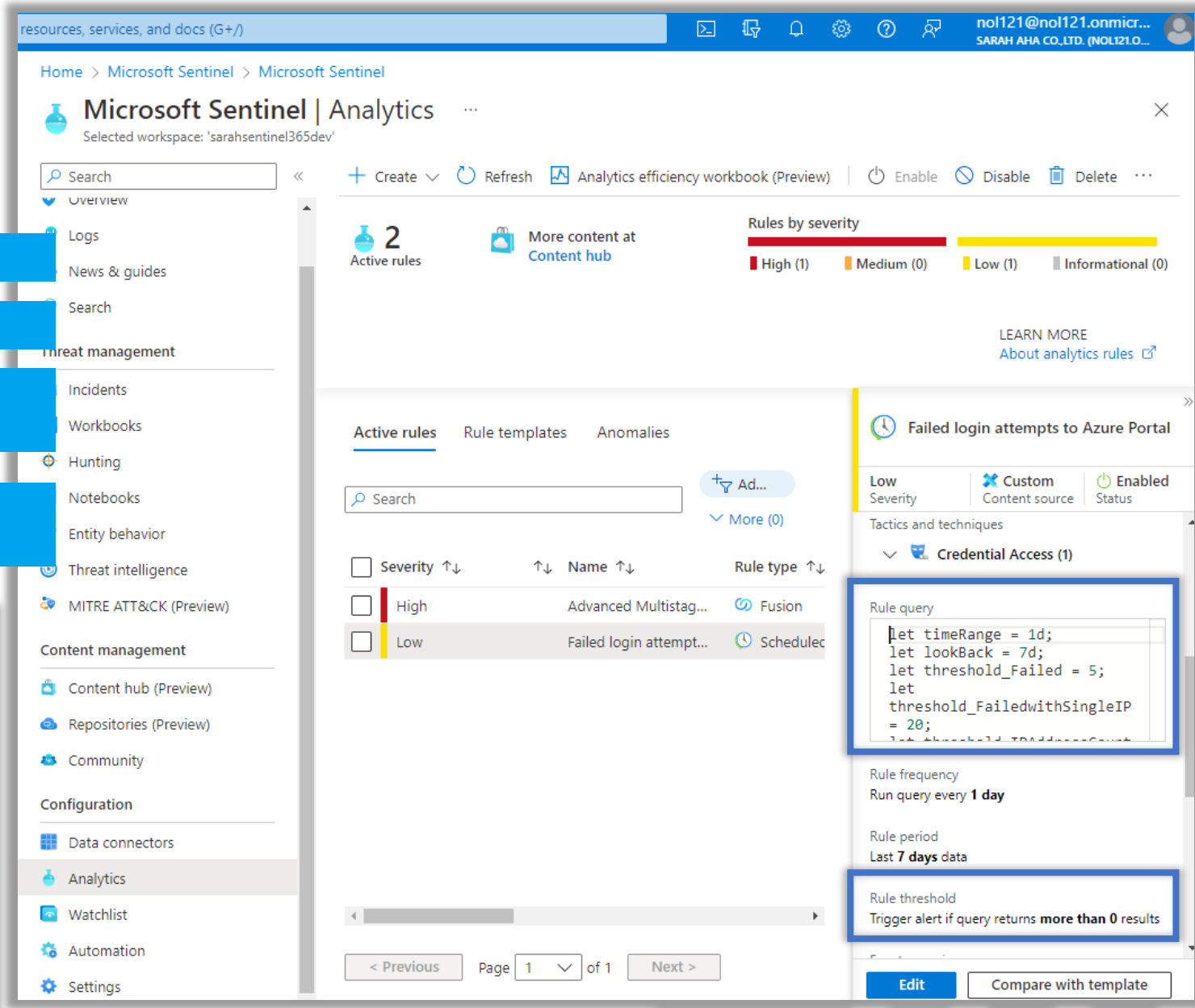
a log query to detect event we want to know as “alert”

📣 No rule = No alert

“Fusion” rule: only “one” rule detect multi-stage attacks (ATP)

“Fusion” rule: fusion from many connectors, so should connect all connectors that they are suggested.





mvpskill
change the world by contributions

You configure several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.
You need to allow a user named User1 to view Defender for Office 365 reports from the Threat management dashboard.
Which role provides User1 with the required role permissions?

A. Security administrators
B. Information Protection administrator
C. Message center reader
D. Service administrator

Answer: A

Because no Sec Reader in choices

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.
You need to allow a user named User1 to view ATP reports from the Threat management dashboard.
Which role provides User1 with the required role permissions?

A. Compliance administrator
B. Security reader
C. Message center reader
D. Reports reader

Answer: B

Sec.Reader is the “least privilege” that can read/view anything in security.microsoft.com

You have a Microsoft 365 subscription that contains a user named User1.
You plan to use Compliance Manager.
You need to ensure that User1 can assign Compliance Manager roles to users. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Compliance Manager Assessor
B. Global Administrator
C. Portal Admin
D. Compliance Manager Administrator

Answer: B

Role assignment is for “Global” admin only

You configure Microsoft Defender for Endpoint as:

Device group	Automation level
Group1	Full – remediate threats automatically
Group2	Semi – require approval for core folders
Group3	Semi – require approval for all folders

You onboard devices to Microsoft Defender for Endpoint as:

Name	In device group
Device1	Group1
Device2	Group2
Device3	Group3

Microsoft Defender for Endpoint contains the incidents shown:

Name	Device	File evidence	File verdict
Case1	Device1	C:\Temp\File1.exe	Suspicious
Case2	Device2	C:\Temp\File2.exe	Malicious
Case3	Device3	C:\Temp\File3.exe	Malicious

Statements	Yes	No
C:\Temp\File1.exe will be remediated automatically.	○	○
C:\Temp\File2.exe will be remediated automatically.	○	○
C:\Temp\File3.exe will be remediated automatically.	○	○

Answer: N/Y/N

Suspicious for Full-remediate is not auto-rem.
And C:\Temp\ is not core folders

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users:

Name	Member of
User1	Group1
User2	Group2

You register devices in contoso.com as shown in the following table.

Name	Platform	Member of	Microsoft Intune managed
Device1	Windows 10	GroupA	Yes
Device2	iOS	GroupB	No

You create app protection policies in Intune as shown in the following table.

Name	Platform	Management state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	With enrollment	Group2
Policy3	iOS	Apps on Intune managed devices	GroupA
Policy4	iOS	Apps on Intune managed devices	GroupB

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	○	○
When User2 uses Device1, Policy2 applies.	○	○
When User2 uses Device2, Policy4 applies.	○	○

Answer: N/Y/N

Consider from “users” POV:

User 1- Group 1 is for Policy 1, but Device 1 is Win10, so should be Policy 1, not 3.

User 2-Group 2 is for Policy 2, and Device 1 is Win10, so should be Policy 2 as the statement.

User 2-Group 2 is for Policy 2, but Device 2 is iOS, so no any policy applied.

You have several Conditional Access policies that block noncompliant devices from connecting to services.
You need to identify which devices are blocked by which policies.
What should you use?

A. the Device compliance report in the Microsoft Endpoint Manager admin center
B. the Device compliance trends report in the Microsoft Endpoint Manager admin center
C. Activity log in the Cloud App Security portal
D. the Conditional Access Insights and Reporting workbook in the Azure Active Directory admin center

Answer: D, in AAD

All sign-ins / access logs must be in Entra > AAD

Your company has a Microsoft 365 subscription.
The company does not permit users to enroll personal devices in mobile device management (MDM).

Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.

The users must be prevented from backing up the app's data to iCloud.
What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
B. an app protection policy in Microsoft Endpoint Manager
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
D. a device compliance policy in Microsoft Endpoint Manager

Answer: B, use App Protection in Intune

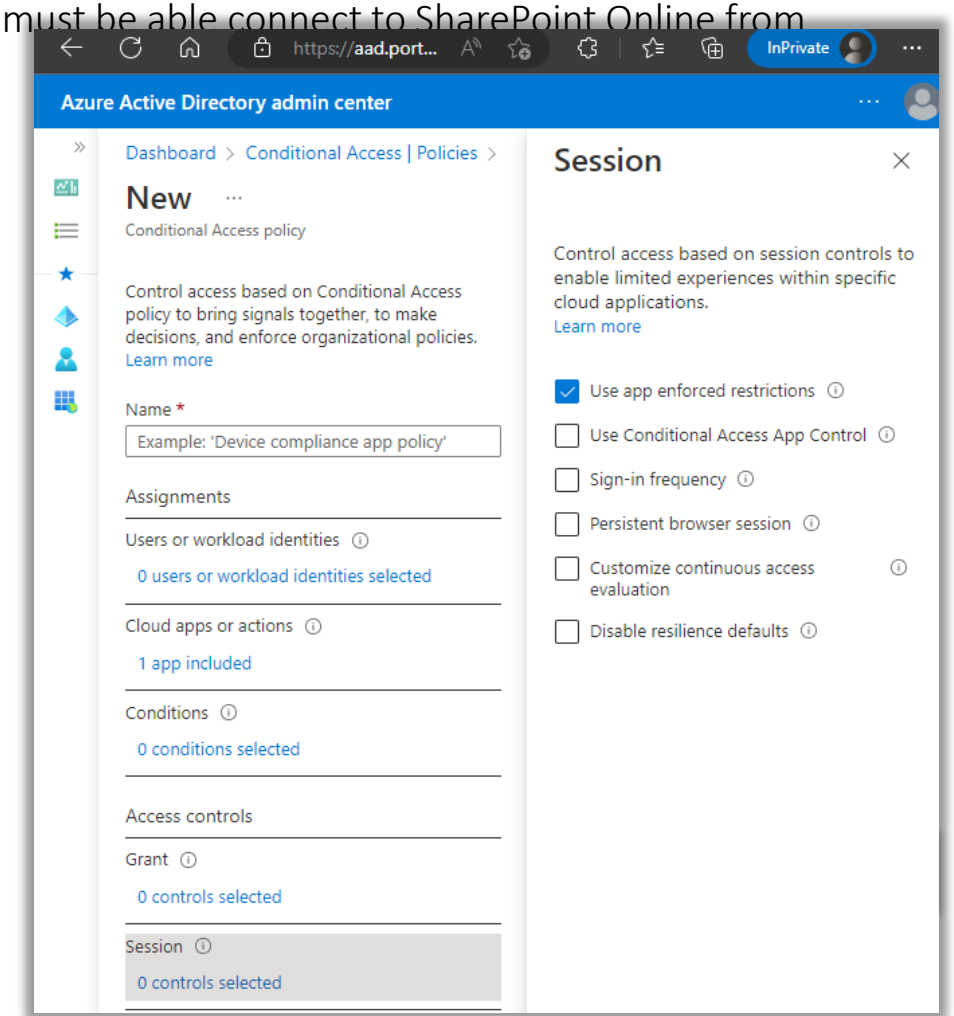
You can use Intune app protection policies independent, or even “not enrolled” of any mobile-device management (MDM) solution.

You have a Microsoft 365 tenant.
You need to implement a policy to enforce the following requirements:
☞ If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint
Online only from a web browser. The user must be prevented from downloading files or syncing files from SharePoint Online.
☞ If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files.
What should you create?

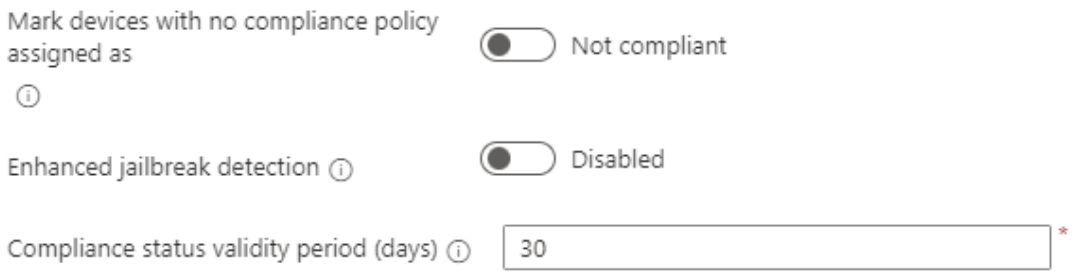
A. a conditional access policy in Azure AD that has Client apps conditions configured
B. a conditional access policy in Azure AD that has Session controls configured
C. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured
D. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured

Answer: B "Session" controls in Cond.Acc

Use App Enforce Restriction for Office 365, Sharepoint, Exchange Online



The Compliance policy settings are configured as shown:



On February 25, 2020, you create the device compliance policies:

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

On March 1. 2020, users enroll Windows 10 devices as:

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Answer: Y/Y/N

Grace period start when “enrolled” or “not compliant”

Your network contains an on-premises Active Directory domain. The domain contains a domain controller named DC1.
You have a Microsoft 365 E5 subscription.
You install the Microsoft Defender for Identity sensor on DC1.
You need to configure enhanced threat detection in Defender for Identity. The solution must ensure that the following events are collected from DC1:
☞ 4726 - User Account Deleted
☞ 4728 - Member Added to Global Security Group
☞ 4776 - Domain Controller Attempted to Validate Credentials for an Account (NTLM)
What should you do on DC1?

A. Install the Azure Monitor agent.
B. Install System Monitor (SYSMON).
C. Configure the Windows Event Collector service.
D. Configure the Advanced Audit Policy Configuration policy.

Answer: D. configure “advanced” windows event logging

Some events require configure “Advance Audit Policy” on Group Policy

You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Endpoint Manager.
You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network.
What should you do first?

A. From the Azure Active Directory admin center, create a new certificate

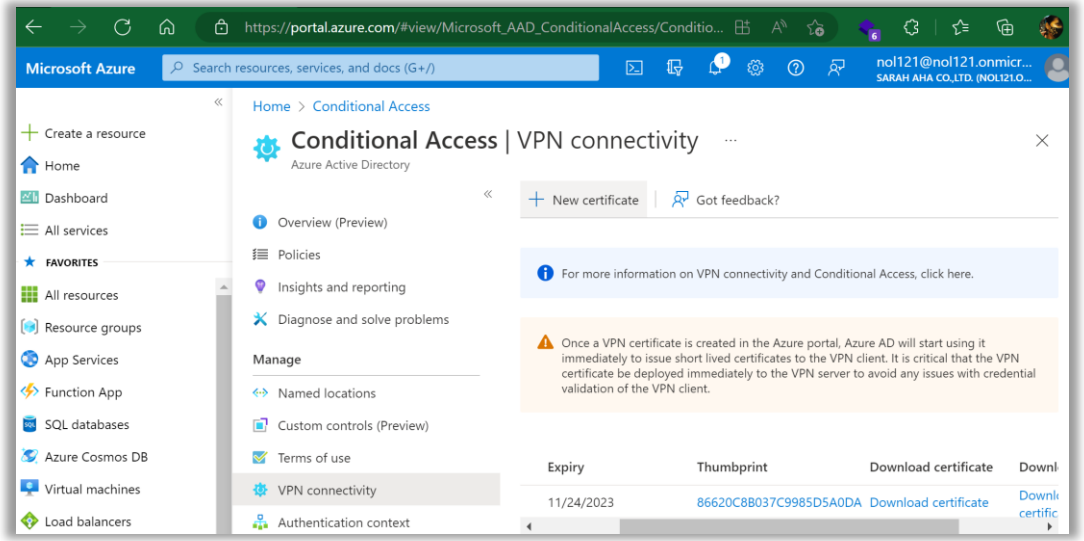
B. Enable Application Proxy in Azure AD

C. From Active Directory Administrative Center, create a Dynamic Access Control policy

D. From the Azure Active Directory admin center, configure authentication methods

Answer: A

Remote Access VPN always starts with creating VPN cert.



You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. All the devices in the tenant are managed by using Microsoft Endpoint Manager.
You purchase a cloud app named App1 that supports session controls.
You need to ensure that access to App1 can be reviewed in real time.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
From the Azure Active Directory admin center, register App1.	
From the Cloud App Security admin center, create an access policy.	
From the Cloud App Security admin center, create an app discovery policy.	
From the Endpoint Management admin center, create an app configuration policy.	
From the Azure Active Directory admin center, create a conditional access policy.	
From the Endpoint Management admin center, add App1.	

Answer: Register App, CA policy, Access Policy

Must create CA policy App Control before Access Policy

You have a Microsoft 365 Enterprise E5 subscription.
You use Microsoft Defender for Endpoint.
You plan to use Microsoft 365 Attack simulator.
What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA).
B. Configure Microsoft Defender for Office 365.
C. Create a Conditional Access App Control policy for accessing Microsoft 365.
D. Integrate Microsoft 365 Threat Intelligence and Microsoft Defender for Endpoint.

Answer: A

Enable MFA is required for admin who run attack.

You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.
Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.
You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Executive group members.
What should you do first?

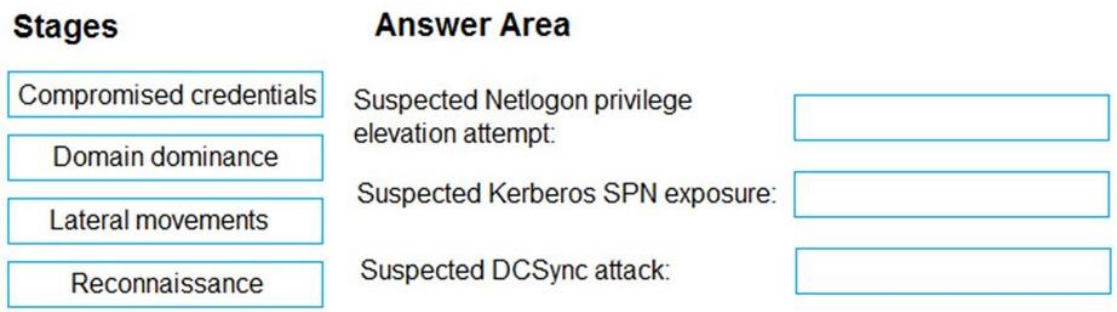
A. From the Microsoft Defender for Identity portal, configure the primary workspace settings.
B. From the Microsoft Azure portal, configure the user risk policy settings in Azure AD Identity Protection.
C. Enable MFA for the Research group members.
D. Migrate the Executive group members to Exchange Online.

Answer: D

Target mailboxes have to be on-cloud

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Identity.
You receive the following alerts:
- Suspected Netlogon privilege elevation attempt
- Suspected Kerberos SPN exposure
- Suspected DCSync attack

To which stage of the cyber-attack kill chain does each alert map?



Answer: Comp.Cred, Comp.Cred, Domain Dominance

According to MDI Attack Kill Chain

You have a Microsoft 365 E5 subscription.
Some users are required to use an authenticator app to access Microsoft SharePoint Online.
You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.
What should you do?

A. From the Azure Active Directory admin center, view the sign-ins.

B. From the Microsoft 365 Security admin center, download a report.

C. From the Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.

D. From the Azure Active Directory admin center, view the authentication methods.

Answer: A

AAD Sign-in logs always is everything for sign-in details

You have a Microsoft 365 E5 subscription.
Some users are required to use an authenticator app to access Microsoft SharePoint Online.
You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.
What should you do?

A. From the Microsoft 365 Security admin center, download a report.

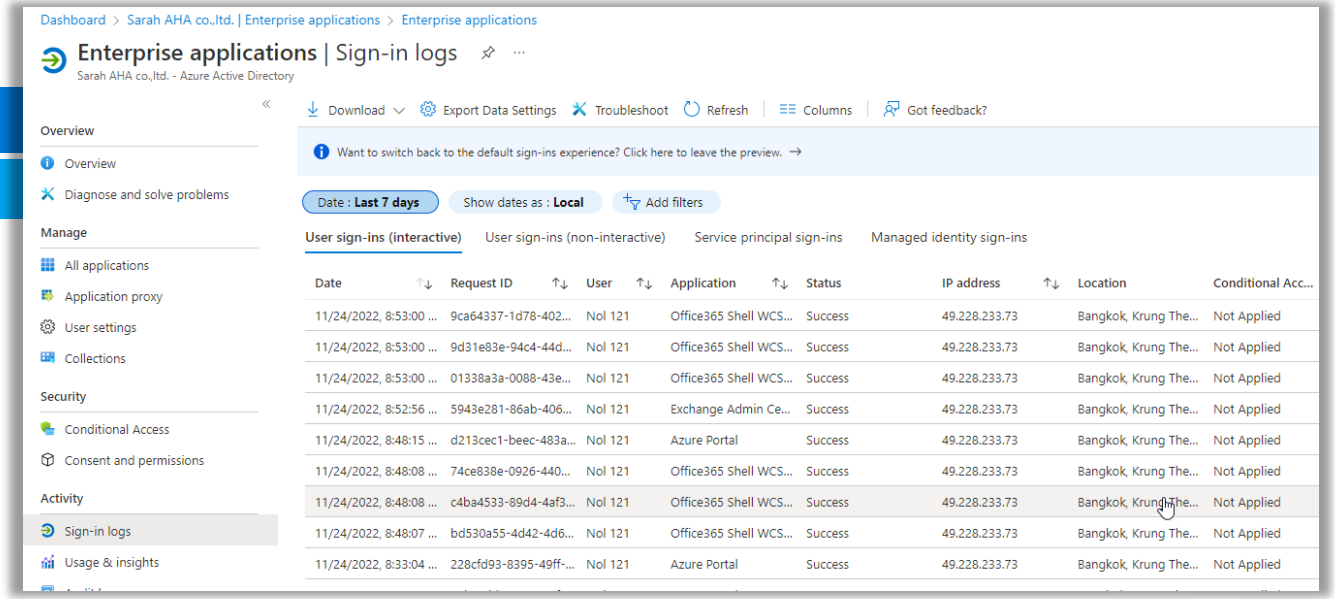
B. From Azure Log Analytics, query the logs.

C. From the Microsoft 365 Security admin center, perform an audit log search.

D. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

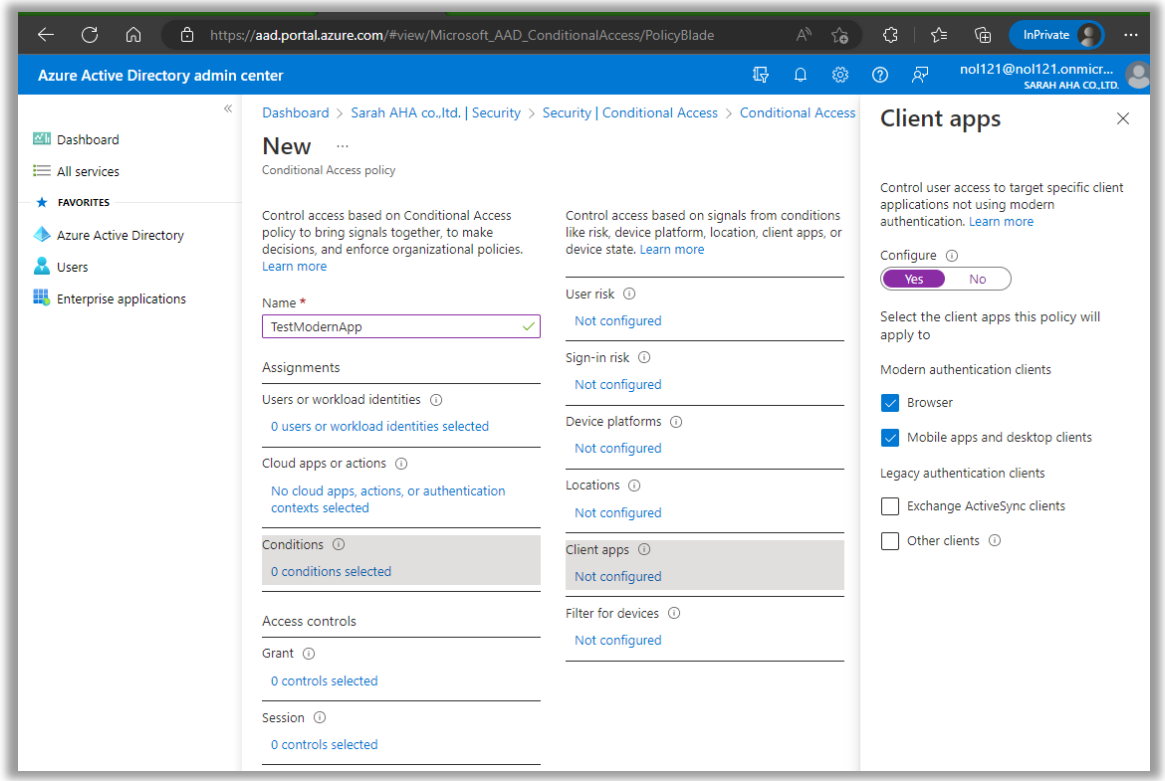
Answer: D

AAD "Sign-in" logs always is everything for sign-in details



You have a Microsoft 365 tenant that has modern authentication enabled.
You have Windows 10, MacOS, Android, and iOS devices that are managed by using Microsoft Endpoint Manager.
Some users have older email client applications that use Basic authentication to connect to Microsoft Exchange Online.
You need to implement a solution to meet the following security requirements:
☞ Allow users to connect to Exchange Online only by using email client applications that support modern authentication protocols based on OAuth 2.0.
☞ Block connections to Exchange Online by any email client applications that do NOT support modern authentication.
What should you implement?

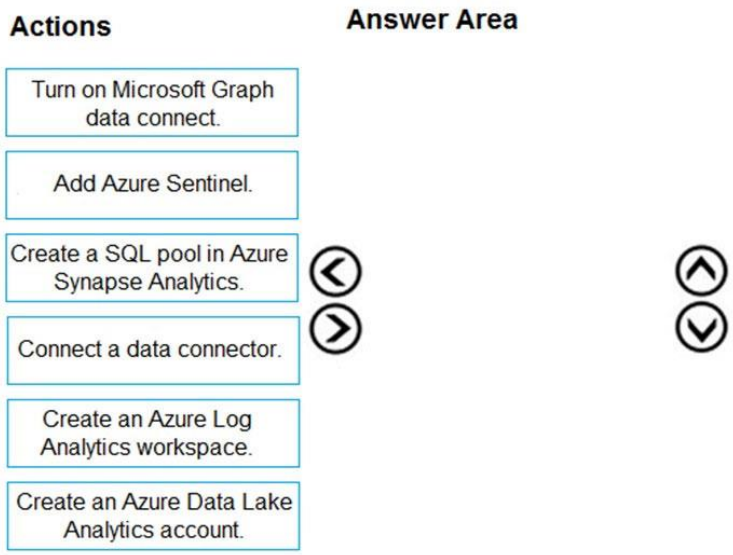
A. a conditional access policy in Azure Active Directory (Azure AD)
B. an application control profile in Microsoft Endpoint Manager
C. a compliance policy in Microsoft Endpoint Manager
D. an OAuth app policy in Microsoft Defender for Cloud Apps



Answer: A

"Client App" with "Modern Authen" config is in Condition control in CA

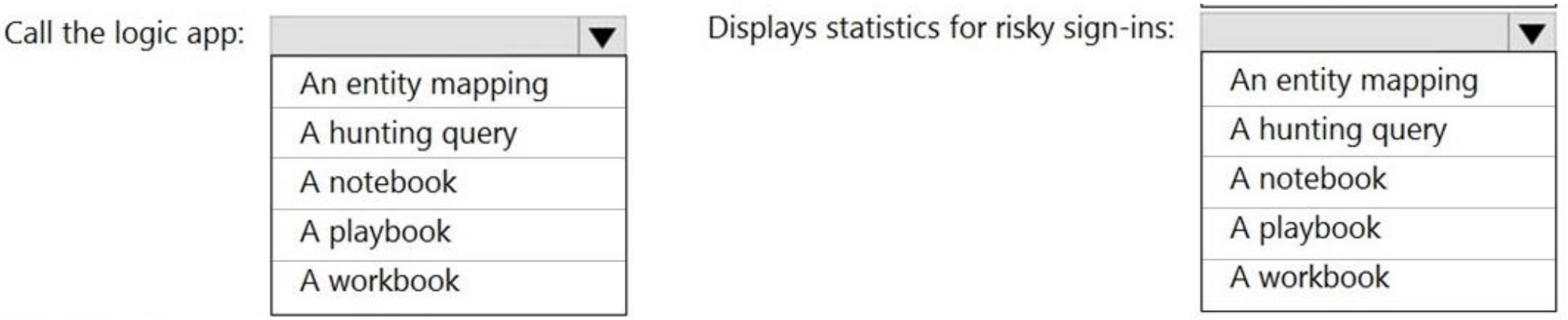
You have an Azure subscription and a Microsoft 365 subscription.
You need to perform the following actions:
☞ Deploy Microsoft Sentinel.
☞ Collect the Office 365 activity log by using Microsoft Sentinel.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer: Create Log Workspace > Add Sentinel > Connect

Sentinel engine must be on existing Workspace, then it can connect to connectors to gather data to Workspace.

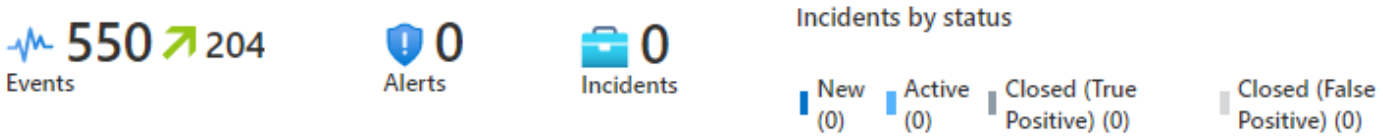
You have an Azure Sentinel workspace.
You configure a rule to generate Azure Sentinel alerts when Azure Active Directory (Azure AD) Identity Protection detects risky sign-ins.
You develop an Azure
Logic Apps solution to contact users and verify whether reported risky sign-ins are legitimate.
You need to configure the workspace to meet the following requirements:
☞ Call the Azure logic app when an alert is triggered for a risky sign-in.
☞ To the Azure Sentinel portal, add a custom dashboard that displays statistics for risky sign-ins that are detected and resolved.
What should you configure in Azure Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.



Answer: Playbook / Workbook

Logic App = Playbook, Stat = Workbook

You create an Azure Sentinel workspace.
You configure Azure Sentinel to ingest data from Azure Active Directory (Azure AD).
In the Azure Active Directory admin center, you discover Azure AD Identity Protection alerts. The Azure Sentinel workspace shows the status as shown in the following exhibit.



In Azure Log Analytics, you can see Azure AD data in the Azure Sentinel workspace.
What should you configure in Azure Sentinel to ensure that incidents are created for detected threats?

A. data connectors
B. rules
C. workbooks
D. hunting queries

Answer: B

No rule = No alert that rule detected

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a Microsoft Office 365 connector.
You need to use a Fusion rule template to detect multistage attacks in which users sign in by using compromised credentials, and then delete multiple files from
Microsoft OneDrive.
Based on the Fusion rule template, you create an active rule that has the default settings.
What should you do next?

A. Add data connectors.

B. Add a workbook.

C. Add a playbook.

D. Create a custom rule template.

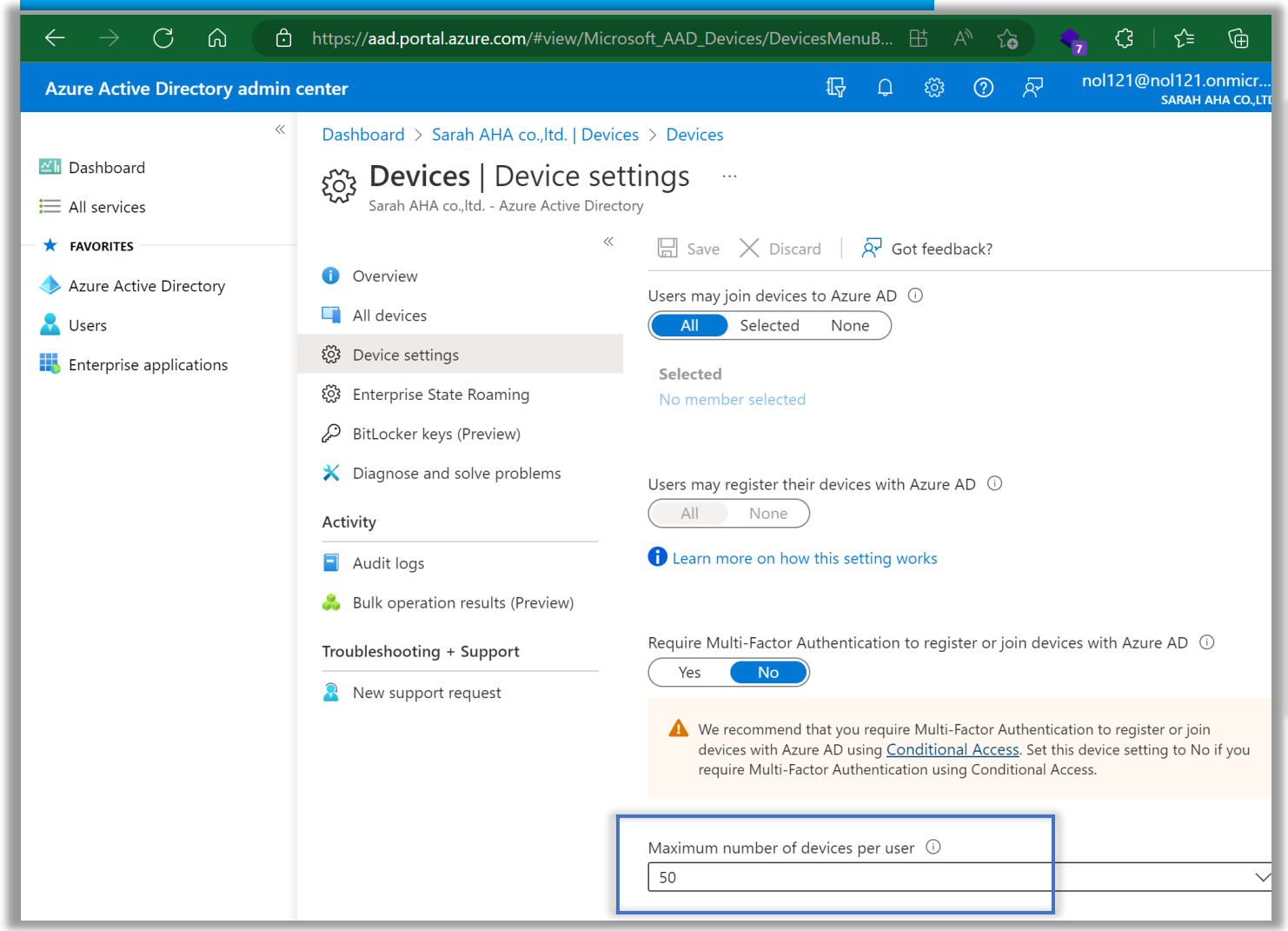
Answer: A

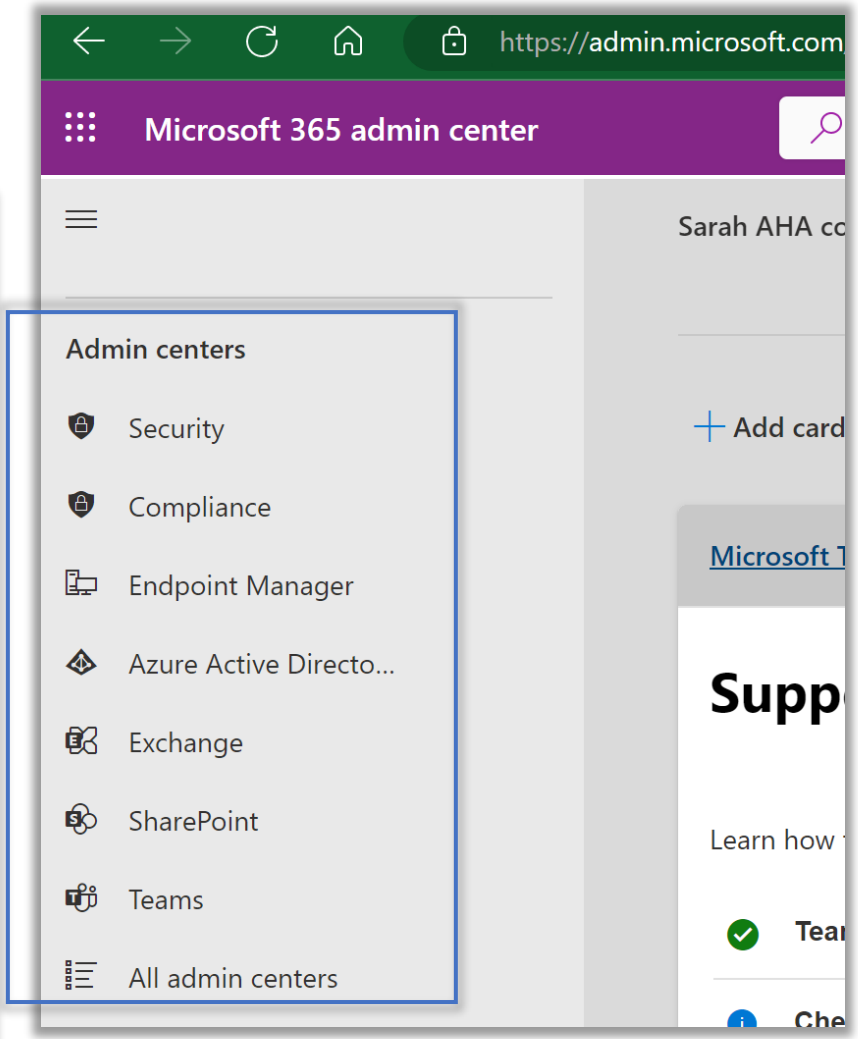
'Cause only these two connectors are not enough for fusion rules to detect efficiently

You need to ensure that each user can join up to five devices to Azure Active Directory (Azure AD).
To complete this task, sign-in to the Microsoft Office 365 admin center.

Answer:

Go to AAD > Devices > Device Settings

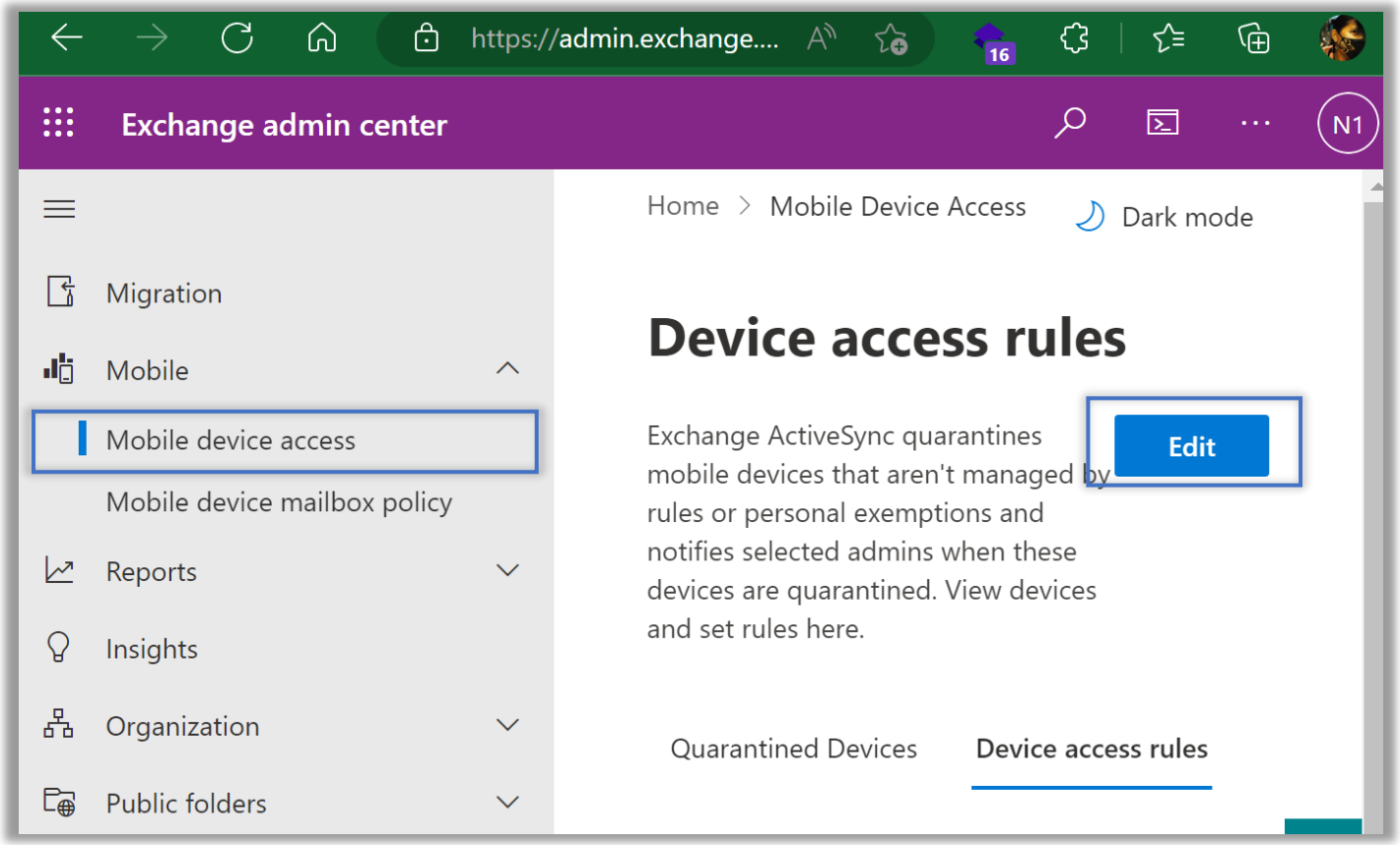


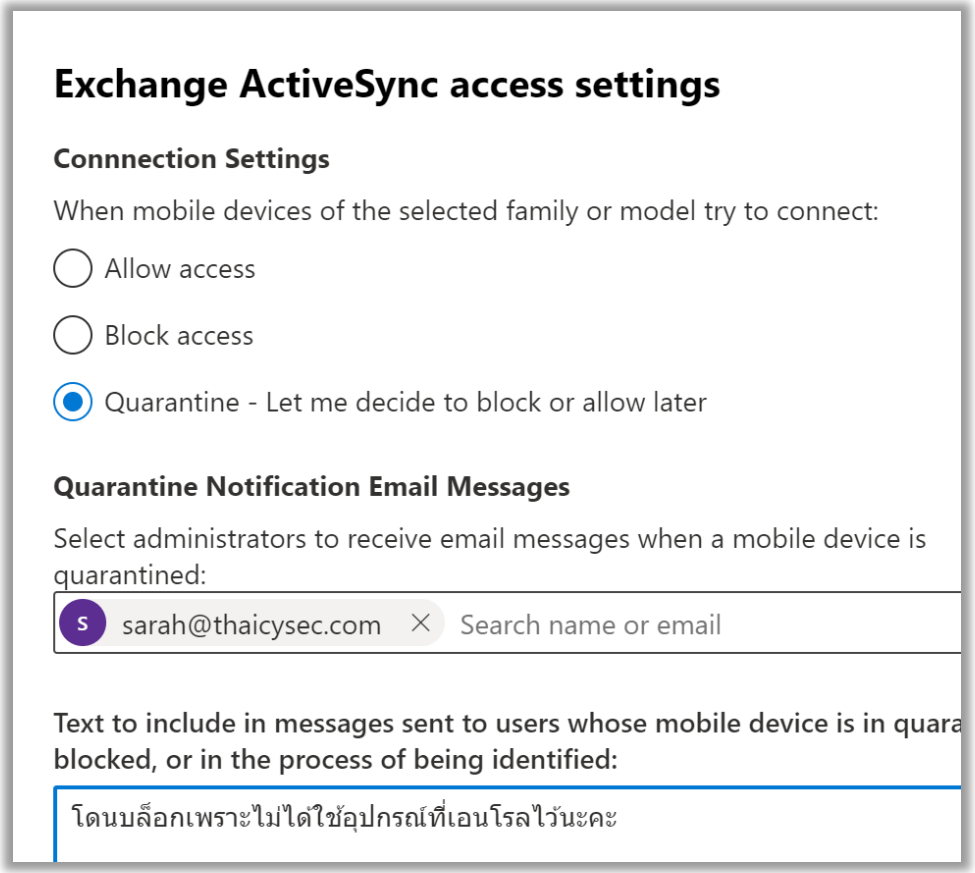


You need to ensure that unmanaged mobile devices are quarantined when the devices attempt to connect to Exchange Online.
To complete this task, sign in to the Microsoft 365 portal.

Answer:

Go to admin.exchange.microsoft.com > Mobile > Mobile Device Access > Edit

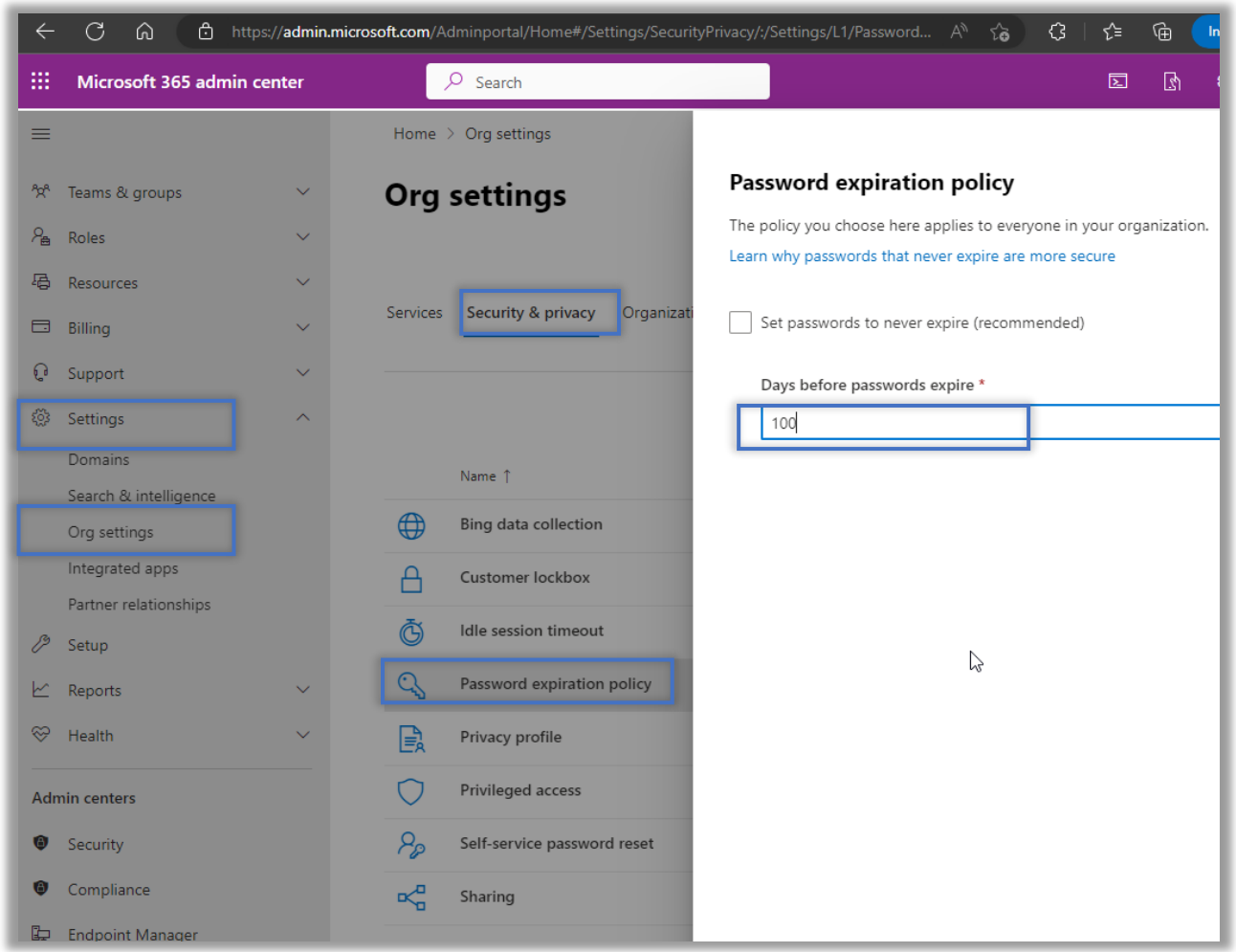




You need to ensure that all users must change their password every 100 days.
To complete this task, sign in to the Microsoft 365 portal.

Answer:

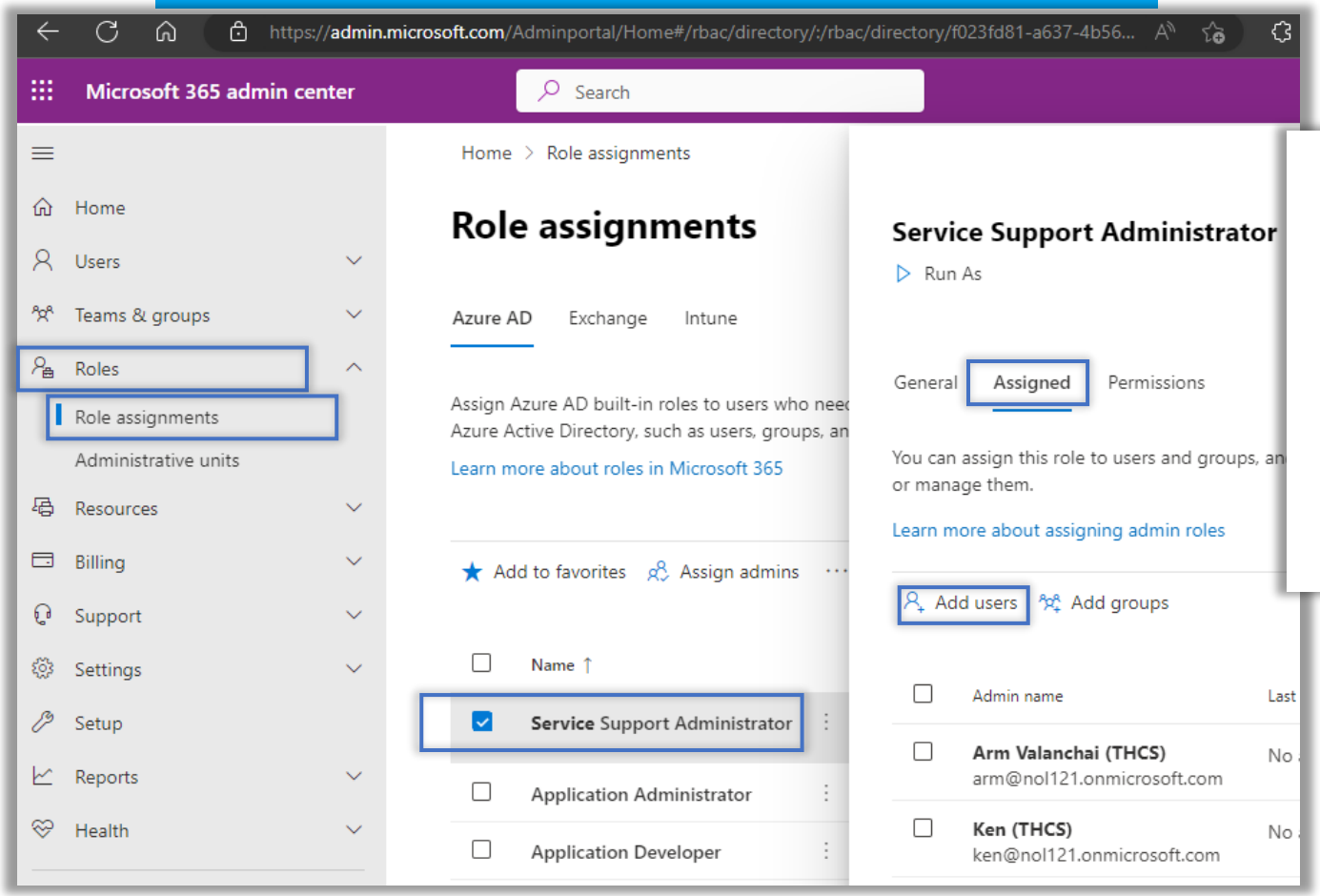
Go to Settings > Org Settings > Security & privacy > Password expiration policy

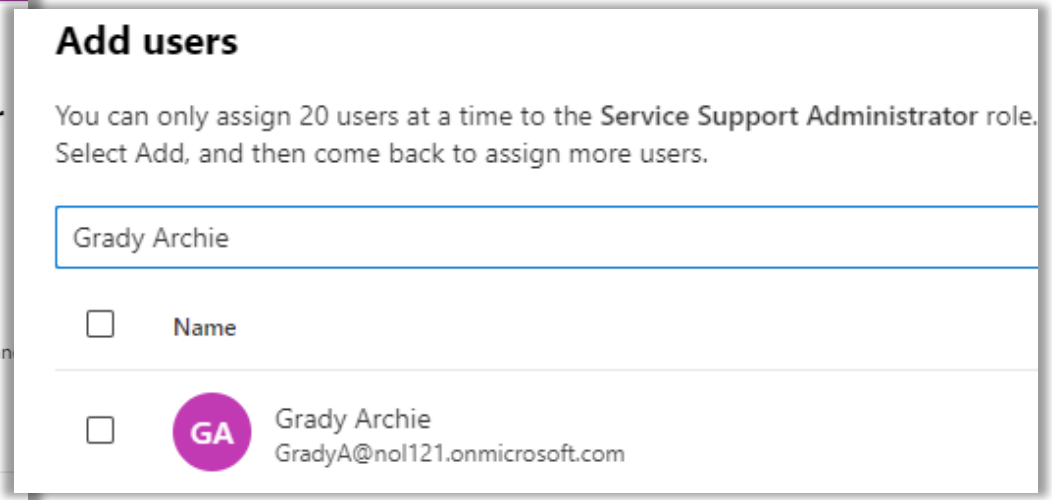


You need to ensure that a user named Grady Archie can monitor the service health of your Microsoft 365 tenant. The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft 365 portal.

Answer:

Go to Roles > Role Assignment > search for “Service Support Admin” > Assigned > Add User





SC-900

SECURITY
COMPLIANCE
IDENTITY

With On-Prim VM/AWS etc.
By Azure Arc

Defender for Cloud (s) = Security Posture

Security Center

Cloud Security
Posture Management (CSPM)

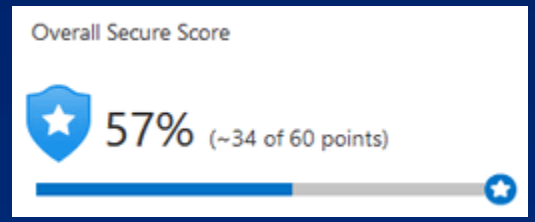
- **Free! across** all subscriptions
- Secure Score
  - **Security Baseline**
  - Guidance to **Azure Security Benchmark (ASB)**

+ Azure Defender

Cloud Workload Protection (CWP)

- **Pay** per use
- For each resource
  - Servers
  - **Storage**
  - SQL
  - Container
  - App Service
  - Key Vault, etc.

How to increase score: update system / MFA / etc.



THCS

SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

portal.azure.com/#view/Microsoft_Azure_Security/SecurityMenuBlade/~/23

Microsoft Azure | Search resources, services, and docs (G+/) | nol121@hotmail.com DEFAULT DIRECTORY

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Security posture

Showing 2 subscriptions

Search (Ctrl+/)

General
- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security
- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager

Management
- Environment settings

Secure score over time | Governance report (preview) | Guides & Feedback

Azure environment

Azure | AWS | GCP

Secure score

Environment

0 Management groups
1 Subscriptions
2/4 Unhealthy resources
17 Recommendations

Governance (preview)

No data to display

Environment | Owner (preview)

Search by name | Environment == Azure | Group by environment

Name	Secure score	Unhealthy resources	Recommendations
Visual Studio Enterprise Subscription Azure subscription	8%	2 of 2	View recommendations >

ommendations

fresh | Download CSV report | Open query | Governance report (preview) | Guides & Feedback

e score recommendations | All recommendations

ure score | Active items | Resource health | Governan

8% | Controls 10/12 | Recommendations 7/17

Unhealthy (2) | Healthy (0) | Not applicable (2)

Overdue recommendations 0/0
Unassigned recommendations 7/7

rch recommendations | Environment == Azure | Add filter | More (5) | Show my items only: Off

me	Max score	Current score	Potential score increase	Status	Unhealthy resources
able MFA	10	0.00	+ 20%	Unassigned	1 of 1 resources
cure management ports	8	0.00	+ 16%	Unassigned	1 of 1 resources
ply system updates	6	0.00	+ 12%	Unassigned	1 of 1 resources
mediate vulnerabilities	6	0.00	+ 12%	Unassigned	1 of 1 resources
anage access and permissions	4	4.00		Completed	0 of 1 resources

THCS

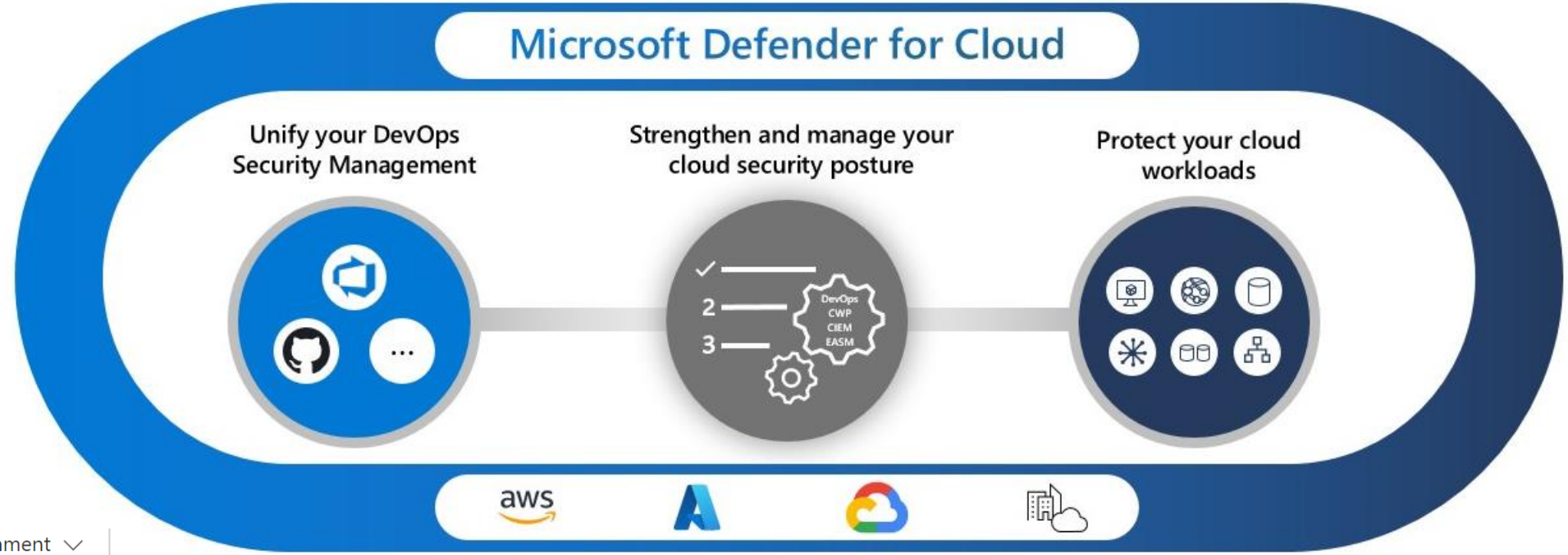
Azure Security Technologies

Defender for Cloud (MDC)

Continuously Assess
Know your security posture. Identify and track vulnerabilities.

Secure
Harden resources and services with Azure Security Benchmark.

Defend
Detect and resolve threats to resources, workloads, and services.



Add environment

- Amazon Web Services
- Google Cloud Platform
- GitHub (preview)
- Azure DevOps (preview)

DevSecOps

Code Pipeline Sec

CSPM

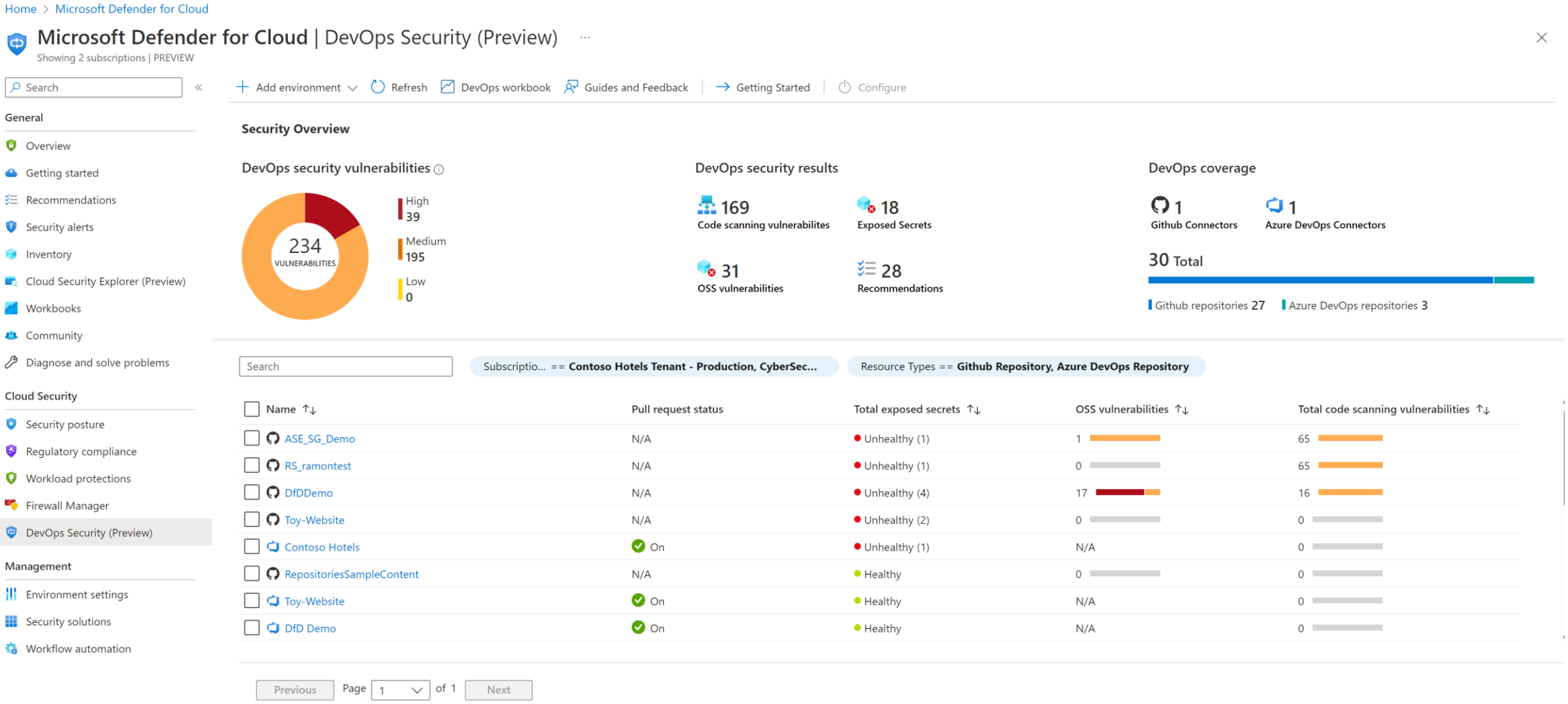
Foundation (FREE)

Defender (Premium)

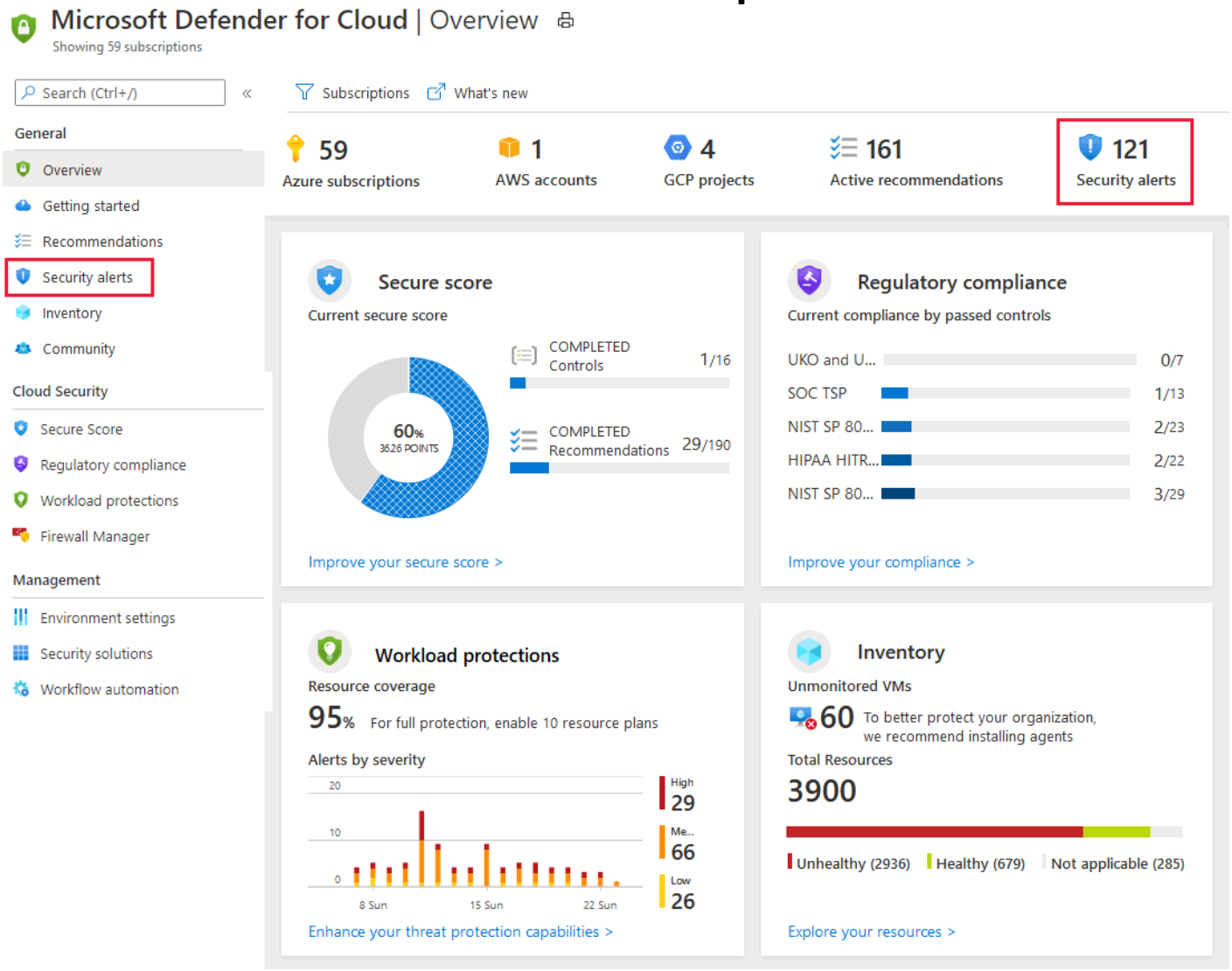
CWPP

ITGeist

DevOps environments in Defender for Cloud



Cloud workload protection



Evaluated categories

Access

Compute

SQL server

IoT

Network

App Services

Containers

Free foundational CSPM

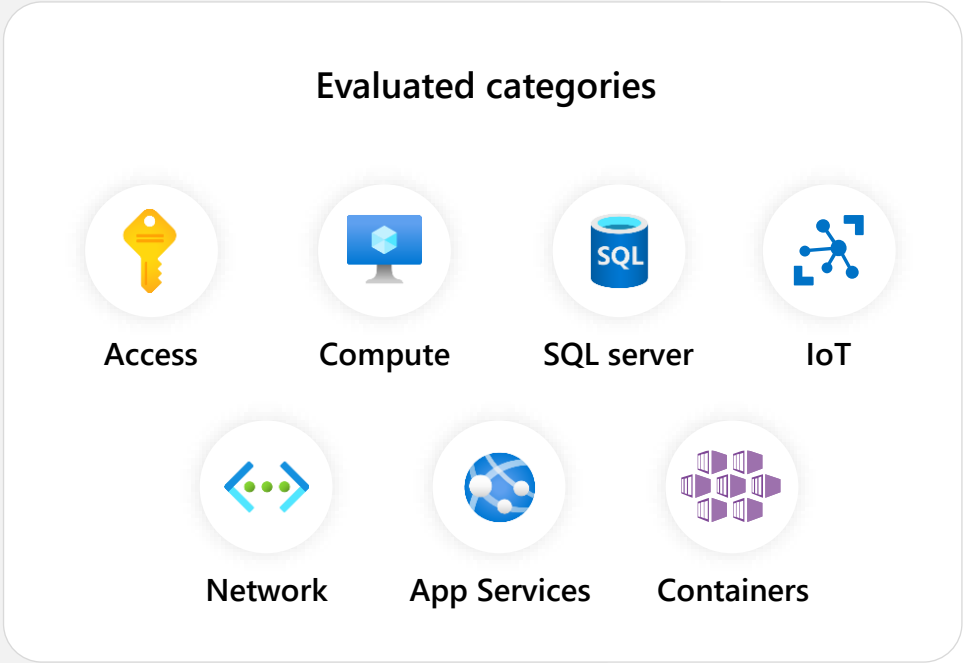
Hardening guidance and Secure Score

- Strengthen security posture across all critical cloud resources including network, access, compute, databases, your service layer, and more
- 450+ out-of-the-box recommendations
- Create custom recommendations to meet organizational requirements

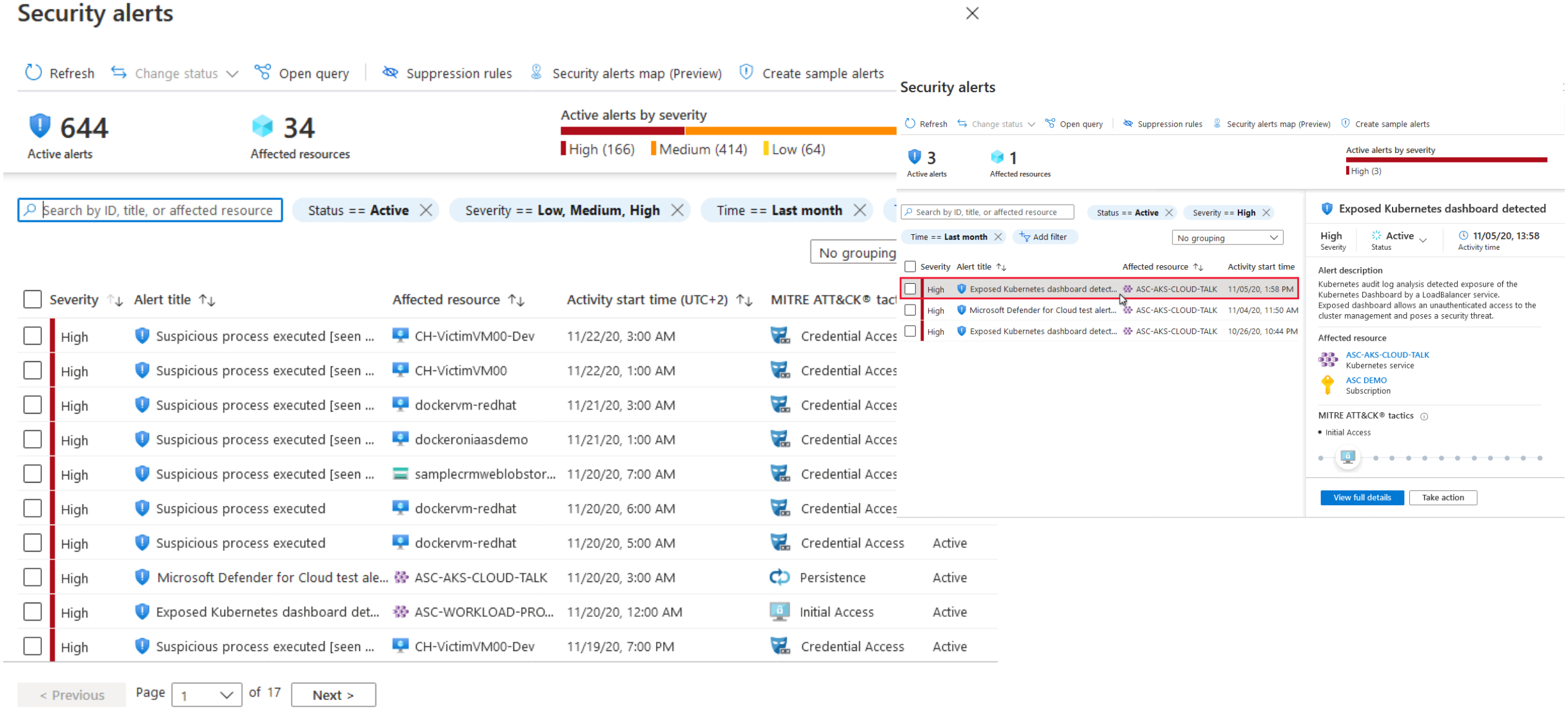
Multicloud security benchmark for security compliance

- Manage cloud security compliance with continuous assessment of cloud resources across Amazon Web Services, Microsoft Azure, and Google Cloud Platform in a single, integrated dashboard
- Use industry standards, regulatory compliance frameworks, and cloud-specific benchmarks to implement best practices (CIS, PCI, NIST, SOC, ISO HIPAA, etc.)
- Create custom recommendations to meet unique organizational needs

Continuous assessment and prioritized security recommendations with secure score, and verify compliance with regulatory standards



Manage and Assign Security Alerts



Azure
Security
Technologies

Defender
for Cloud (MDC)

Cloud Security Posture Management (CPSM)

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

Visual Studio Enterprise Subscription

Search

Settings

- Defender plans
- Email notifications
- Workflow automation
- Integrations
- Continuous export

Save | Settings & monitoring

Select Defender plan | Enable all

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >			On
Defender CSPM	Free (during preview) Details >	N/A		

Use Azure Policy (Audit)

- Continuous assessment of the security configuration of your cloud resources
- Security recommendations to fix misconfigurations and weaknesses
- Secure score summarizing your current security situation

Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.

Pricing: Free (during preview)

- Identity and network exposure detection
- Attack path analysis
- Cloud security explorer for risk hunting
- Agentless vulnerability scanning
- Governance rules to drive timely remediation and accountability
- Regulatory compliance and industry best practices

Azure
Security
Technologies

Defender
for Cloud (MDC)

+

Azure
Policy

Cloud Security Posture Management (CPSM)

Policy | Compliance

Search

Overview
Getting started
Compliance
Remediation
Events

Authoring

Definitions
Assignments
Exemptions

Assign policy | Assign initiative | Refresh

2 selected | All definition types | All compliance states | Filter by name or ID...

Overall resource compliance
20%
1 out of 5

Resources by compliance state
5
1 - Compliant
0 - Exempt
4 - Non-compliant

Non-compliant initiatives
2
out of 6

Non-compliant policies
16
out of 439

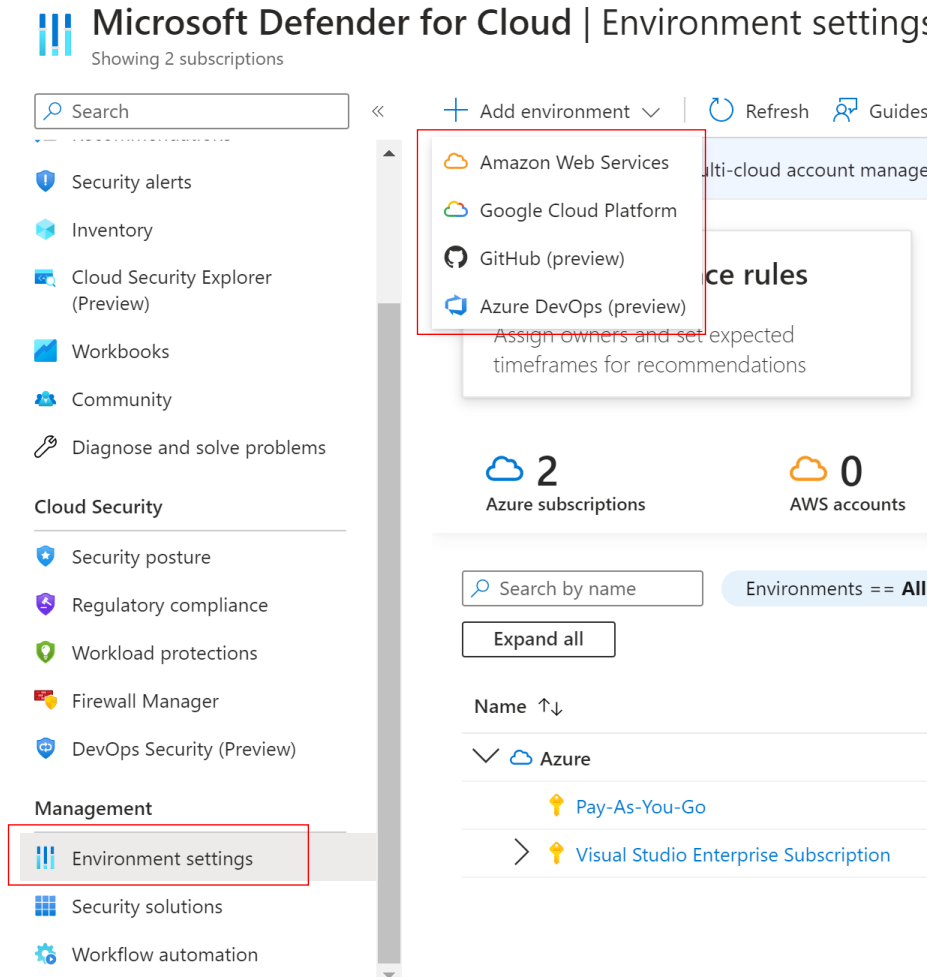
Name	Scope	Compliance state	Resource compli...	Non-Compliant Res...	Non-compliant poli...
ASC Default (subscriptio...	Visual Studio Enterpr...	Non-compliant	25% (1 out of 4)	3	10
ASC Default (subscriptio...	Pay-As-You-Go	Non-compliant	0% (0 out of 1)	1	5
Configure Azure Activity ...	Visual Studio Enterpr...	Non-compliant	0% (0 out of 1)	1	1
ASC DataProtection (sub...	Visual Studio Enterpr...	Compliant	100% (0 out of 0)	0	0
Defender for Containers ...	Pay-As-You-Go	Compliant	100% (0 out of 0)	0	0
Defender for Containers ...	Visual Studio Enterpr...	Compliant	100% (0 out of 0)	0	0
Defender for Containers ...	Pay-As-You-Go	Compliant	100% (0 out of 0)	0	0

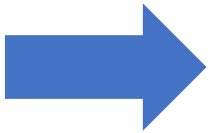
ITGeist

Azure
Security
Technologies

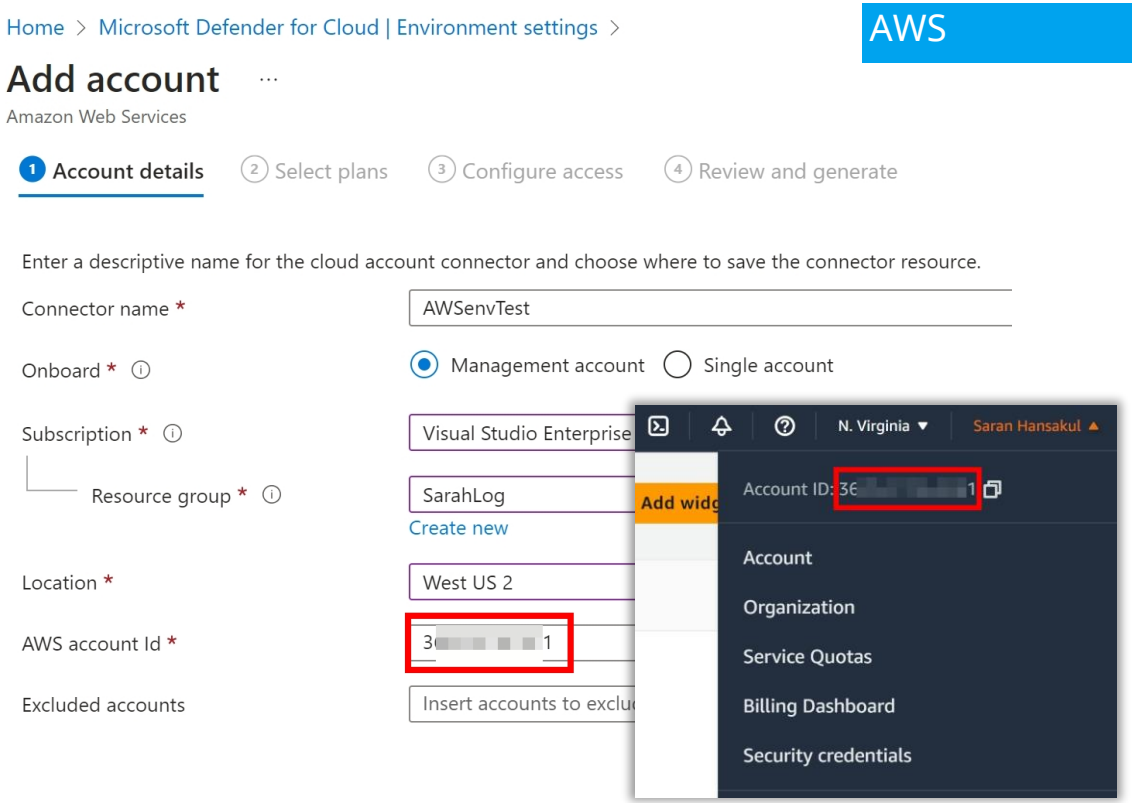
Defender
for Cloud (MDC)

Add Multicloud Environment with “Native” (agentless) Connector





AWS



ITGeist

Azure
Security
Technologies

Defender
for Cloud (MDC)

Add Multicloud Environment with “Native” (agentless) Connector

AWS

Home > Microsoft Defender for Cloud | Environment settings >

Add account

Amazon Web Services

Account details | 2 Select plans | 3 Configure access | 4 Review and generate

Agentless scanning (preview)

On

Scan your EC2 instances for installed software and vulnerabilities without requiring agents, network connectivity or impacting machine performance. Results are powered by Microsoft Defender Vulnerability Management engine. Learn more

Select plans

To check the status of AWS resources, we'll use read-only API calls. If you're logging read events in AWS CloudTrail, and if you're exporting data to SIEM, ingestion costs might increase Learn more

Plan	Pricing	Monitoring coverage
Foundational CSPM	Free Details >	Permissions: Read (SecurityAudit)
Defender CSPM	Free (during preview) Details >	Full Settings >
Servers	**Plan 2** ($15/Server/Month) Select tier >	Partial Settings >
Databases	15$/Server/Month Details >	
Containers	Free (during preview) Details >	

Azure Arc agent

On

Connects your servers to the Azure platform. When you enable the Arc agent, it’ll be installed on new and existing instances with Systems Manager (SSM) agent enabled.

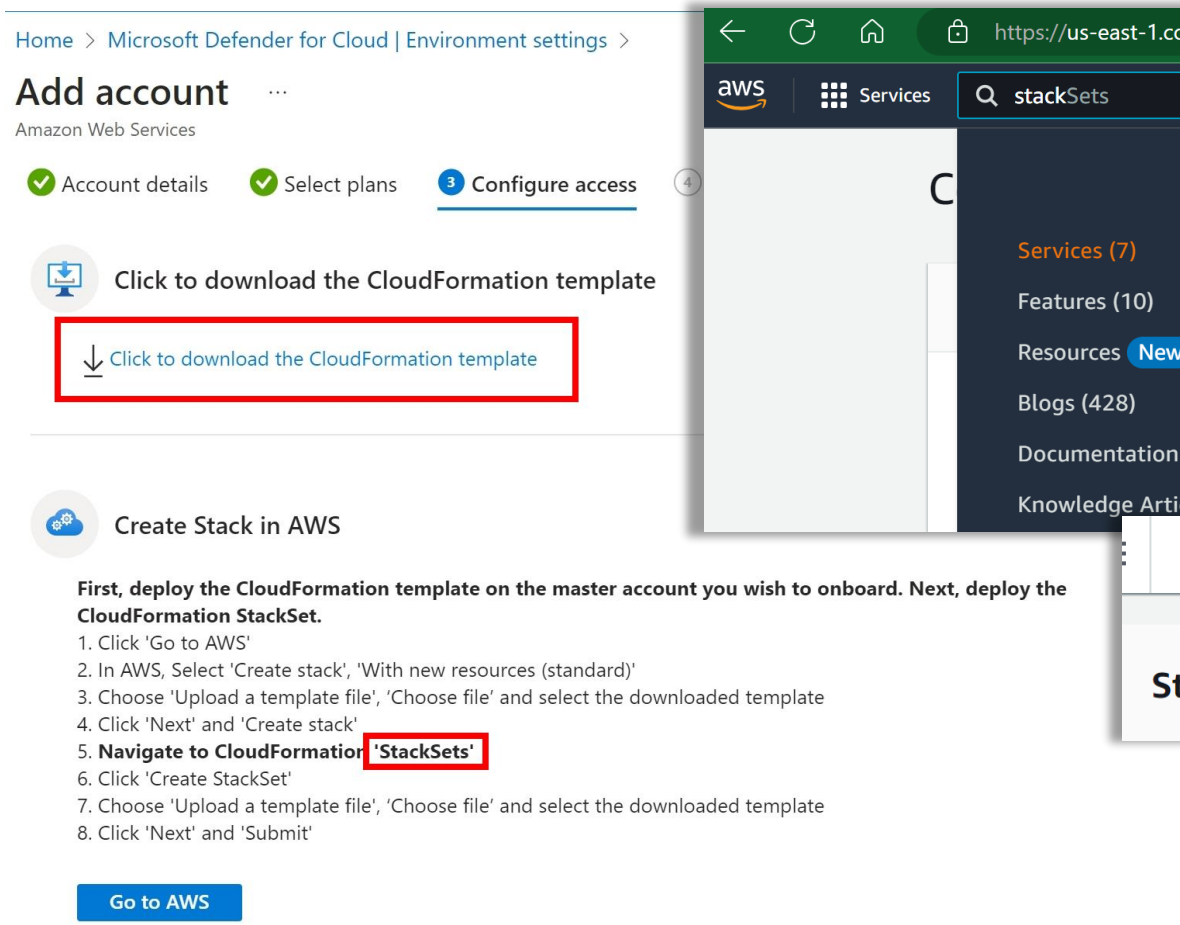
Note: Arc auto-provisioning registers your account to the Azure resource providers “Microsoft.HybridCompute” and “Microsoft.GuestConfiguration”.

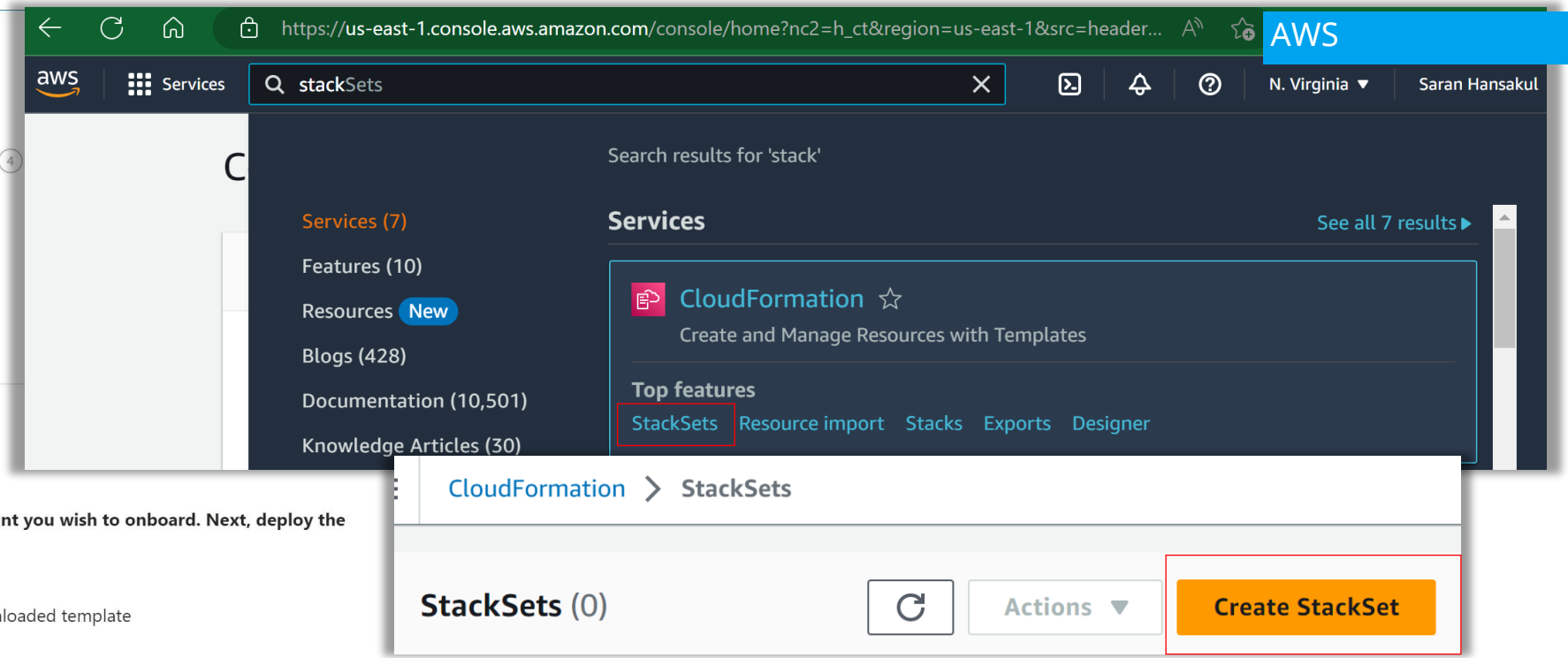
ITGeist

Azure
Security
Technologies

Defender
for Cloud (MDC)

Add Multicloud Environment with “Native” (agentless) Connector





ITGeist

Azure Security Technologies

Defender for Cloud (MDC)

Add Multicloud Environment with “Native” (agentless) Connector

AWS

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

- (•) Template is ready
- ( ) Use a sample template

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

- ( ) Amazon S3 URL
- (•) Upload a template file
- ( ) From stack ID

Upload a template file

[Choose file] *CloudFormation.template*

JSON or YAML formatted file

S3 URL: https://s3.us-east-1.amazonaws.com/cf-templates-d1zh5rwmjgo9-us-east-1/2023-03-11T003336.901Zgb4-CloudFormation.template [View in Designer]

Cancel **Next**

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more

☑ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

Cancel Previous **Submit**

ITGeist mvpskill change the world by contributions M↓ THCS Spark Tech Thailand

Azure Security Technologies

Defender for Cloud (MDC)

Add Multicloud Environment with “Native” (agentless) Connector

GCP

Home > Microsoft Defender for Cloud | Environment settings >

Create GCP connector

Google cloud

Organization details | Select plans | 3 Configure access | 4 Review and generate

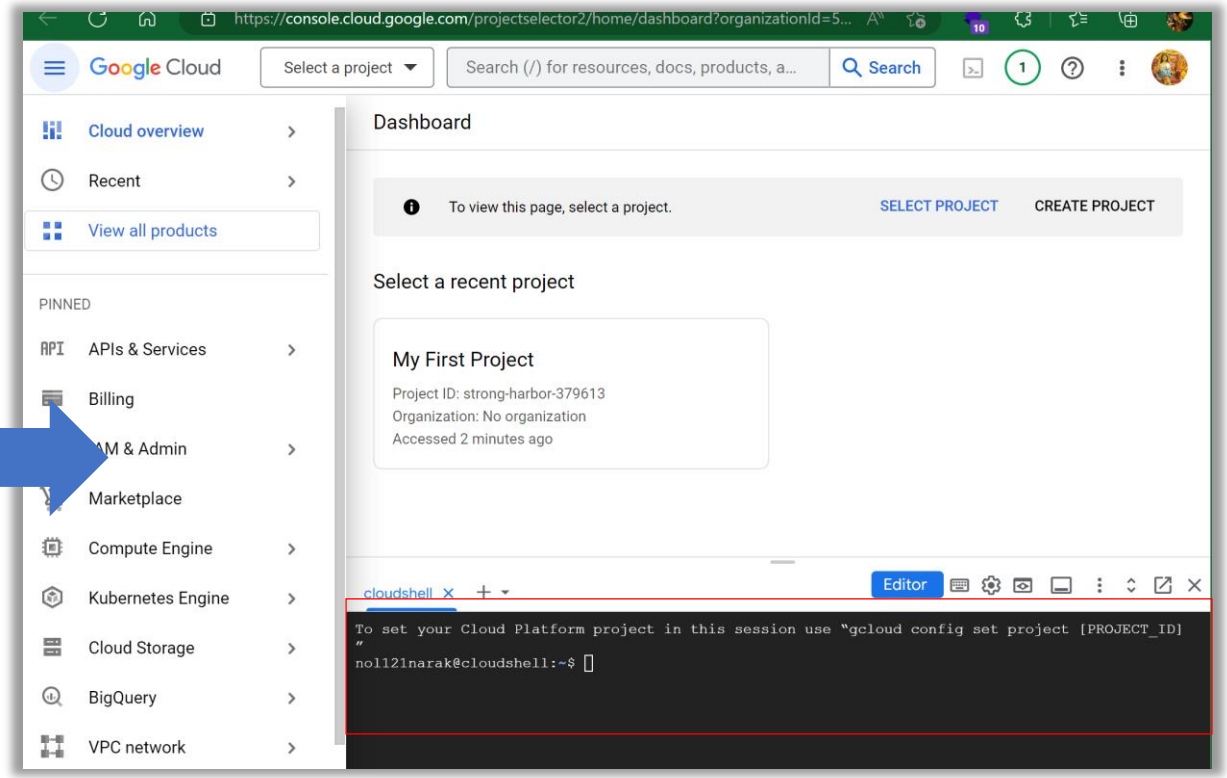
Copy script to GCP Cloud Shell

A Cloud Shell template to configure access on GCP side has been created according to the plans selected in the previous tab.
By running the template, we'll create a management project and organization custom role to onboard the organization and e

```
# Setting The Environment Variables
MgmtProjectId="mdc-mgmt-proj-567890123456"
AutoProvisionerServiceAccountName="mdc-onboarding-sa"
CspmServiceAccountName="microsoft-defender-cspm"
OrganizationID="567890123456"
IAMRoleID="MDCCustomRole"
CspmCustomRoleID="MDCCspmCustomRole"
WorkloadIdentityPoolName="microsoft defender for cloud"
WorkloadIdentityPoolId="31dd4bda873047a38d1c5af9179cfa52"
# Create a custom role for MDC CSPM
gcloud iam roles create ${CspmCustomRoleID} --organization=${OrganizationID} --title=${CspmCustomRoleID} --
description="Microsoft Defender for cloud CSPM custom role" \
```

Copy

GCP Cloud Shell >



ITGeist

Azure
Security
Technologies

Defender
for Cloud (MDC)

Defender
EASM

Similar to VA tool

*Price per Asset

SarahEASM ☆ ···
Microsoft Defender EASM

Search

Overview

General

Inventory

Dashboards

Attack Surface Summary

Security Posture

GDPR Compliance

OWASP Top 10

Manage

Discovery

Labels (Preview)

Billable Assets (Preview)

Support + troubleshooting

New Support Request

Custom Attack Surface

Tell us what you know

Confirmation

Seed → Discovery → Inventory → Inspection → Asset details → Analysis → Reports

Tell us what you know

Tip: We recommend starting with a single domain for your
be entered for more discoveries.

Organization information

Seed Organization names for asset discovery ⓘ

ThaiCySec

Example: Microsoft | One per

“External (=internet exposed)” (view of) Attack Surface Mgmt

Start scanning with custom seeds:

Seeds

- Domains
- IP Blocks
- Hosts
- Email Contacts
- ASNs
- Whois Organizations

Seeds

Domains (1)

Seed Domains for

thaicysec.com

Example: office.com | On

IP Blocks

Confirmation

ⓘ Custom Attack Surfaces take 24-48 hours to build as we scan our security gra

Seeds

Type	Seed Name
Org Name	ThaiCySec
Domain	thaicysec.com

Back | Confirm

Azure
Security
Technologies

Defender
for Cloud (MDC)

Defender
EASM

Attack Surface Summary

Domains	Hosts	Pages	SSL Certs	ASNs	IP Blocks	IP Addresses	Contacts
449.9K	2.8M	894.6K	2.6K	68	720	2.4M	1.2K

Attack Surface Priorities

8
High Severity Observations

4
Medium Severity Observations

2
Low Severity Observations

Found from 2 of 11 Insights

Top Observations

Deprecated Tech - Nginx	2
Deprecated Tech - WordPress	0
Affected CVSS Page	0
Deprecated Tech - Microsoft IIS	0
Self Signed Certificates	0

All 11 Insights

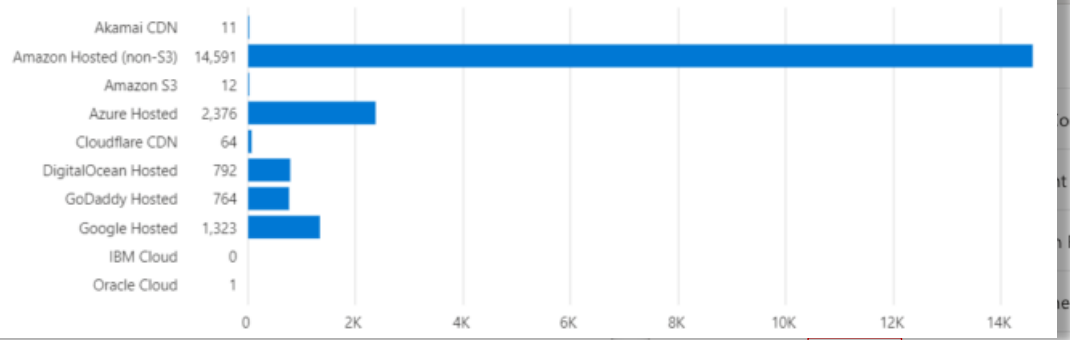
CVE-2020-12720 - vBulletin SQL Injection Leads to Remote Cod... 0

CVE-2020-1147 [Potential] .NET Deserialization Vulnerability Lea... 0

All 77 Insights

Securing the Cloud

Most organizations adopt the cloud gradually, creating a hybrid environment that can be difficult to manage. Defender EASM is able to understand the usage of specific cloud technologies and providers in order to give you insight into your externally facing Attack Surface. Dashboards, Reports and Insights can all be used to inform your cloud adoption program and ensure it's compliant with your organization's process.



Potential = not sure (e.g. cannot detect version)

ITGeist

SC-900

SECURITY
COMPLIANCE
IDENTITY

Data Connector

Sentinel = SIEM + SOAR

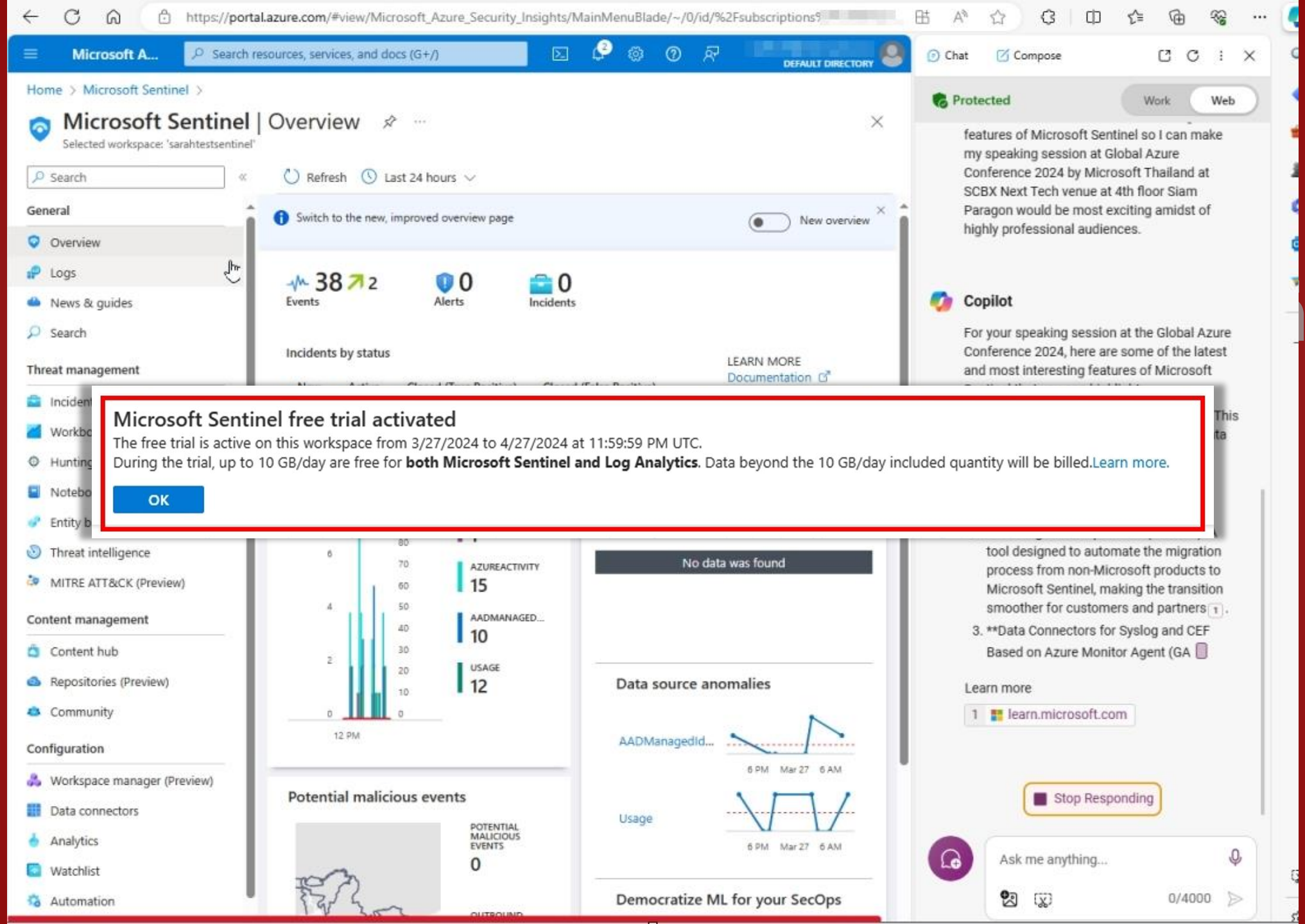
Sec.Info+Event Mgmt

- **Workbook** > Visualize Data
  - Kusto Query

Sec.Orchestrate+AutoRespond

- Automation > **Playbook** > Logic App
- Sync status with **Microsoft Defender (XDR)**
  - Defender for Cloud
  - 365 Defender

THCS


Microsoft A...
Search resources, services, and docs (G+/)
DEFAULT DIRECTORY
Home > Microsoft Sentinel >
Microsoft Sentinel | Overview
Selected workspace: 'sarahtestsentinel'
Search
Refresh
Last 24 hours
General
Overview
Logs
News & guides
Search
Threat management
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Watchlist
Automation
Switch to the new, improved overview page
New overview
38 2
Events
0
Alerts
0
Incidents
Incidents by status
LEARN MORE
Documentation
Microsoft Sentinel free trial activated
The free trial is active on this workspace from 3/27/2024 to 4/27/2024 at 11:59:59 PM UTC.
During the trial, up to 10 GB/day are free for both Microsoft Sentinel and Log Analytics. Data beyond the 10 GB/day included quantity will be billed.Learn more.
OK
AZUREACTIVITY
15
AADMANAGED...
10
USAGE
12
12 PM
No data was found
Data source anomalies
AADManagedId...
Usage
6 PM
Mar 27
6 AM
Potential malicious events
POTENTIAL MALICIOUS EVENTS
0
Democratize ML for your SecOps
Chat
Compose
Protected
Work
Web
features of Microsoft Sentinel so I can make my speaking session at Global Azure Conference 2024 by Microsoft Thailand at SCBX Next Tech venue at 4th floor Siam Paragon would be most exciting amidst of highly professional audiences.
Copilot
For your speaking session at the Global Azure Conference 2024, here are some of the latest and most interesting features of Microsoft
tool designed to automate the migration process from non-Microsoft products to Microsoft Sentinel, making the transition smoother for customers and partners 1.
3. **Data Connectors for Syslog and CEF Based on Azure Monitor Agent (GA
Learn more
1 learn.microsoft.com
Stop Responding
Ask me anything...
0/4000

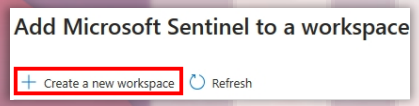
Simplified Microsoft Sentinel

ENGINE

- **Connect** Services / APIs
- Process w/ Preset **Templates**

LOG WORKSPACE

- Retain Log etc.



RESOURCE GROUP

- Set RBAC roles
  - Sen Reader
  - Sen Responder
  - Sen Contributor
  - Playbook Op
  - Auto Contributor
  - Template Spec Contributor

Microsoft Security Community Thailand

Simplified Microsoft Sentinel

ENGINE

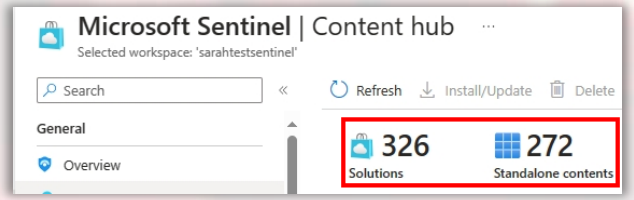
w/ Template Spec Contributor
In Subscription RBAC level

Get "**Content**"

OOTB

CONTENT HUB

- Solution
- Standalone



Custom

REPOSITORIES

- GitHub
- Azure DevOps

Microsoft Security Community Thailand

Cloud-native Security Operations with Microsoft Sentinel

Content is Connector + TEMPLATES

w/ Template Spec Contributor

Get "**Content**"

OOTB

CONTENT HUB

Standalone

MUST "SAVE" / "CREATE" TO USE

Custom

REPOSITORIES

GitHub

Azure DevOps

Microsoft Sentinel | Content hub

Selected workspace: 'sarahtestsentinel'

Standalone

Search

General
- Overview
- Logs
- News & guides
- Search

Threat management
- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management
- Content hub
- Repositories (Preview)
- Community

Configuration

Refresh | Install/Update | Delete | Guides & Feedback

326 Solutions | 272 Standalone contents | 2 Installed | 1 Updates

Search...

Status : All | Content type : All | Support : All | Provider : All | Category : All

Content title	Content source	Provider
SOC Handbook FEATURED	Solution	Community
Threat Int... FEATURED PREVIEW	Solution	Microsoft
UEBA Essentials FEATURED	Solution	Microsoft
VirusTotal FEATURED	Solution	VirusTotal
Workspace Usage Rep... FEATURED	Standalone	
42Crunch Microsoft Sentinel Connec...	Solution	42Crunch
A client made a web request to a po...	Standalone	
A host is potentially running a crypt...	Standalone	

Workspace Usage Report

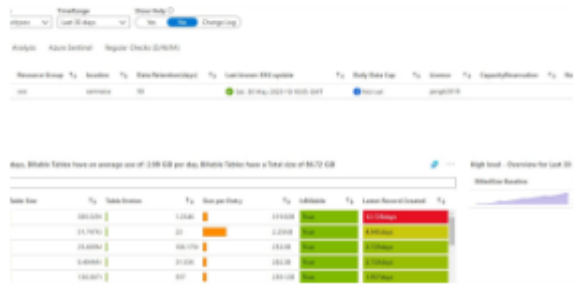
Description
Gain insights into your workspace's usage. In this workbook, you can view your workspace's data consumption, latency, recommended tasks and Cost and Usage statistics.

Content source
Standalone

Template version
1.6.2

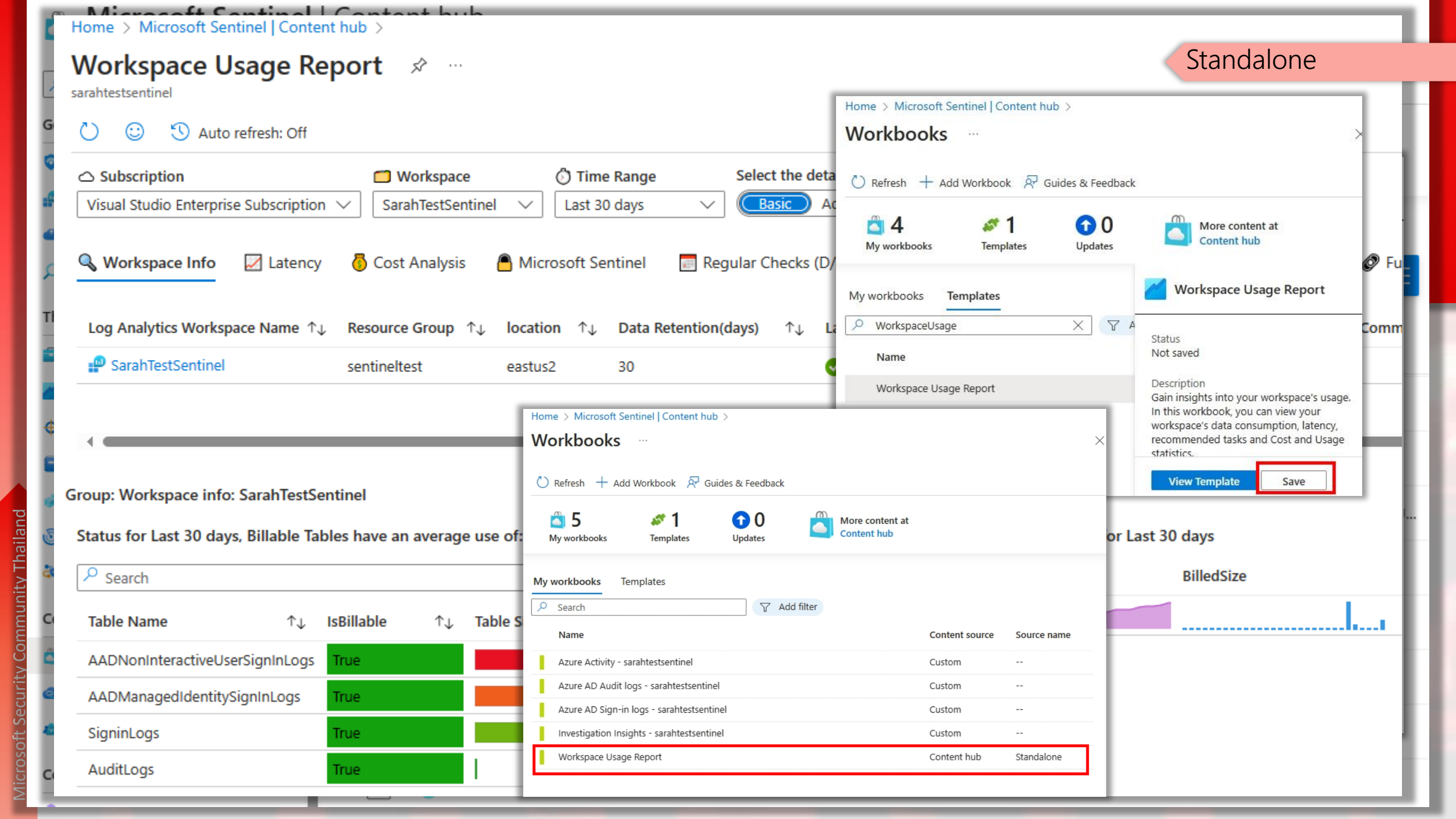
Author
Clive Watson

Supported by
Community



Configuration | View Template | Delete

Community | Security - Threat Protection


Home > Microsoft Sentinel | Content hub >
Workspace Usage Report
sarahtestsentinel
Standalone
Auto refresh: Off
Subscription
Visual Studio Enterprise Subscription
Workspace
SarahTestSentinel
Time Range
Last 30 days
Basic
Workspace Info
Latency
Cost Analysis
Microsoft Sentinel
Regular Checks (D/
Log Analytics Workspace Name
Resource Group
location
Data Retention(days)
SarahTestSentinel
sentineltest
eastus2
30
Group: Workspace info: SarahTestSentinel
Status for Last 30 days, Billable Tables have an average use of:
Search
Table Name
IsBillable
AADNonInteractiveUserSignInLogs
True
AADManagedIdentitySignInLogs
True
SigninLogs
True
AuditLogs
True
Home > Microsoft Sentinel | Content hub >
Workbooks
Refresh
Add Workbook
Guides & Feedback
4
My workbooks
1
Templates
0
Updates
More content at
Content hub
My workbooks
Templates
WorkspaceUsage
Name
Workspace Usage Report
Workspace Usage Report
Status
Not saved
Description
Gain insights into your workspace's usage. In this workbook, you can view your workspace's data consumption, latency, recommended tasks and Cost and Usage statistics.
View Template
Save
Home > Microsoft Sentinel | Content hub >
Workbooks
Refresh
Add Workbook
Guides & Feedback
5
My workbooks
1
Templates
0
Updates
More content at
Content hub
My workbooks
Templates
Search
Add filter
Name
Content source
Source name
Azure Activity - sarahtestsentinel
Custom
--
Azure AD Audit logs - sarahtestsentinel
Custom
--
Azure AD Sign-in logs - sarahtestsentinel
Custom
--
Investigation Insights - sarahtestsentinel
Custom
--
Workspace Usage Report
Content hub
Standalone
or Last 30 days
BilledSize
Microsoft Security Community Thailand

Workspace Usage Report - sarahtestsentinel

sarahtestsentinel

Standalone

Done Editing | Open | Help

Workspace Usage Report

Change Log

Use this report to analyze the the sizes of the different tables and Latency in your workspace and agents. This report checks the overall workspace health.

Version	Description
v1.1	Added Events Per Second (EPS) to Workspace Info Tab.
v1.2	Added EPS with a breakdown for Device Vendor in CommonSecurityLog
v1.3	Added EPS Tab and Min, Max values
v1.4	Added Checks Tab for Daily, Weekly and Monthly suggested checking routines. Also Defender for Cloud info in Costs Tab.
v1.4.2	Added Groups to all Tabs. Added Price info and Help button.
v1.4.3	Added to [COST] tab and report of "GBytes used per Computer"
v1.4.4	Quick fix to get the TableName duplicate removed. Added value to Y axis of [Cost] trend graph, Remove content (EPS) that is planned for the Sentinel Health workbook.
v1.4.5	Added extra Cost info, improve Weekly reports and other grids , testing release ONLY
v1.4.6	Moved Price to Costs Analysis Tab (all pricing is now in the same place). Added some table data, description and links to Latency grid. Filter on Queries in Weekly report and Workspace audit filters
v1.4.7	Add Pie chart of % billable vs. free to Cost Analysis. Add count of Rules, Rule Templates and Hunting Queries (just unique ones). Extra Defender for Cloud report for "minimal","common" and "all". Additional troubleshooting displays when Help toggle is on. % used for Tables. User

Help File

More details in the Wiki: https://github.com/clivewatson/KQLpublic/wiki/Workbook-Usage

Usage

```
- Please select your **Subscription** and **Workspace**
- Time Range: is the time you wish to query back to. i.e 7days from now, into the past.
- Help is available in various parts of this Workbook.
- Select the Detail Level - is a toggle to reduce the page load time of certain queries.
```

Categories

```
- Azure Monitor Logs (Workspace)
- Sentinel
- Defender for Cloud
```

Solutions

Solution	Description
Workspace Infomation	info about the workspace, usage and statistics
Latency	Which Tables or machines have latency issues, average, minimun and maximum values

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

Workspace Usage Report - sarahtestsentinel

sarahtestsentinel

Standalone

Done Editing | Open | Help

Workspace Usage Report

Change Log

Use this report to analyze the the sizes of the different tables and Latency in your workspace and agen
report checks the overall workspace health.

Version	Description
v1.1	Added Events Per Second (EPS) to Workspace Info Tab.
v1.4.7	Add Pie chart of % billable vs. free to Cost Analysis. Add count of Rules, Rule Templates and Hunting Queries (just unique ones). Extra Defender for Cloud report for "minimal","common"

1 **Editing parameters item: parameters - 1**

Settings | Advanced Settings | Style | Advanced Editor

Add Parameter | Style: Standard

Required?	Parameter name	Display name
✓	DefaultSubscription_Internal	
	Subscription	Sarah! Subscription?
	Workspace	My beauty, Workspace?
	resourceGroup	
	TimeRange	Time Range

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

Workspace Usage Report - sarahtestsentinel

sarahtestsentinel

Edit | Open | Help | Auto refresh: Off

Sarah! Subscripti... | My beauty, Wor... | Time Range

Visual Studio Enterprise Subscription | SarahTestSentinel | Last 30 days

Workspace Info | Latency | Cost Analysis | Microsoft Sentinel

ions

lution	Description
pace ation	info about the workspace, usage and statistics
Latency	Which Tables or machines have latency issues, average, minimun and maximum values

Simplified Microsoft Sentinel

Watchlist
Workbook
Parser
Hunting Query
Playbook
Analytic Rule
Data Connector

ENGINE

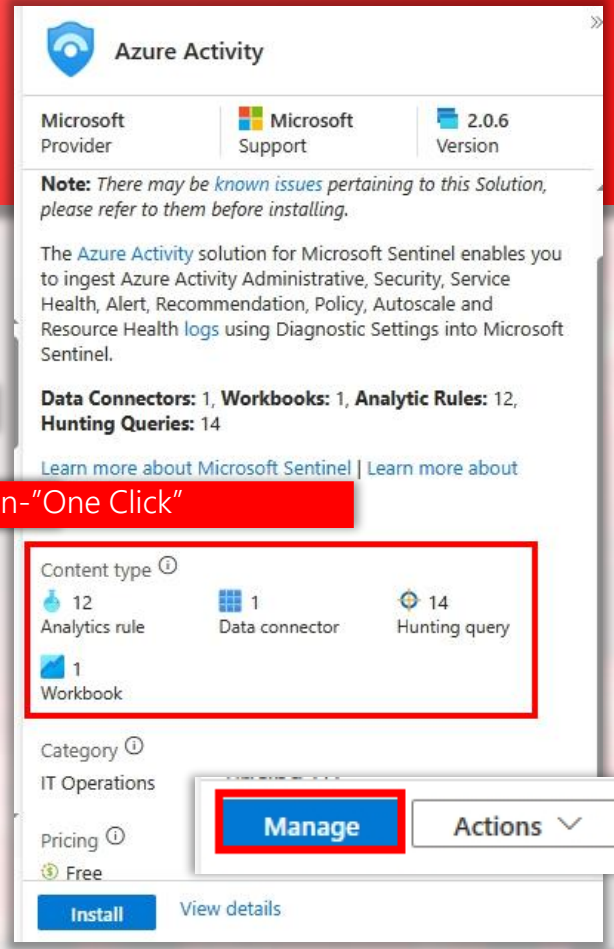
w/ Template Spec Contributor
In Subscription RBAC level

Get "**Content**"

OOTB

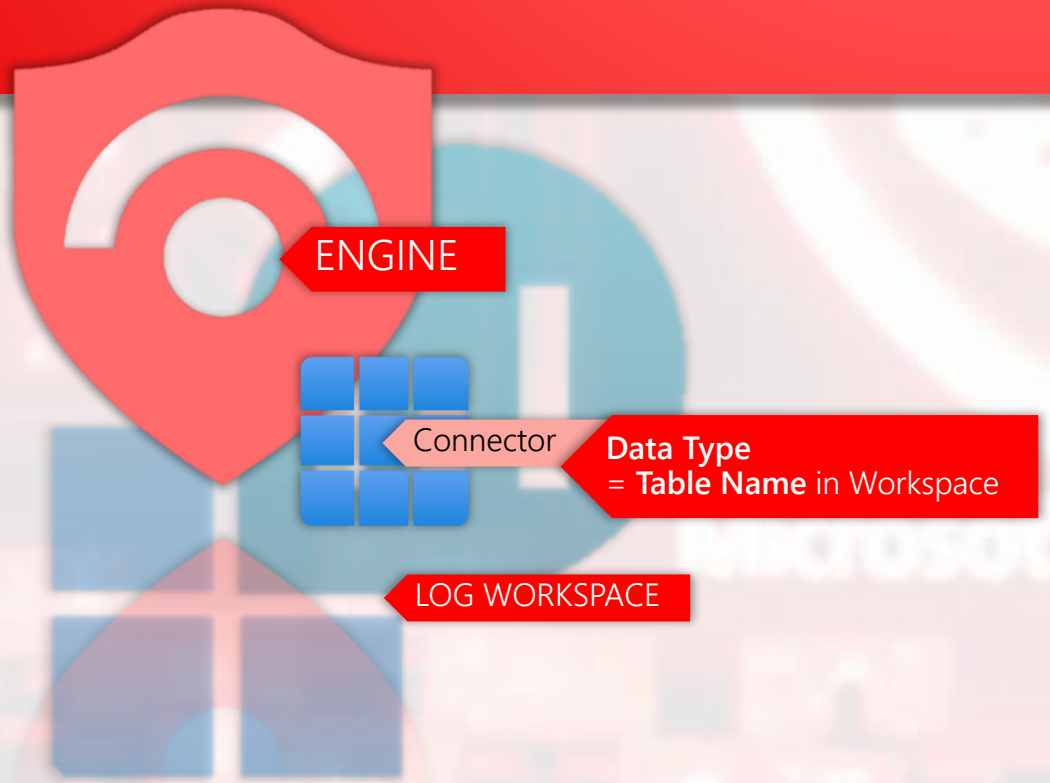
CONTENT HUB

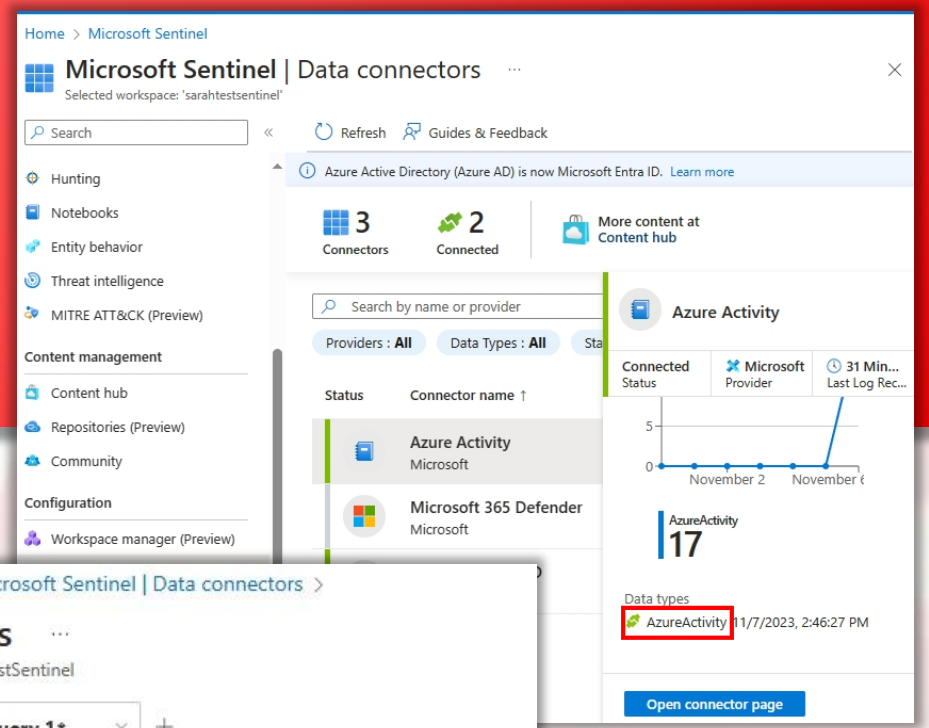
Solution All-in-"One Click"

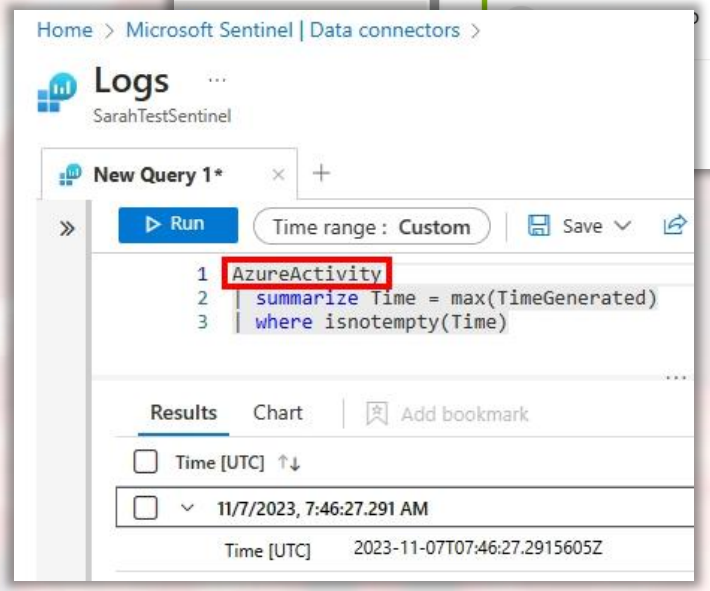


Microsoft Security Community Thailand

Simplified Microsoft Sentinel







Microsoft Security Community Thailand

Azure Activity

Refresh | Delete | Reinstall

28 Installed content items

13 Configuration needed

Azure Activity

Microsoft Provider | Microsoft Support | 2.0.6 Version

Description

Note: *There may be known issues pertaining to this Solution, please refer to them before installing.*

The Azure Activity solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel.

Data Connectors: 1, **Workbooks:** 1, **Analytic Rules:** 12, **Hunting Queries:** 14

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type
- 12 Analytics rule
- 1 Data connector
- 14 Hunting que
- 1 Workbook

Category
IT Operations

Pricing
Free

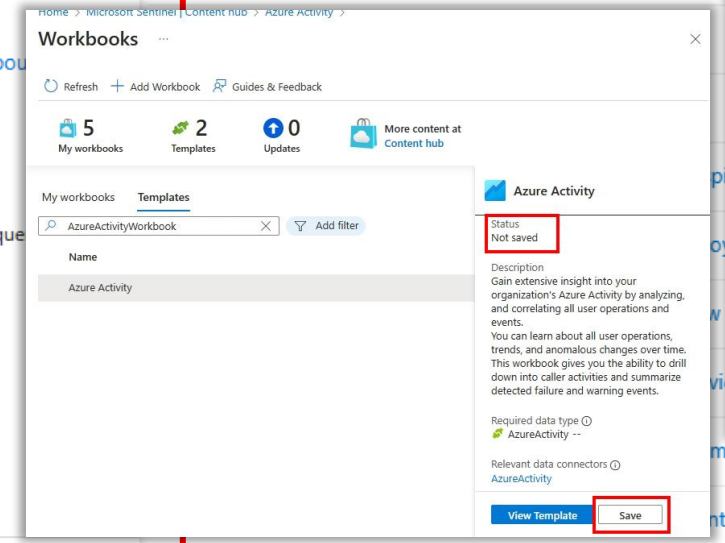
Manage | Actions | View details

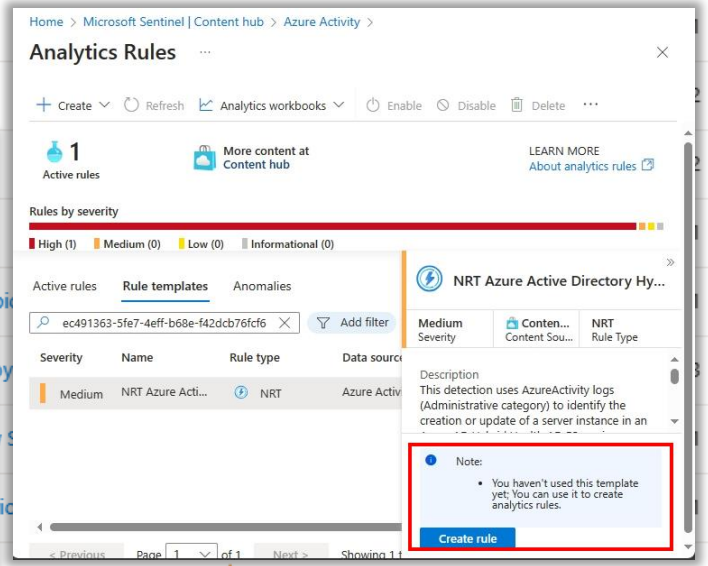
Search...

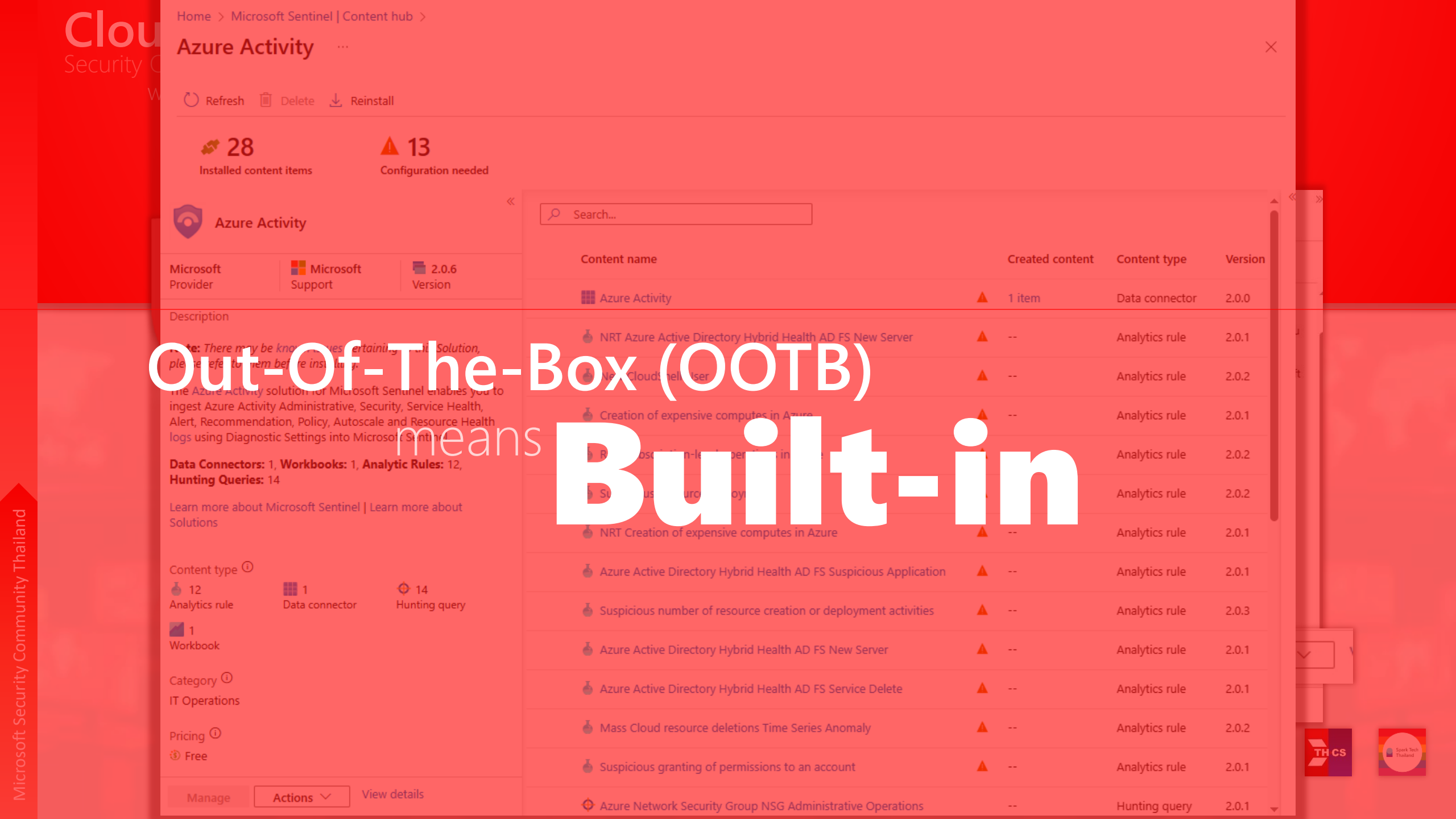
Content name		Created content	Content type	Version
Azure Activity	⚠	1 item	Data connector	2.0.0
NRT Azure Active Directory Hybrid Health AD FS New Server	⚠	--	Analytics rule	2.0.1
New CloudShell User	⚠	--	Analytics rule	2.0.2
Creation of expensive computes in Azure				
Rare subscription-level operations in Azure				
	⚠	--	Analytics rule	2.0.2
	⚠	--	Analytics rule	2.0.1
Azure Network Security Group NSG Administrative Operations		--	Hunting query	2.0.1

Connector

Templates







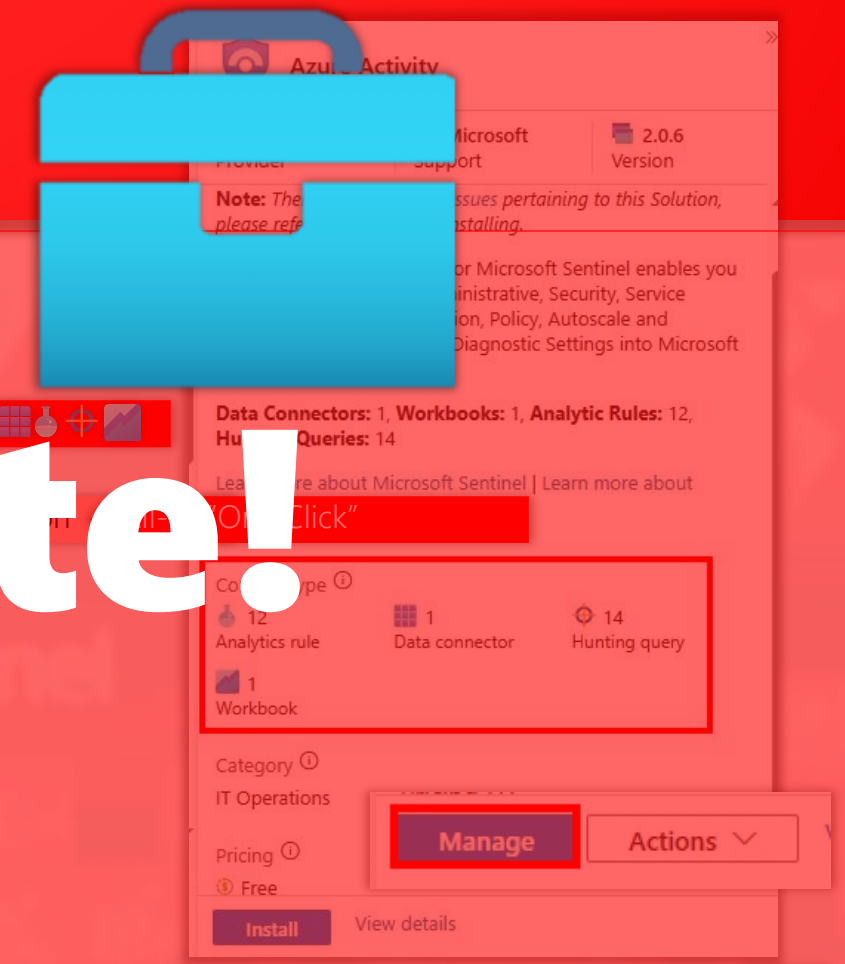
Out-Of-The-Box (OOTB) means Built-in

Microsoft Security Community Thailand

Cloud-native
Security Operations
with Microsoft **Sentinel**

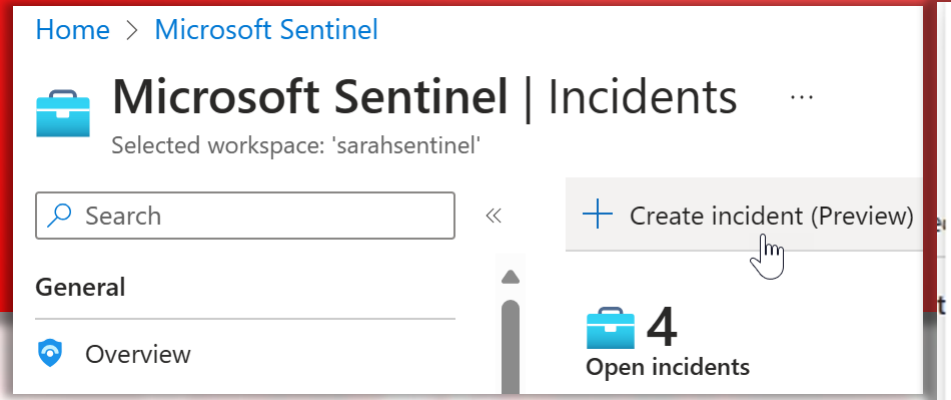
If no Incident to study

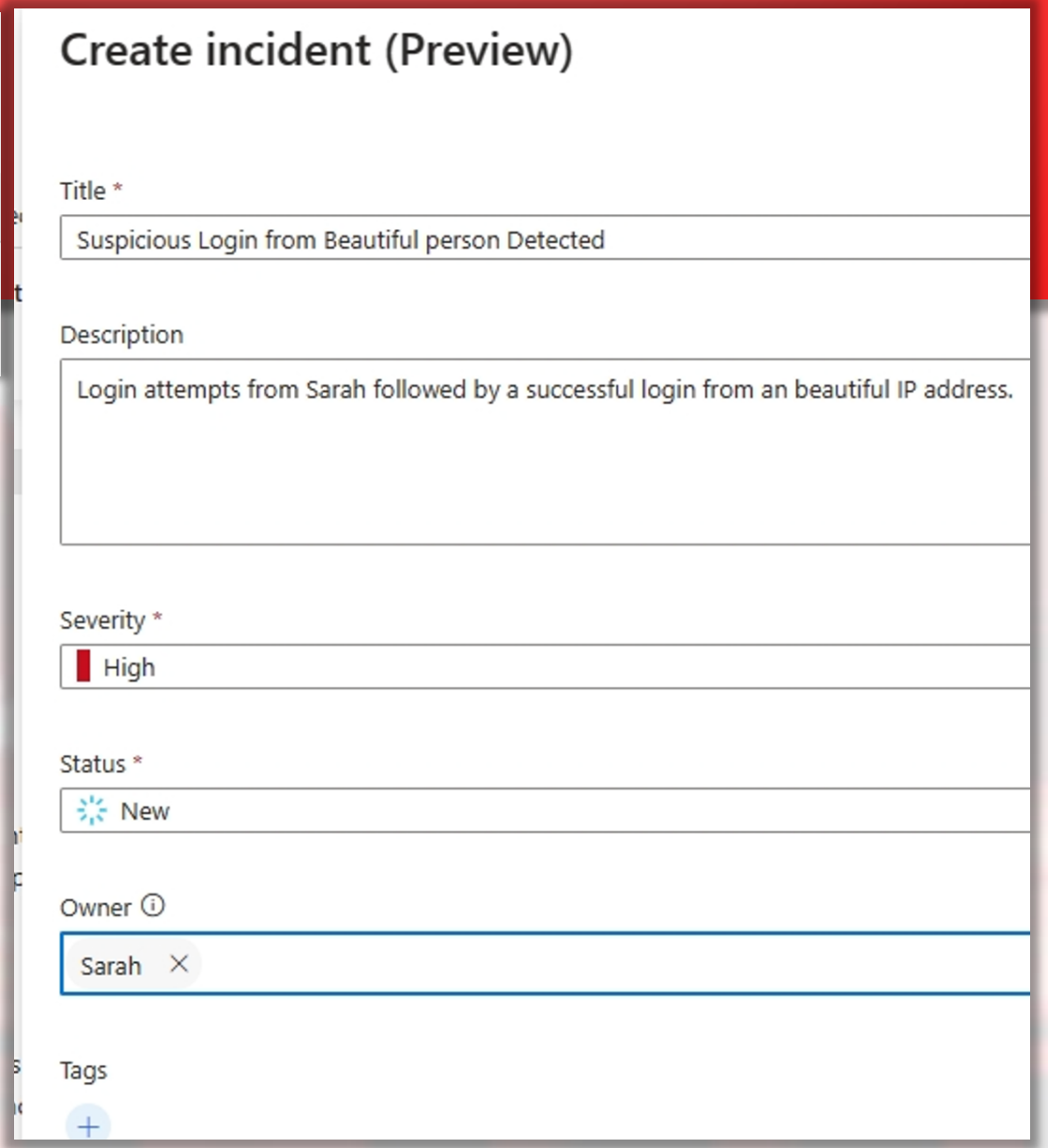
Just **Create!**



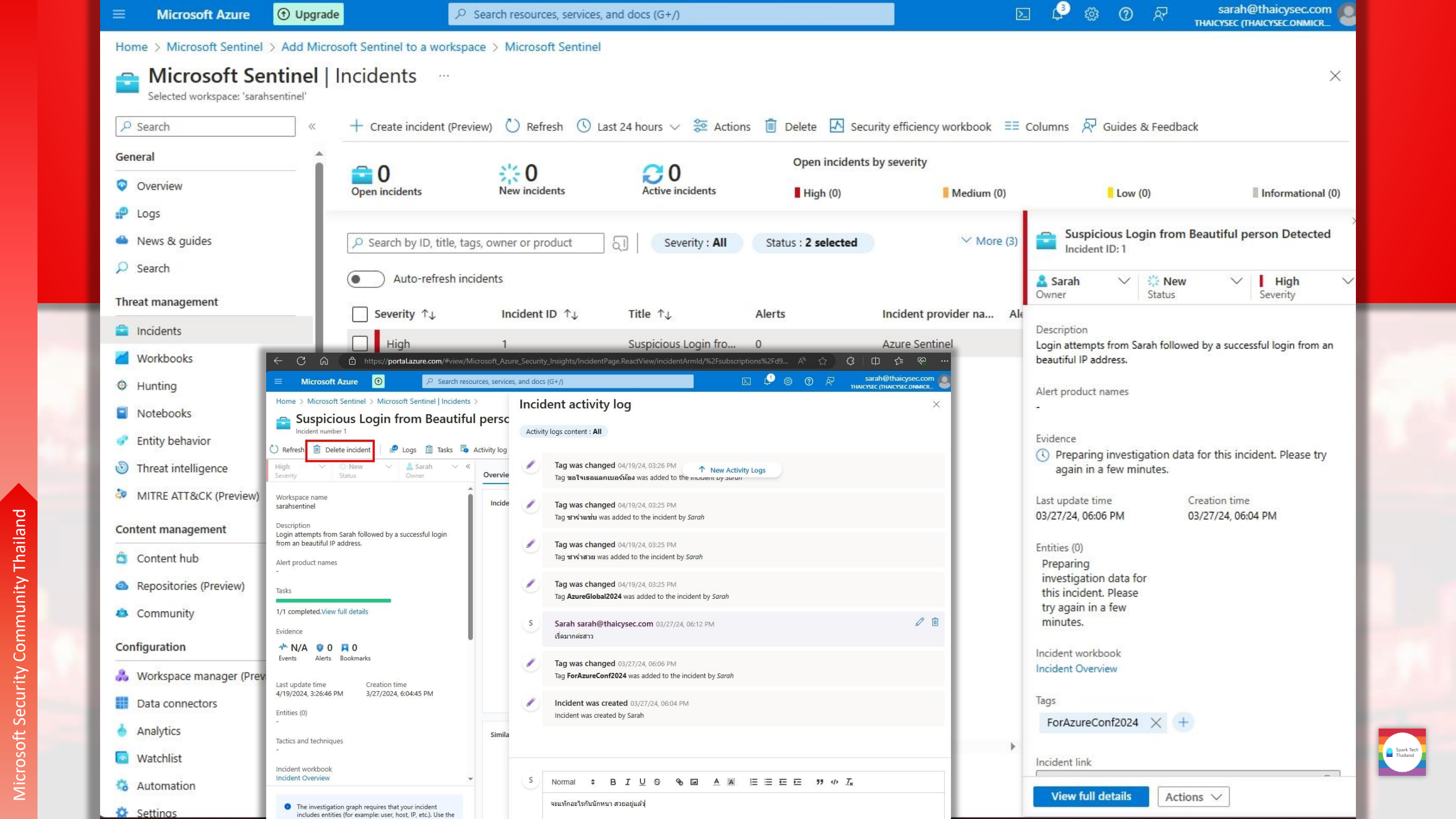
Microsoft Security Community Thailand

Simplified Microsoft Sentinel

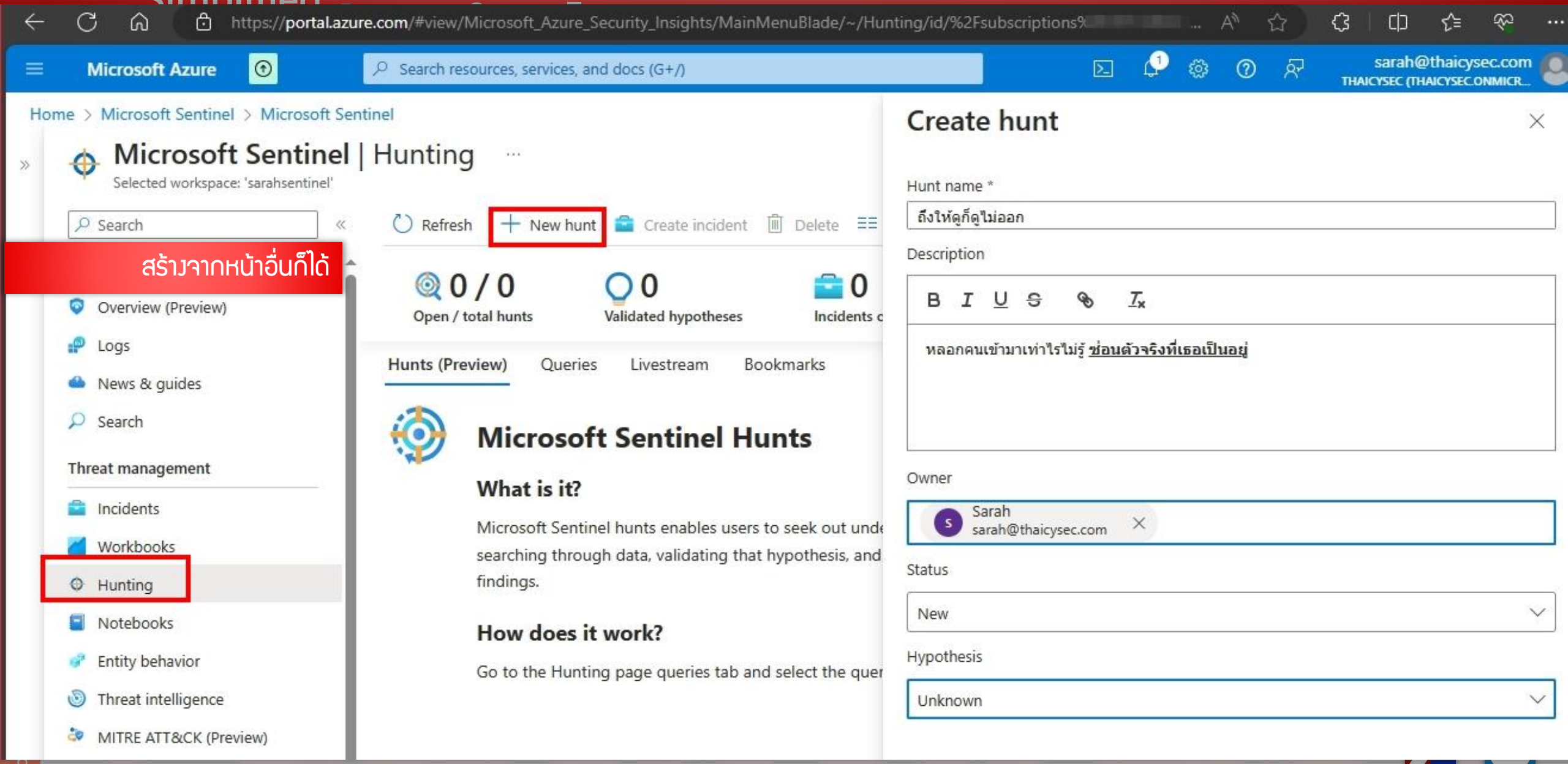


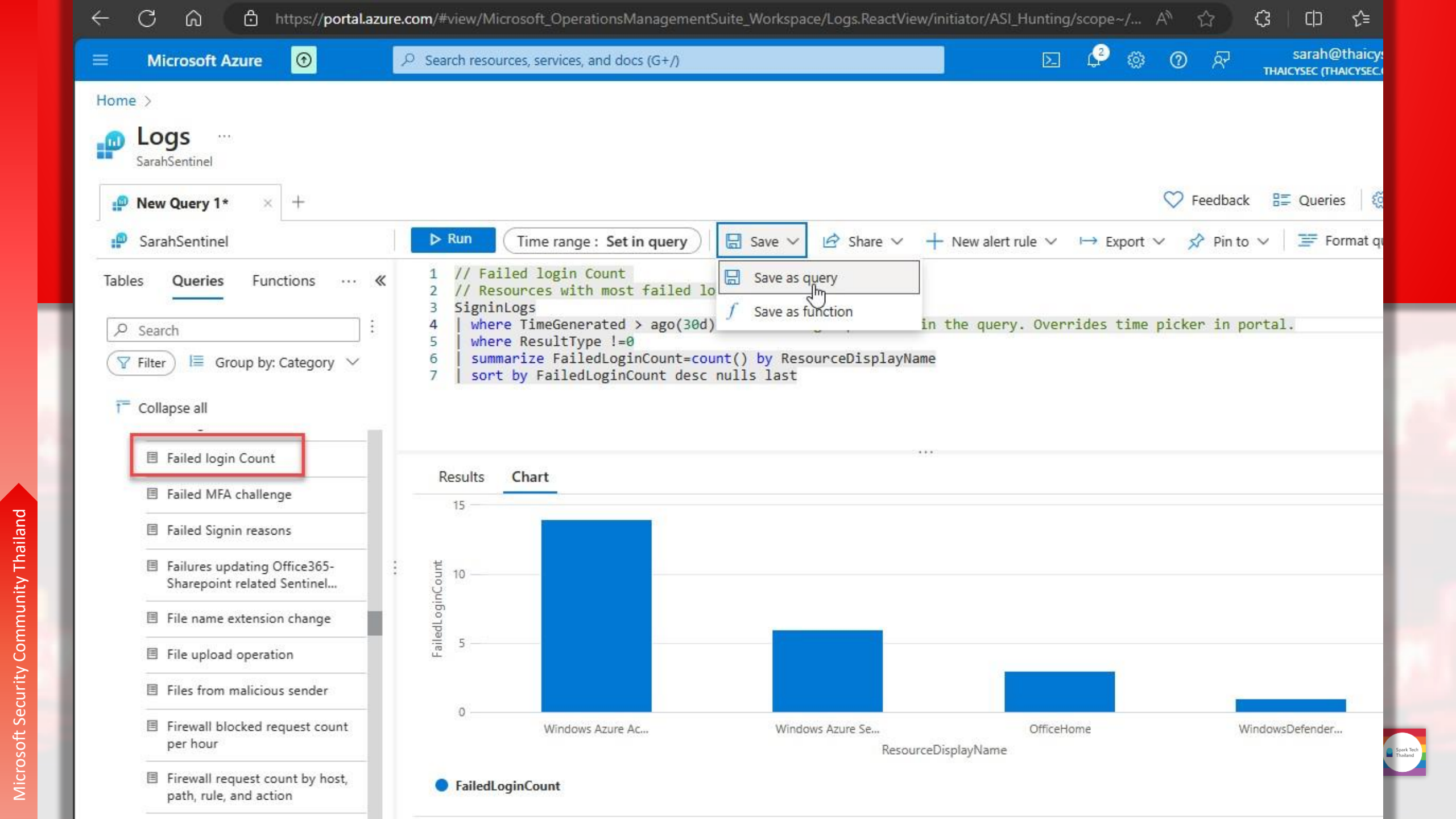


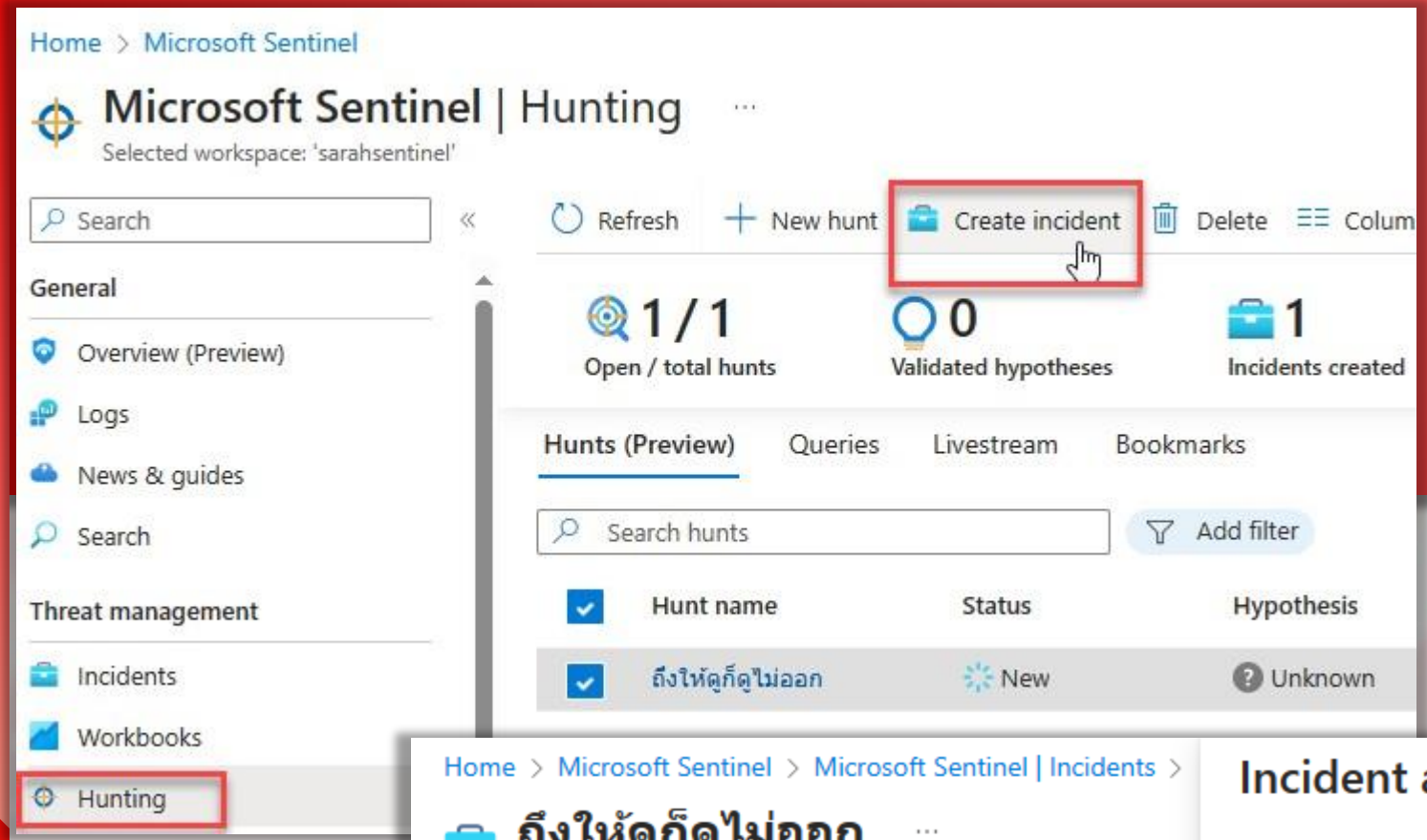
Microsoft Security Community Thailand

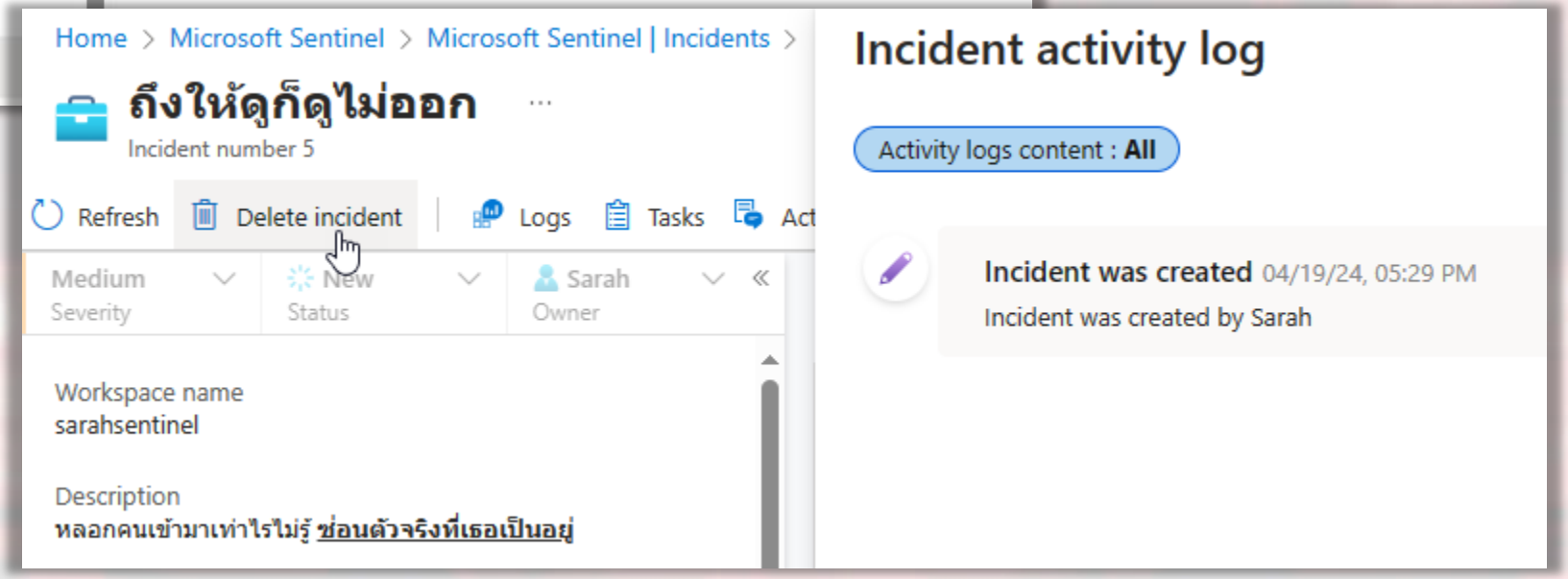

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
sarah@thaicysec.com
THAICYSEC (THAICYSEC.ONMICR...
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'sarahsentinel'
Search
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Security efficiency workbook
Columns
Guides & Feedback
General
Overview
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Prev
Data connectors
Analytics
Watchlist
Automation
Settings
0
Open incidents
0
New incidents
0
Active incidents
Open incidents by severity
High (0)
Medium (0)
Low (0)
Informational (0)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
More (3)
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Incident provider na...
High
1
Suspicious Login fro...
0
Azure Sentinel
Suspicious Login from Beautiful person Detected
Incident ID: 1
Sarah
Owner
New
Status
High
Severity
Description
Login attempts from Sarah followed by a successful login from an beautiful IP address.
Alert product names
-
Evidence
Preparing investigation data for this incident. Please try again in a few minutes.
Last update time
03/27/24, 06:06 PM
Creation time
03/27/24, 06:04 PM
Entities (0)
Preparing investigation data for this incident. Please try again in a few minutes.
Incident workbook
Incident Overview
Tags
ForAzureConf2024
Incident link
View full details
Actions
Incident activity log
Activity logs content : All
Tag was changed 04/19/24, 03:26 PM
New Activity Logs
Tag was changed 04/19/24, 03:25 PM
Tag ชาร่าแซ่บ was added to the incident by Sarah
Tag was changed 04/19/24, 03:25 PM
Tag ชาร่าสวย was added to the incident by Sarah
Tag was changed 04/19/24, 03:25 PM
Tag AzureGlobal2024 was added to the incident by Sarah
Sarah sarah@thaicysec.com 03/27/24, 06:12 PM
เริ่ดมากค่ะสาว
Tag was changed 03/27/24, 06:06 PM
Tag ForAzureConf2024 was added to the incident by Sarah
Incident was created 03/27/24, 06:04 PM
Incident was created by Sarah
Normal
จะแท็กอะไรกันนักหนา สวยอยู่แล้ว
Suspicious Login from Beautiful perso
Incident number 1
Refresh
Delete incident
Logs
Tasks
Activity log
Workspace name
sarahsentinel
Description
Login attempts from Sarah followed by a successful login from an beautiful IP address.
Alert product names
-
Tasks
1/1 completed.View full details
Evidence
N/A Events
0 Alerts
0 Bookmarks
Last update time
4/19/2024, 3:26:46 PM
Creation time
3/27/2024, 6:04:45 PM
Entities (0)
-
Tactics and techniques
-
Incident workbook
Incident Overview
The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the
Microsoft Security Community Thailand

Simplified

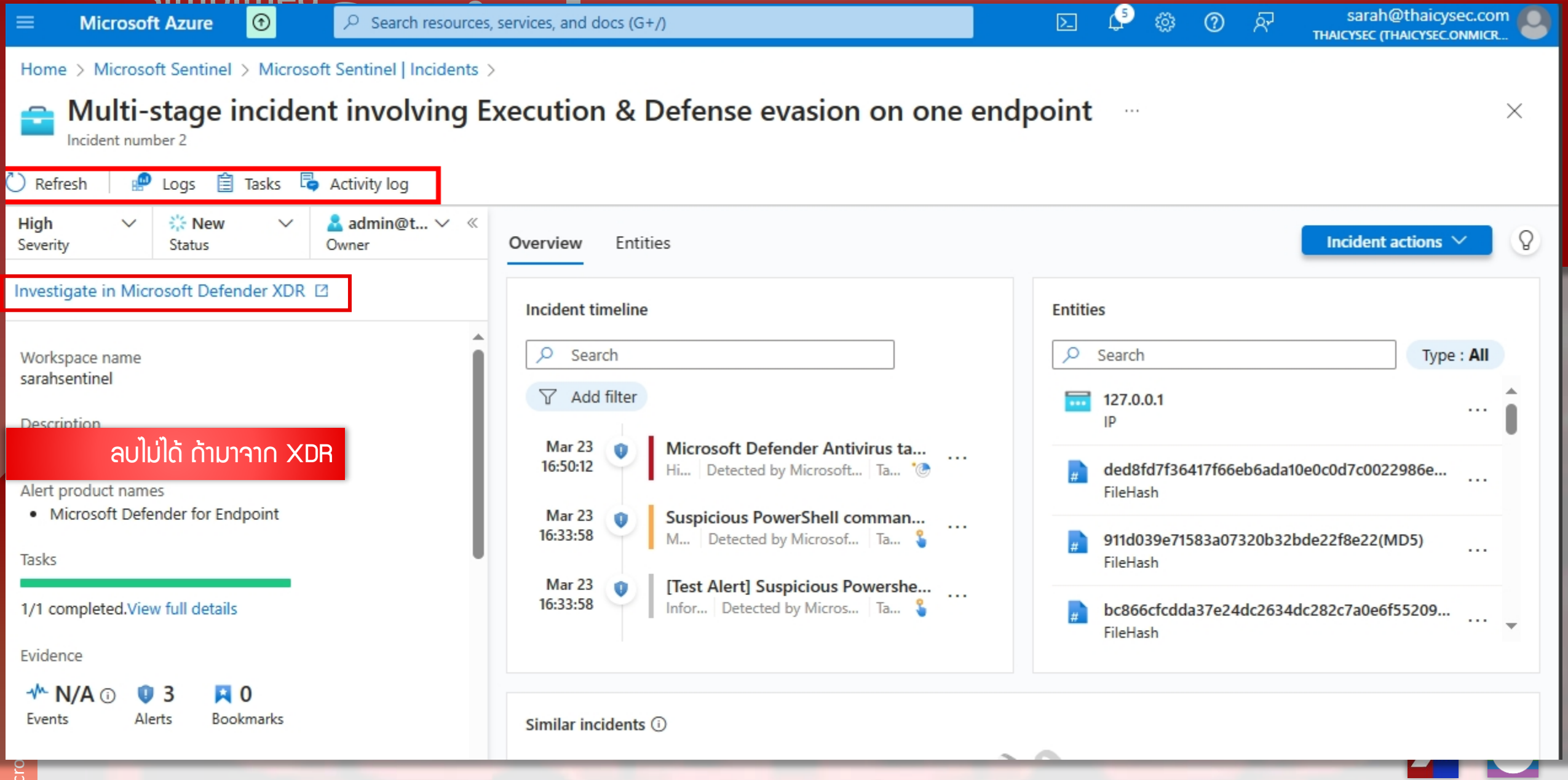

https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/Hunting/id/%2Fsubscriptions%
Microsoft Azure
Search resources, services, and docs (G+/)
sarah@thaicysec.com
THAICYSEC (THAICYSEC.ONMICR...
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Hunting
Selected workspace: 'sarahsentinel'
Search
Refresh
New hunt
Create incident
Delete
สร้างจากหน้าอื่นก็ได้
0 / 0
Open / total hunts
0
Validated hypotheses
0
Incidents c
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Hunts (Preview)
Queries
Livestream
Bookmarks
Microsoft Sentinel Hunts
What is it?
Microsoft Sentinel hunts enables users to seek out unde
searching through data, validating that hypothesis, and
findings.
How does it work?
Go to the Hunting page queries tab and select the quer
Create hunt
Hunt name *
ถึงให้ดูก็ดูไม่ออก
Description
หลอกคนเข้ามาเท่าไรไม่รู้ ซ่อนตัวจริงที่เธอเป็นอยู่
Owner
Sarah
sarah@thaicysec.com
Status
New
Hypothesis
Unknown





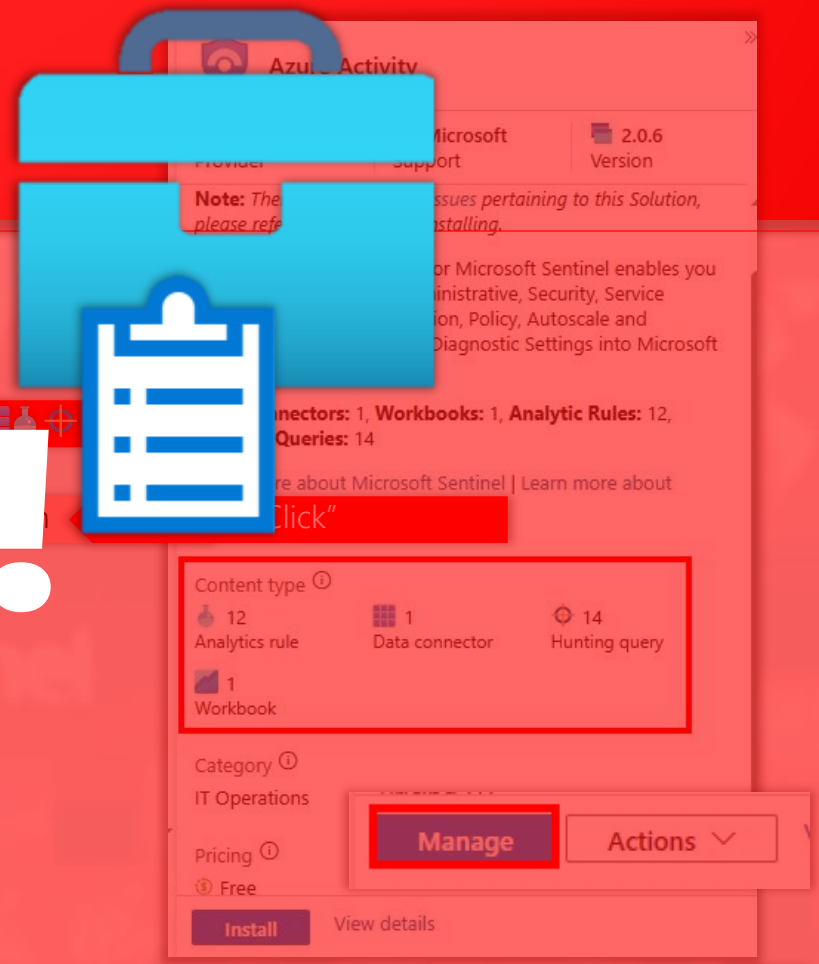


Simplified


Microsoft Azure
Search resources, services, and docs (G+/)
sarah@thaicysec.com
THAICYSEC (THAICYSEC.ONMICR...
Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >
Multi-stage incident involving Execution & Defense evasion on one endpoint
Incident number 2
Refresh
Logs
Tasks
Activity log
High
Severity
New
Status
admin@t...
Owner
Investigate in Microsoft Defender XDR
Workspace name
sarahsentinel
Description
ลบไม่ได้ ถ้ามาจาก XDR
Alert product names
Microsoft Defender for Endpoint
Tasks
1/1 completed.View full details
Evidence
N/A
Events
3
Alerts
0
Bookmarks
Overview
Entities
Incident actions
Incident timeline
Search
Add filter
Mar 23 16:50:12
Microsoft Defender Antivirus ta...
Hi... Detected by Microsoft... Ta...
Mar 23 16:33:58
Suspicious PowerShell comman...
M... Detected by Microsof... Ta...
Mar 23 16:33:58
[Test Alert] Suspicious Powershe...
Infor... Detected by Micros... Ta...
Entities
Search
Type : All
127.0.0.1
IP
ded8fd7f36417f66eb6ada10e0c0d7c0022986e...
FileHash
911d039e71583a07320b32bde22f8e22(MD5)
FileHash
bc866cfcdda37e24dc2634dc282c7a0e6f55209...
FileHash
Similar incidents

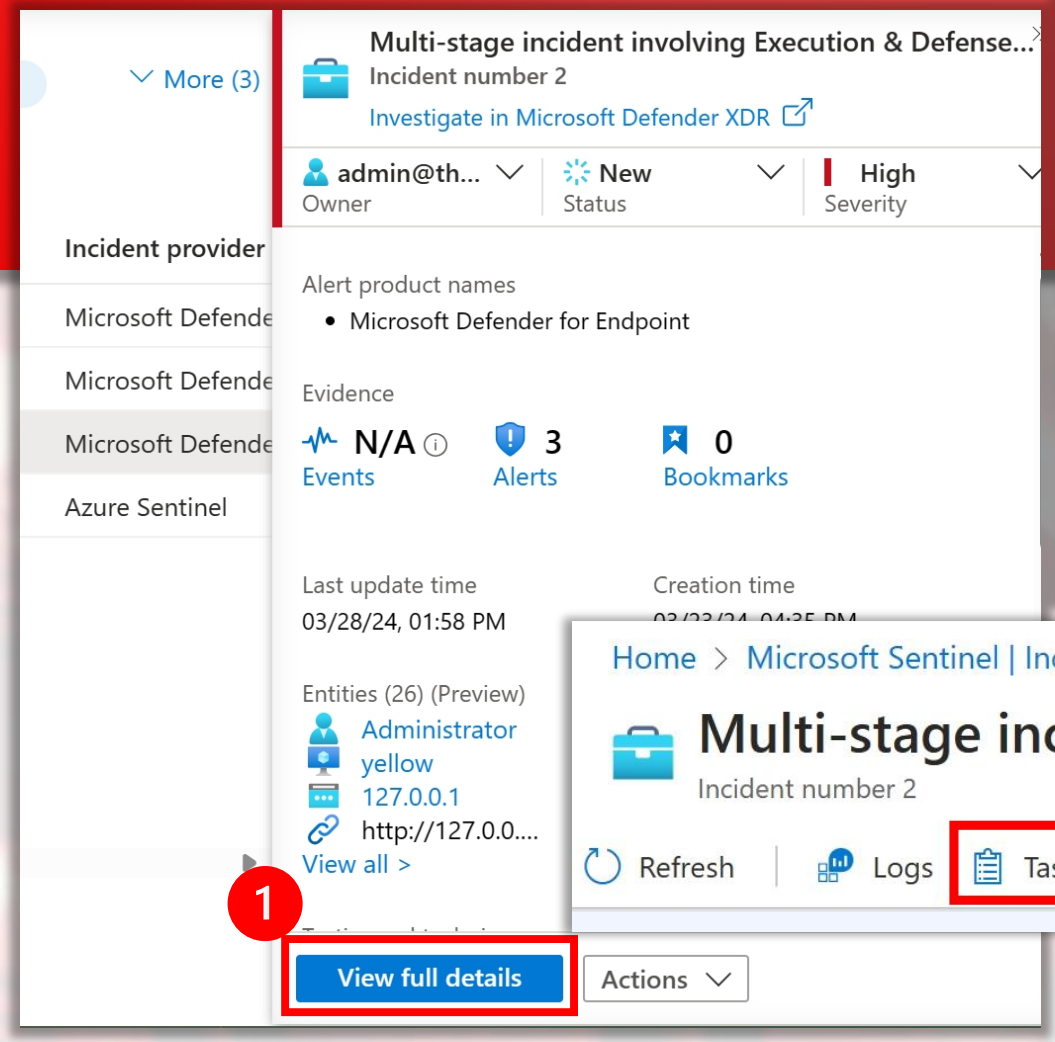
Cloud-native
Security Operations
with Microsoft **Sentinel**

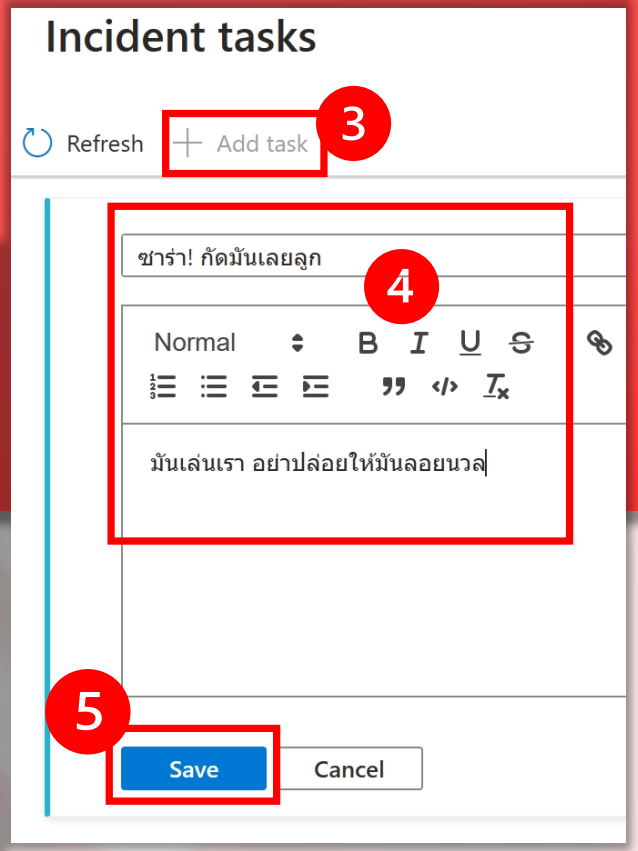
To-do List / Invite team?
Then create **Task!**

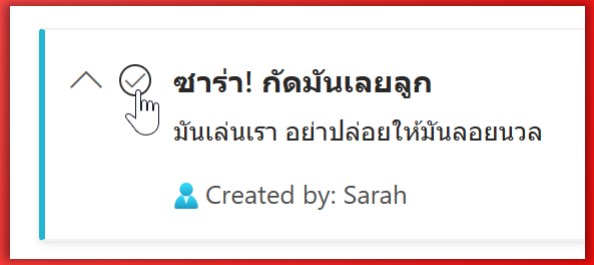


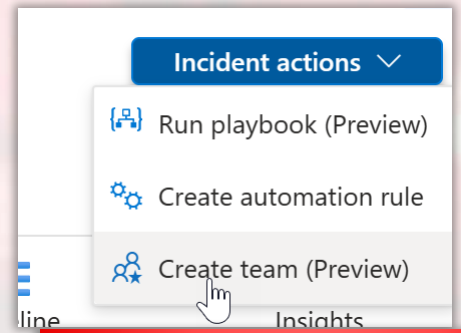
Microsoft Security Community Thailand

Simplified Microsoft Sentinel

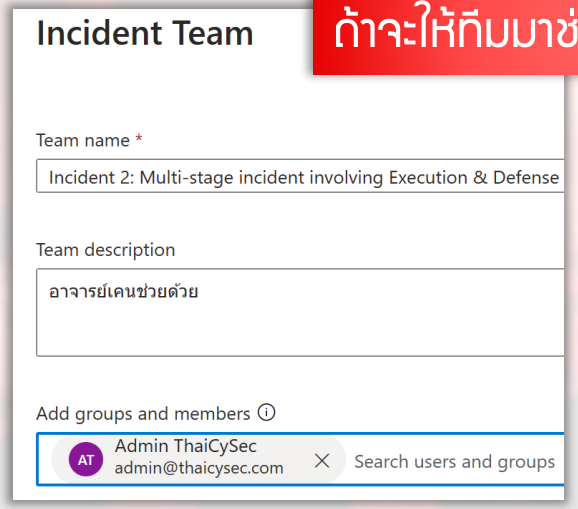








ถ้าจะให้ทีมมาช่วยจัดการ



Microsoft Security Community Thailand

Multi-stage incident involving Execution & Defense evasion on one end

Incident number 2

Refresh | Logs | Tasks | Activity log

This is the new, improved incident page - **Now generally available**. You can use the toggle to switch back.

High
Severity

New
Status

admin@thai...
Owner

Investigate in Microsoft Defender XDR

Workspace name
sarahsentinel

Description
--

Alert product names
- Microsoft Defender for Endpoint

Tasks
1/1 completed.View full details

Evidence

N/A	3	0
Events	Alerts	Bookmarks

Last update time
4/15/2024, 9:18:16 PM

Creation time
3/23/2024, 4:35:36 PM

Investigate

Overview | Entities

Search | Type : All

Name	Type
127.0.0.1	IP
ded8fd7f36417f66eb6ada10e0c0d7c0022986e	FileHas
911d039e71583a07320b32bde22f8e22(MD5)	FileHas
bc866cfcdda37e24dc2634dc282c7a0e6f55209c	FileHas
6cbce4a295c163791b60fc23d285e6d84f28ee4	FileHas
7353f60b1739074eb17c5f4dddefe239(MD5)	FileHas
de96a6e69944335375dc1ac238336066889d9ff	FileHas
yellow	Host
aedf41adc7a2d1b9bec091ece86a6fcc1e63e1d2	FileHas
79ef9cc16b1ecf09e424077014473e4b(MD5)	FileHas
e1a139c25d9069ca030bc6c6acdd1be4a8d5d81	FileHas
5fc5d3c811f87bcf1fa10f4aad355879647b1d7d	FileHas
719a31eeb64b9caeb66e0f992c9ac206(MD5)	FileHas

Incident tasks

Refresh | Add task

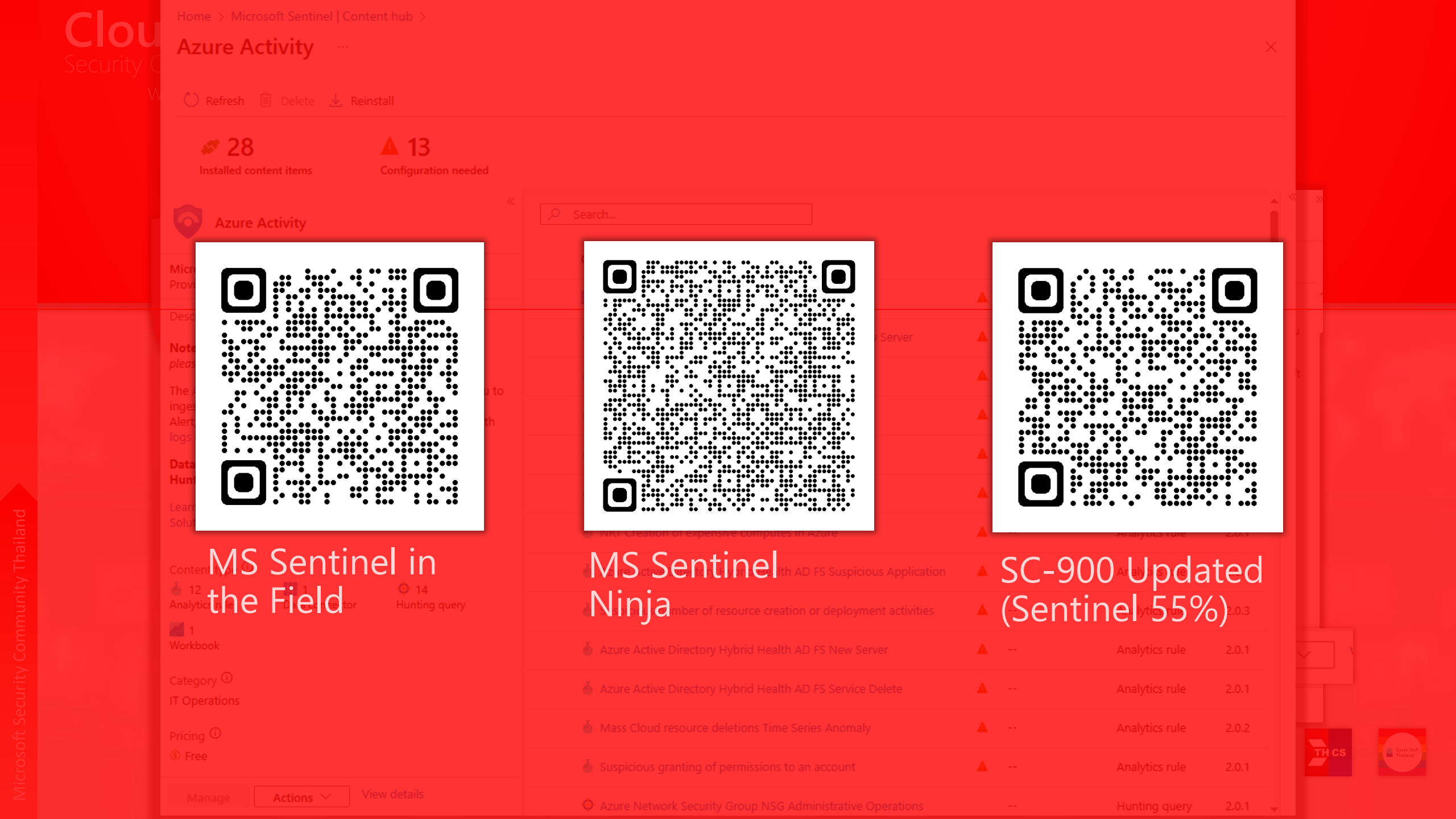
1/1 completed

Search | Status : All

ซาร่า! กัดมันเลยลูก

Created by: Sarah


Home > Microsoft Sentinel | Content hub
Azure Activity
Refresh
Delete
28
Installed content items
Azure Activity
Microsoft
Provider
Microsoft
Support
Description
Content type
12
Analytics rule
1
Data connector
1
Workbook
Category
IT Operations
Pricing
Free
Manage
Actions
View details
Content type
Version
Data connector
2.0.0
Analytics rule
2.0.1
Analytics rule
2.0.2
Analytics rule
2.0.2
Analytics rule
2.0.1
Analytics rule
2.0.1
Analytics rule
2.0.3
Analytics rule
2.0.1
Analytics rule
2.0.1
Analytics rule
2.0.2
Analytics rule
2.0.1
Suspicious granting of permissions to an account
Azure Network Security Group NSG Administrative Operations
Hunting query
2.0.1
Content Hub
Simulation
Lab
Microsoft Security Community Thailand


Azure Activity
Refresh
Delete
Reinstall
28
Installed content items
13
Configuration needed
Azure Activity
Search...
MS Sentinel in the Field
MS Sentinel Ninja
SC-900 Updated (Sentinel 55%)
Microsoft Security Community Thailand

Exam Example in SC-900

Azure Basic Security

1	can provide NAT.
2	can provide remote access service to VM inside Vnet.
3	can filter traffic per IP/port/protocol, both at specific subnet and VM interfaces.

A.	Azure Virtual Network Gateway	
B.	Azure Firewall	1
C.	Azure DDoS Protection	
D.	Azure Bastion	2
E.	NSG	3

Answer: **Firewall/Bastion/NSG**

Hint: **Firewall=NAT, Bastion=Remote, NSG=**Basic **Filter**

Exam Example in SC-900

Azure Basic Security

Encryption “at rest”, for example:

A. encrypting email and send
B. encrypting disk in VM
C. encrypting HTTPS connection when visiting website
D. encrypting VPN connection with IPsec
E. encrypting logs sending from Log Analytics Workspace

Answer: encrypting **Disk** in Virtual Machine

Hint: **at rest** is encrypting data on disk/database, not in sending/receiving connection (Encryption in Transit)

Exam Example in SC-900

Azure Basic Security

Which two resources can be protected by Azure Firewall directly?

A. On-premise Endpoints
B. Azure Active Directory
C. Active Directory Domain Service (AD DS)
D. Virtual Machine (VM)
E. Virtual Network (VNET)
F. Azure KeyVault

Answer: VM and VNet
Hint: Per Virtual Network topology in Azure **IaaS** services

Exam Example in SC-900

Defender for Cloud

[ ] gives recommendations from benchmark and guidance for protecting services on Azures.

A. Trust Center
B. Cloud Adoption Framework
C. Application Insights
D. Security Baseline
E. Log Analytics

Answer: **Security Baseline**

Hint: **recommendations** from Secure Score in Security Center is from Azure Security **Benchmark = Security Baseline**

Exam Example in SC-900

Defender for Cloud

Secure Score in M365 Defender:

1. Can provide MS Cloud App Security's Recommendations Yes/No
2. Can compare score with organizations like yours Yes/No
3. Can be improved if follow recommendations for Active Directory Yes/No
4. Can be improved even using 3rd party software for actions Yes/No

Answer: **Y/Y/Y/Y**

Hint: MCAS = Defender for Cloud Apps, M365 Secure Score came from M365 products including AAD

Exam Example in SC-900

Defender for Cloud

Which feature can detect threat in Azure SQL Managed Instance?

A. Azure ATP
B. Azure Sentinel
C. Azure Defender
D. Azure AD
E. Azure Monitor

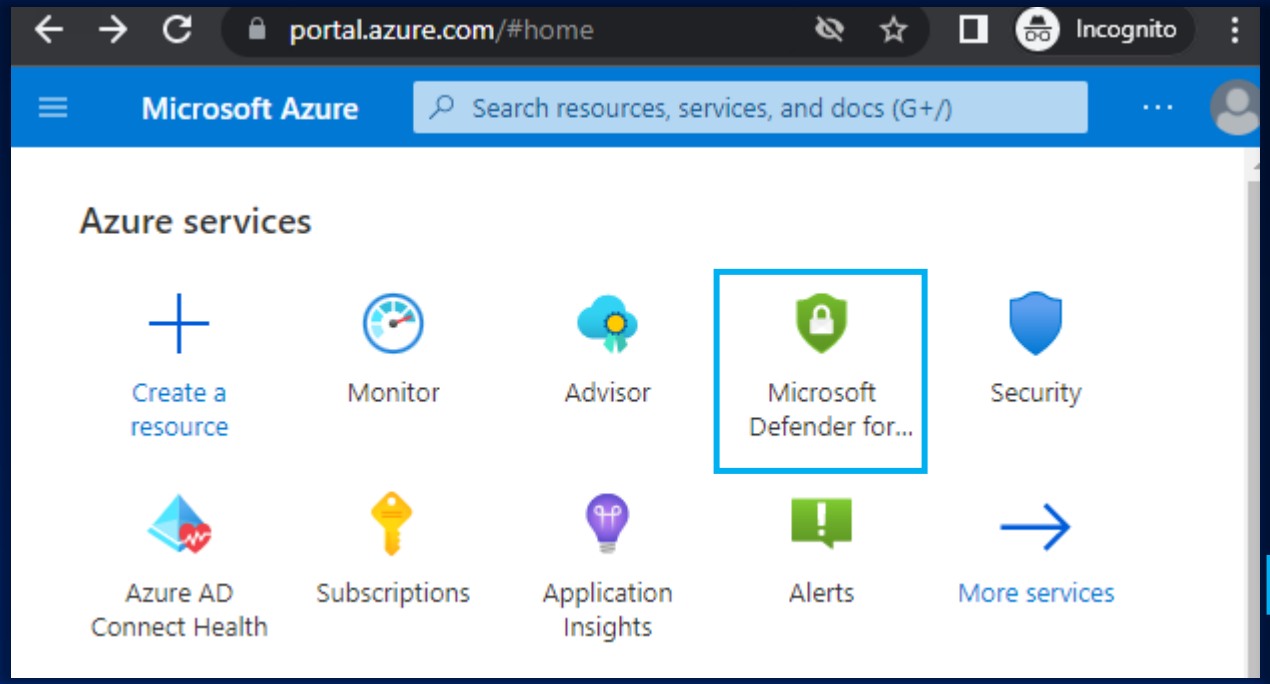
Answer: **Azure Defender (Defender for Cloud)**

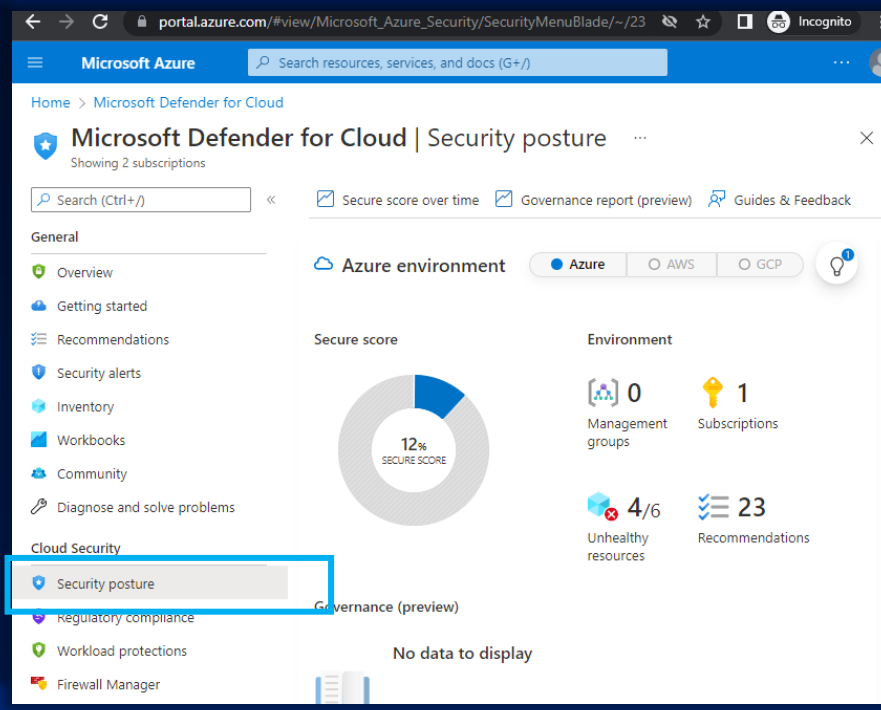
Hint: Defender for Cloud – Cloud Workload Protection (CWP) such as Defender for Server/SQL/Container etc.

Exam Example in SC-900

Defender for Cloud

Where can you see Azure Secure Score?





Answer: **Security Center (or new name: Defender for Cloud)**

Hint: Security Center/Score is CSPM module in Defender for Cloud that now is called “Security Posture”

Exam Example in SC-900

(Azure) Microsoft Sentinel

_____ is what Sentinel use for automatic response, automate common tasks.

A. Workbook
B. Playbook
C. Microsoft 365 Defender
D. Notebook
E. Defender for Cloud
F. Lookbook

Answer: **Playbook**
Hint: **“Play”book** is Logic App for task automation

Exam Example in SC-900

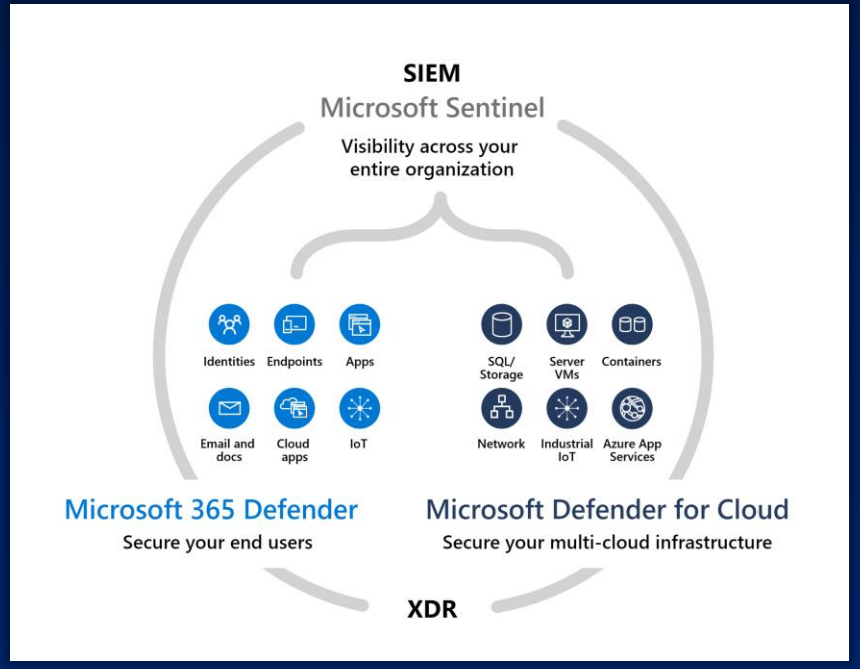
(Azure) Microsoft Sentinel

[ ] can be integrated as the eXtended Detection and Response (XDR) capabilities for Sentinel?

A. Azure AD
B. Purview 365 Compliance
C. 365 Defender (MDE) + Defender for Cloud
D. Active Threat Hunting
E. Workbook

Answer: **365 Defender**

Hint: **Defender** is cloud-based EDR (XDR) that is integrated with SIEM for “end-to-end” visibility – bi-directional alert sync



Exam Example in SC-900

365 Defender

[ ] is solution on cloud that use signals from on-premises AD DS to manage advanced threats.

A. Defender for Cloud Apps
B. Defender for Identity
C. Defender for Office 365
D. Defender for Endpoint

Answer: Defender for **Identity**

Hint: Defender for **Identity** use signals from **on-premises** Active Directory Domain Service (AD DS)

Exam Example in SC-900

365 Defender

As first line of defense, which feature of MS Defender for Endpoint (MDE) can reduce attack surface?

A. Vulnerability Assessment
B. Next-Generation Protection
C. Automatic Remediation
D. Advance Hunting
E. Network Protection

Answer: **Network Protection**

Hint: refer to Defense in Depth principle, **"Network"** Protection feature for blocking unwanted network access would be 1st line of defense.

Exam Example in SC-900

365 Defender

Which menu in security.microsoft.com (365 Security Center) that you can see details of alerts, such as affected devices?

A. Incidents & Alerts
B. Hunting
C. Action & Submission
D. Secure Score
E. Vulnerability Management

Answer: **Incidents**
Hint: Incidents = set of Alerts

Exam Example in SC-900

365 Defender

Which two of these are direct functions of Defender for Endpoint?

A. Checking impossible travel/unusual sign in locations
B. Scan malware in mail attachment
C. Automated investigation and remediation
D. Detecting Shadow IT
E. Attack Surface Reduction (ASR) with Defender Antivirus and Intune

Answer: **C, D**

Hint: MDE = Alert Management, so Automated resolving alerts are MDE feature. ASR use Intune endpoint security policy with “Defender Antivirus” on clients, so it is also MDE feature.

Exam Example in SC-900

365 Defender

Which product can use for scanning email and guarantee that email forwarded to others is free from malware?

A. Defender for Identity
B. Defender for Endpoint
C. Defender for Office 365
D. Defender for Cloud App
E. Defender for IoT
F. Defender for Cloud

Answer: **Defender for Office 365**
Hint: Office 365 services = **Exchange** + SharePoint/OneDrive

Exam Example in SC-900

Microsoft Intune

To control how Intune managed devices can access resources, you have to use which feature in Azure AD?

A. Previledge Identity Management (PIM)
B. Access Review
C. Azure Policy
D. Multi-Factor Authentication (MFA)
E. Conditional Access

Answer: **Conditional Access**
Hint: **control/restrict access** from which **cloud apps** (MCAS/Defender for Cloud Apps) or which enrolled **devices** in **Intune**, all is using Azure AD's **Conditional Access**