

A graphic element on the left side of the slide features a stylized map of Thailand. The map is composed of several overlapping triangles in shades of red, blue, and grey, creating a layered effect. The word "THAILAND" is overlaid on this graphic in large, white, sans-serif capital letters.

THAILAND

Cyber
Security



 Microsoft Security

Cloud SECURITY Intensive





Security Operations

XDR +
SIEM





AntiVirus Endpoint DR eXtended DR

SC-900

SECURITY
COMPLIANCE
IDENTITY



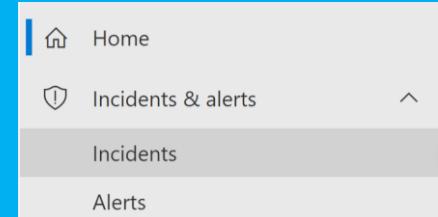
365 Defender



-  for Identities
 - Prevent Cred./Password Leak
 - Signal from On-Prem 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
-  Reports
-  Audit
- Report > Trend + Status



SC-900

SECURITY
COMPLIANCE
IDENTITY



Microsoft Secure Score

Overview Recommended actions History Metrics & trends

(i) SaaS Security Posture Management for non-Microsoft applications is currently in public preview for every customer with Defender.

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

Applied filters:

Export

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

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

The screenshot shows the Microsoft 365 Defender Microsoft Secure Score dashboard. The main header says "afe afe Microsoft 365 Defender". The left sidebar has sections like Home, Incidents & alerts, Hunting, Actions & submissions, Threat analytics, Secure score (which is selected), Learning hub, Trials, Assets, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management, Email & collaboration, and Investigations. The main content area starts with "Microsoft Secure Score" and "Secure Score: 29.03%". It includes a progress bar for "36/124 points achieved" and a breakdown by category: Identity (17.86%) and Apps (38.24%). Below this are "Actions to review" (0 Regressed, 19 To address, 0 Planned, 0 Risk accepted, 0 Recently added, 0 Recently updated) and a list of recommended actions such as "Require MFA for administrative roles" and "Ensure all users can complete multi-factor authentication for secure". A "Comparison" section on the right shows "Your score" at 29.03/100 and "Organizations like yours" at 48.38/100. A callout box says "Compare score with Organizations like yours".

Microsoft Secure
Score can provide
recommendations
for MCAS

Licensing of this capability may be changed

SC-900

SECURITY
COMPLIANCE
IDENTITY



security.microsoft.com

The screenshot shows the Microsoft 365 Defender interface with the following navigation bar items: Microsoft 365 Defender, Search, and a star icon labeled "afe afe". The main content area is titled "Endpoints" under "Settings > Endpoints". It includes sections for "Attack simulation training", "Policies & rules", "Cloud apps", "Cloud discovery", "Cloud app catalog", "OAuth apps", "Activity log", "Reports", "Audit", "Health", "Permissions", and "Settings". A sidebar on the left lists "Endpoints", "APIs", "SIEM", "Rules", "Alert suppression", "Indicators", "Process Memory Indicators", "Web content filtering", "Available caps", "Automation uploads", and "File hashes", "IP addresses", "URLs/Domains", "...". At the bottom, there are "Export", "Search title or value", "Import", "Add item", "1-2 < > 30 items per page", and a table with columns "URL/Domain", "Applicat...", and "Action".

Network Protection (MDE feature + Intune ASR Policy)

The screenshot shows the Microsoft Endpoint Manager admin center with the URL "https://endpoint.microsoft.com/#blade/Microsoft_Intune_Workflows/IntentReportPerIntentMenu/intentReportPe". The main content area is titled "ThaCySec Web Protection | Per-setting status". It includes sections for "Overview", "Manage", "Properties", and "Monitor". A table on the right shows "Setting" and "Status" for "Enable network protection" (Succeeded) and "Require SmartScreen for Microsoft Edge Legacy" (Succeeded). On the left, there is a sidebar with links: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support.

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



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 privilege” 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)

Deploy Security Policies via Intune/GPO (optional)

Tune/Suppress Alert Levels to reduce noise

The screenshot shows the Microsoft Defender for Endpoint portal. At the top, there's a navigation bar with 'Defender' and a search bar. Below it, a card displays an alert titled '[Test Alert] Suspicious Powershell commandline'. The alert is categorized as 'Detected' (red dot). It includes links to 'Open alert page', 'Manage alert', 'See in timeline', 'Create suppression rule' (which is highlighted with a blue box), and 'Edit alert another incident'. Below the alert card, there are tabs for 'Details' and 'Recommendations'. The 'Details' tab shows 'RECOMMENDATIONS' and 'Remediation & prevention actions you should take'. The 'Recommendations' tab shows 'View all recommendations'. At the bottom, there are filters for 'Alert name', 'Tags', 'Severity', and 'Investigation state', with one item selected: '[Test Alert] Suspicious... Informational'.

and assign Remediation level (to full?) to each group

Ex. ASR, EDR (AV), Compliance/Configuration

A modal dialog box titled 'Resolve alert [Test Alert] Suspicious Powershell commandline'. It contains the following details:

Rule details	
Status	Enabled
Type	Advanced
Scope	Organization
Action	Resolve alert
Matching Alerts	0
Created by	sarah.h@akeake.com
Created on	Nov 24, 2022, 11:37:15 PM

Below the rule details, there's a section for 'Suppression conditions' with the text 'Suppress whenever alert is triggered by any IO'.



Defender for Endpoint (MDE)

Remediation for Files

The screenshot shows the Microsoft 365 Defender interface. On the left, there's a navigation sidebar with various sections like 'Evaluation & tutorials', 'Configuration management', 'Email & collaboration', 'Review', 'Exchange message trace', 'Policies & rules', 'Cloud apps', 'App governance', 'Reports', 'Audit', 'Health', 'Permissions', and 'Settings'. The 'Settings' tab is currently selected. In the main area, under 'Endpoints', there's a 'Device groups' section. A modal window titled 'Edit device group' is open, showing a 'General' tab where a device group named 'Sarah1' is being configured. A dropdown menu for 'Automation level' is open, showing options: 'Semi - require approval for core folders' (selected), 'No automated response', 'Semi - require approval for all folders', 'Semi - require approval for non-temp folders', and 'Full - remediate threats automatically'. Below the modal, a table lists device groups: 'Sarah1' (rank 1, 1 device, remediation level 'Semi - require approval for core folders') and 'Last' (rank Last, 0 devices, remediation level 'Full - remediate threats automatically').

Edit device group

General Devices Preview devices User access

Provide a name and a description for this notification rule to m

Device group name *

Sarah1

Automation level *

Semi - require approval for core folders

No automated response

Semi - require approval for all folders

Semi - require approval for non-temp folders

Semi - require approval for core folders

Full - remediate threats automatically

Organize devices into groups, set automated remediation levels, and assign administrators.

+ Add device group

Rank	Device group	Devices	Remediation level	Description
1	Sarah1	1	Semi - require approval for core folders	ເກມສັກ
Last	Ungrouped devices (de...)	0	Full - remediate threats automatically	Devices that c

Remediation level based on Device Group



Defender for Endpoint (MDE)

Remediation for Files

← → 🔍 security.microsoft.com/incidents/7/evidence?tid=c2807b7e-9e2d-4e50-b000-82a3f42183eb

File Verdict

Lazagne post-exploitation tool > Lazagne post-exploitation tool on one endpoint

Lazagne post-exploitation tool on one endp...

Attack story Alerts (1) Devices (1) Users (0) Apps (0) **Evidence and Response (6)** Summary

All evidence (6)

	First seen	Entity	Verdict	Remediation
10/7/2022, 7:23 P...	lazagne.NaYmZata.exe.part	Suspicious		
10/7/2022, 7:22 P...	unconfirmed 209949.crdownload	Suspicious		
10/7/2022, 7:22 P...	09f70edd-519e-4e20-8bfd-c78c38e23a84.t...	Suspicious		
10/7/2022, 7:21 P...	unconfirmed 724637.crdownload	Suspicious		
10/7/2022, 7:19 P...	Unconfirmed 729013.crdownload	Suspicious		
10/7/2022, 7:19 P...	Unconfirmed 171203.crdownload	Suspicious		

lazagne.NaYmZata.exe.part

File Suspicious

+ Add Allowed/Blocked list rule for this file

File details

Verdict	● Suspicious
Device	SARAH-AKEAKE
File Name	lazagne.NaYmZata.exe.part
File Path	C:\Users\User\Downloads\lazagne.NaYmZata.exe.part
File Size	6.64 MB
Directory	C:\Users\User\Downloads
Hashes	Show Hashes
Virus Total	50/72

Virus Total

Malware detected

Malware: HackTool:Win32/LaZagne

mvpskill
change the world by contributions

M> THCS

Spark Tech Thailand



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

The screenshot shows the Microsoft Defender for Endpoint Action Center interface. On the left is a navigation sidebar with links like Home, Incidents & alerts, Actions & submissions, Submissions, Secure score, Learning hub, Trials, Partner catalog, Assets, and Devices. The main area is titled "Action Center" and "History". It lists six actions taken by user "SARAH-AKEAKE" and "sarah.h@akeake.com" over a 6-month period. The actions are: "Start antivirus scan" on 11/24/2022 at 4:59 PM, "Quarantine file" on 10/7/2022 at 7:27 PM, "Quarantine file" on 8/3/2022 at 6:13 PM, "Quarantine file" on 8/3/2022 at 6:13 PM, "Quarantine file" on 8/3/2022 at 6:13 PM, and "Quarantine file" on 8/3/2022 at 5:54 PM. The right side of the interface shows a table with columns for Action update time, Action type, Details, Asset, Decision, and Decided by. The last row in the table is highlighted with a blue border.

Action update time	Action type	Details	Asset	Decision	Decided by
11/24/2022, 4:59 PM	Start antivirus scan		sarah-akeake	sarah.h@akeake.com	Approved Automation
10/7/2022, 7:27 PM	Quarantine file	c:\users\user\downloads\unconfirmed 724637.crdownload	SARAH-AKEAKE	Approved Automation	
8/3/2022, 6:13 PM	Quarantine file	c:\users\user\downloads\techsmith snagit 13.0.1 build 6	SARAH-AKEAKE	Approved Automation	
8/3/2022, 6:13 PM	Quarantine file	c:\users\user\downloads\wrar550.exe	SARAH-AKEAKE	Approved Automation	
8/3/2022, 6:13 PM	Quarantine file	c:\users\user\downloads\utorrent.exe	SARAH-AKEAKE	Approved Automation	
8/3/2022, 5:54 PM	Quarantine file	c:\program files\qbittorrent\qbittorrent.exe	SARAH-AKEAKE	Approved Automation	Microsoft Defender AV



Defender for Cloud Apps

Access Policy

Instruction to review sessions in real-time:

The screenshot shows the Azure portal interface for creating a Conditional Access policy. The top navigation bar includes 'Azure Active Directory', 'Cloud App Security', and 'Cloud App Discovery'. The main title is 'Create CA Policy with Session > App Control'.

Name *: App control test

Assignments: 0 users or workload identities selected

Cloud apps or actions: No cloud apps, actions, or authentication contexts selected

Conditions: 0 conditions selected

Access controls: 0 controls selected

Session: 0 controls selected

A dropdown menu under 'Session' is open, showing the following options:

- Use Conditional Access App Control
 - Monitor only (Preview)
 - Block downloads (Preview)
 - Use custom policy...
- Sign-in frequency
- Persistent browser session
- Customize continuous access evaluation
- Disable resilience defaults

A tooltip message states: "This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more."

The screenshot shows the Microsoft 365 Defender portal with the URL https://security.microsoft.com/cloudapp... in the address bar. The top navigation bar includes icons for back, forward, home, and search, along with a notification count of 21.

The main title is 'Microsoft 365 Defender' and the sub-page is 'Policies > Create access policy'.

The left sidebar lists various monitoring and reporting options:

- Cloud apps
- Cloud discovery
- Cloud app catalog
- OAuth apps
- App governance
- Files
- Activity log
- Governance log

The right side of the screen is titled 'Create access policy' and contains the following fields:

- Policy name ***: (empty input field)
- Policy severity ***: (empty input field)
- Category ***: Access control (with three colored severity indicators)
- Description**: (empty input field)

A warning message at the bottom states: "⚠️ You don't have any apps deployed with Conditional Access App Control. Go to the Conditional Access App Control page to deploy an app."





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.

The screenshot shows the Microsoft 365 Defender Threat Explorer interface. On the left, there's a navigation bar with 'Assets', 'Identities', 'Email & collaboration', 'Investigations', and 'Explorer' (which is selected and highlighted with a blue border). In the center, there's an 'Explorer' section with tabs for 'All email', 'Malware', 'Phish', 'Campaigns', and 'Content Malware'. Above this, there's a 'MDE Settings' button. At the bottom, there's a 'Settings' section with 'General' and 'Advanced features' (which has a red arrow pointing to it).

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.

Select Technique

Select the social engineering technique you want to use with this simulation. We've curated these from the MITRE Attack framework. Depending on your selection, you will be able to use certain types of payloads.

- **Credential Harvest**
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a web site, the website often...
[View details of Credential harvest](#)
 - **Malware Attachment**
In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment, typically some arbitrary code such as a macro...
[View details of Malware attachment](#)
 - **Link in Attachment**
In this type of technique, which is a hybrid of a Credential Harvest and Malware Attachment, a malicious actor creates a message, with a URL in an attachment, and then inserts the attachment into the message. When the target opens the attachment, they are represented with a URL in the actual attachment...
[View details of Link in attachment](#)
 - **Link to Malware**
In this type of technique, a malicious actor creates a message, with an attachment added to the message. However instead of directly



3 Attack

⚠ You must enable multi-factor authentication (MFA) to schedule or terminate attacks. [Learn more about enabling MFA.](#)

Next

Save and close

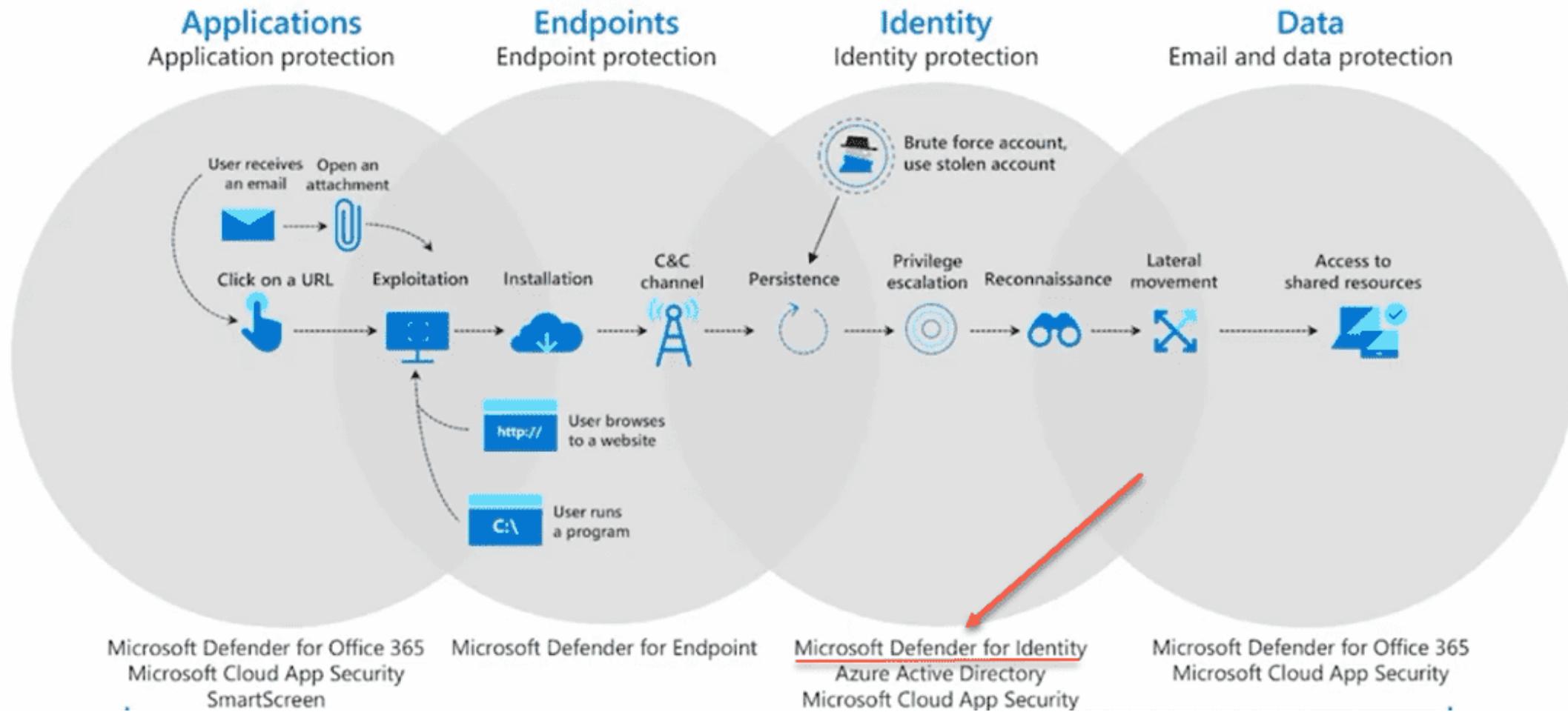
Cance





Defender for Identity

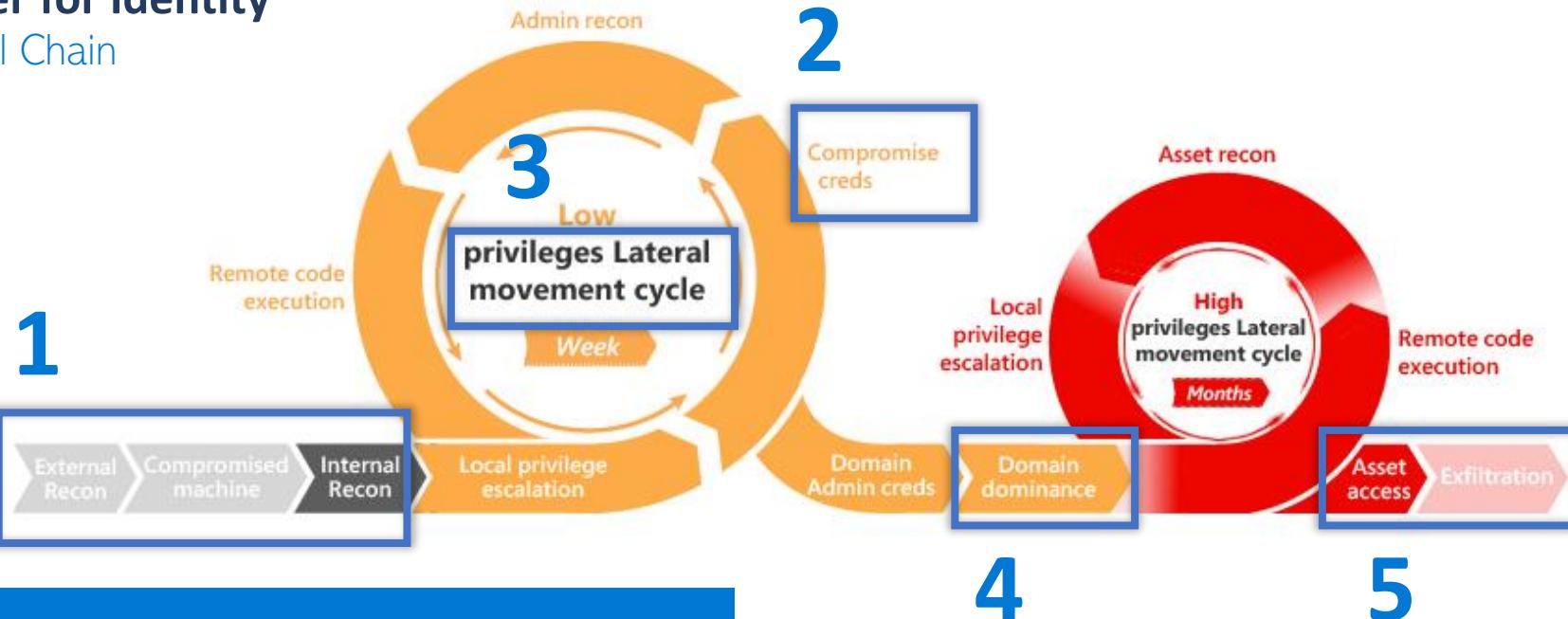
Defense Stack





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

4: Domain Dominance

DCShadow, DCSync, Golden Ticket, Skeleton Key

5

5: Exfiltration

Exfil over SMB, DNS



Defender for Identity

Windows Event Collection

Some requires configure "Advance Audit Policy" in DC

Such as "NTLM" logon

Group Policy Management Editor

The screenshot shows the 'Group Policy Management Editor' window. On the left is a tree view of policy settings under 'Default Domain Controllers Policy [DC1.DOMAIN1.TEST.LOCAL] Policy'. The 'Audit Policies' section is expanded, showing 'Account Logon' and 'Account Management'. The 'Account Management' node is highlighted with a red box. On the right, a detailed view of 'Audit Security Group Management Properties' is shown. It has tabs for 'Policy' (selected) and 'Explain'. Under 'Audit Security Group Management', there is a lock icon. A checkbox labeled 'Configure the following audit events:' is checked, with two sub-options: 'Success' and 'Failure', both of which are also checked and highlighted with a red box. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Not Configured
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Not Configured
Audit User Account Management	Not Configured



MS Sentinel

Getting Start

Create Log Analytic Workspace: as datalake from connectors

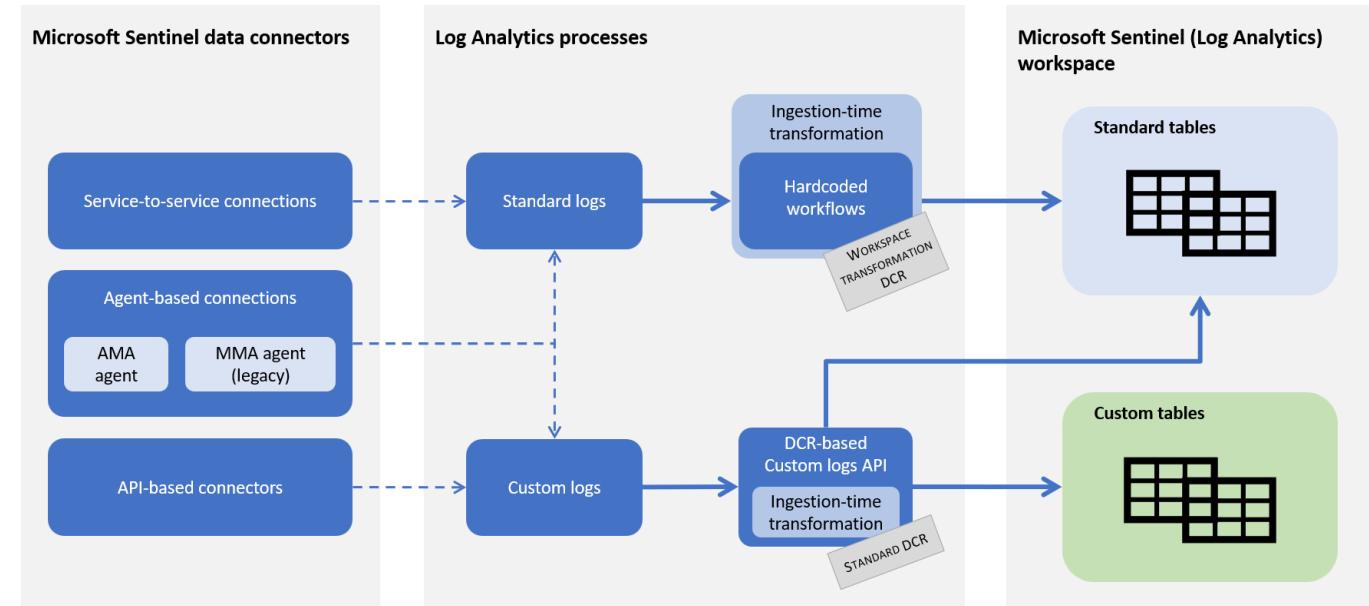
Create MS Sentinel on that Workspace

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)





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.

Active rules Rule templates Anomalies

Search Add filt...

Severity ↑↓	Name ↑↓	Rule type ↑↓
High	IN USE Advanced Mult...	Fusion
High	Create incidents based ...	Microsoft Secur...
High	Create incidents based ...	Microsoft Secur...
High	Create incidents based ...	Microsoft Secur...
High	Create incidents based ...	Microsoft Secur...
High	Create incidents based ...	Microsoft Secur...
High	Create incidents based ...	Microsoft Secur...
Medium	(Preview) Anomalous S...	ML Behavior An...
Medium	(Preview) Anomalous R...	ML Behavior An...

Advanced Multistage Attack Detect...

High Severity Fusion Rule Type

To enable these detections, we recommend you configure the following data connectors for best results:

- Out-of-the-box anomaly detections
- Azure Active Directory Identity Protection
- Azure Defender
- Azure Defender for IoT
- Microsoft 365 Defender
- Microsoft Cloud App Security
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Scheduled analytics rules, both built-in and those created by your security analysts. Analytics rules must contain kill-chain.

Note:
• This template can only be used once.

resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'sarahsentinel365dev'

Search Create Refresh Analytics efficiency workbook (Preview) Enable Disable Delete

Overview Logs News & guides Search Threat management Incidents Workbooks Hunting Notebooks Entity behavior Threat intelligence MITRE ATT&CK (Preview)

2 Active rules More content at Content hub

Rules by severity

High (1) Medium (0) Low (1) Informational (0)

LEARN MORE About analytics rules

Failed login attempts to Azure Portal

Low Severity Custom Content source Enabled Status

Tactics and techniques

Credential Access (1)

Active rules Rule templates Anomalies

Search Add... More (0)

Severity ↑↓ Name ↑↓ Rule type ↑↓

Severity	Name	Rule type
High	Advanced Multistag...	Fusion
Low	Failed login attempt...	Scheduled

Rule query

```
let timeRange = 1d;
let lookBack = 7d;
let threshold_Failed = 5;
let threshold_FailedwithSingleIP = 20;
```

Rule frequency
Run query every 1 day

Rule period
Last 7 days data

Rule threshold
Trigger alert if query returns more than 0 results

Edit Compare with template

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 to 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 screenshot shows the Azure Active Directory admin center with the URL https://aad.portal.azure.com/. The page is titled "Conditional Access | Policies". A new policy is being created, named "New Conditional Access policy". The "Session" tab is selected. The "Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies." section is visible. Under "Assignments", there are sections for "Users or workload identities" (0 users or workload identities selected) and "Cloud apps or actions" (1 app included). Under "Conditions", 0 conditions are selected. Under "Access controls", "Grant" is selected with 0 controls selected. Under "Session", 0 controls are selected. On the right, a sidebar provides information about session controls and links to learn more.



The Compliance policy settings are configured as shown:

Mark devices with no compliance policy assigned as

Not compliant

(i)

Enhanced jailbreak detection

Disabled

Compliance status validity period (days)

30

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.	<input type="radio"/>	<input type="radio"/>
On March 6, 2020, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On March 12, 2020, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

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.

The screenshot shows the Microsoft Azure portal interface. The left sidebar lists various services: Create a resource, Home, Dashboard, All services, FAVORITES (All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers), Policies, Insights and reporting, Diagnose and solve problems, Manage (Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication context), Expiry, Thumbprint, Download certificate, and Download certificate. The 'VPN connectivity' section is currently selected. At the top right, there is a search bar, a user profile, and several icons. A message at the bottom right of the main content area says: "Once a VPN certificate is created in the Azure portal, Azure AD will start using it immediately to issue short lived certificates to the VPN client. It is critical that the VPN certificate be deployed immediately to the VPN server to avoid any issues with credential validation of the VPN client."

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

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 Area

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?

Stages	Answer Area
Compromised credentials	Suspected Netlogon privilege elevation attempt: <input type="text"/>
Domain dominance	Suspected Kerberos SPN exposure: <input type="text"/>
Lateral movements	
Reconnaissance	Suspected DCSync attack: <input type="text"/>

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

The screenshot shows the 'Enterprise applications | Sign-in logs' page in the Azure Active Directory admin center. The left sidebar includes sections for Overview, Manage (All applications, Application proxy, User settings, Collections), Security (Conditional Access, Consent and permissions), and Activity (Sign-in logs, Usage & insights). The main area displays a table of sign-in logs for the last 7 days. The columns include Date, Request ID, User, Application, Status, IP address, Location, and Conditional Acc... (partially visible). The table shows multiple successful sign-ins from the same user (Nol 121) using various applications like Office365 Shell WCS... and Exchange Admin Ce... from the same IP address (49.228.233.73) in Bangkok, Krung The... The 'Sign-in logs' link in the sidebar is highlighted.

Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...
11/24/2022, 8:53:00 ...	9ca64337-1d78-402...	Nol 121	Office365 Shell WCS...	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:53:00 ...	9d31e83e-94c4-44d...	Nol 121	Office365 Shell WCS...	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:53:00 ...	01338a3a-0088-43e...	Nol 121	Office365 Shell WCS...	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:52:56 ...	5943e281-86ab-406...	Nol 121	Exchange Admin Ce...	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:48:15 ...	d213cec1-beec-483a...	Nol 121	Azure Portal	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:48:08 ...	74ce838e-0926-440...	Nol 121	Office365 Shell WCS...	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:48:08 ...	c4ba4533-89d4-4af3...	Nol 121	Office365 Shell WCS...	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:48:07 ...	bd530a55-4d42-4d6...	Nol 121	Office365 Shell WCS...	Success	49.228.233.73	Bangkok, Krung The...	Not Applied
11/24/2022, 8:33:04 ...	228cf93-8395-49ff...	Nol 121	Azure Portal	Success	49.228.233.73	Bangkok, Krung The...	Not Applied

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

The screenshot shows the Azure Active Directory admin center with the URL https://aad.portal.azure.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade. The left sidebar shows 'Dashboard', 'All services', and 'FAVORITES' (Azure Active Directory, Users, Enterprise applications). The main content area is titled 'Conditional Access policy' and describes controlling access based on signals from conditions like risk, device platform, location, client apps, or device state. It includes sections for 'Name' (TestModernApp), 'User risk' (Not configured), 'Sign-in risk' (Not configured), 'Device platforms' (Not configured), 'Locations' (Not configured), 'Cloud apps or actions' (No cloud apps, actions, or authentication contexts selected), 'Conditions' (0 conditions selected), 'Access controls' (0 controls selected), and 'Session' (0 controls selected). On the right, the 'Client apps' section is selected, showing configuration for modern authentication clients (Browser, Mobile apps and desktop clients) and legacy authentication clients (Exchange ActiveSync clients, Other clients). The 'User risk' field is set to 'Not configured'. The 'Sign-in risk' field is also 'Not configured'. Under 'Conditions', there are no conditions selected. Under 'Access controls', there are 0 controls selected. Under 'Session', there are 0 controls selected.

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.

Actions	Answer Area
Turn on Microsoft Graph data connect.	
Add Azure Sentinel.	
Create a SQL pool in Azure Synapse Analytics. 	 
Connect a data connector. 	
Create an Azure Log Analytics workspace.	
Create an Azure Data Lake Analytics account.	

Answer Area

Turn on Microsoft Graph data connect.

Add Azure Sentinel.

Create a SQL pool in Azure Synapse Analytics.
Connect a data connector.


Create an Azure Log Analytics workspace.

Create an Azure Data Lake Analytics account.

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.

Call the logic app:

An entity mapping
A hunting query
A notebook
A playbook
A workbook

Displays statistics for risky sign-ins:

An entity mapping
A hunting query
A notebook
A playbook
A workbook

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

The screenshot shows the Azure Active Directory admin center interface. The left sidebar has a 'FAVORITES' section with 'Azure Active Directory' selected. The main content area is titled 'Devices | Device settings'. It displays sections for 'Overview', 'All devices', 'Device settings' (which is selected), 'Enterprise State Roaming', 'BitLocker keys (Preview)', and 'Diagnose and solve problems'. Below these are sections for 'Activity' (Audit logs, Bulk operation results (Preview)) and 'Troubleshooting + Support' (New support request). At the bottom, there's a setting for 'Maximum number of devices per user' set to 50, which is highlighted with a blue border. The URL in the browser is https://aad.portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuB...

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes back, forward, home, and search icons, along with the URL https://admin.microsoft.com. The title bar says 'Microsoft 365 admin center'. On the right, there's a sidebar for 'Sarah AHA co...' with options like 'Add card' and 'Microsoft 365'. The main content area is titled 'Admin centers' and lists several services: Security, Compliance, Endpoint Manager, Azure Active Directo..., Exchange, SharePoint, Teams, and 'All admin centers'. The 'All admin centers' option is highlighted with a blue border. The URL in the browser is https://admin.microsoft.com.

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

The screenshot shows the Exchange admin center interface. The left sidebar has a 'Mobile' section with 'Mobile device access' selected. The main content area is titled 'Device access rules'. It contains a paragraph about Exchange ActiveSync quarantining unmanaged mobile devices and an 'Edit' button. Below this are links for 'Quarantined Devices' and 'Device access rules'. The top navigation bar shows the URL https://admin.exchange.... and various icons.

Exchange ActiveSync access settings

Connection Settings

When mobile devices of the selected family or model try to connect:

- Allow access
- Block access
- Quarantine - Let me decide to block or allow later

Quarantine Notification Email Messages

Select administrators to receive email messages when a mobile device is quarantined:

 sarah@thaicysec.com X Search name or email

Text to include in messages sent to users whose mobile device is in quarantine, blocked, or in the process of being identified:

โดยบล็อกเพราะไม่ได้ใช้อุปกรณ์ที่เอนໂຣລໄວນະຄະ

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

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a tree view with categories like Teams & groups, Roles, Resources, Billing, Support, Settings (which is selected and highlighted with a blue box), Domains, Search & intelligence, Org settings (which is also selected and highlighted with a blue box), Integrated apps, Partner relationships, Setup, Reports, Health, Admin centers, Security, Compliance, and Endpoint Manager. The main content area is titled "Org settings" and shows a sub-section titled "Password expiration policy". It says, "The policy you choose here applies to everyone in your organization." Below this is a checkbox labeled "Set passwords to never expire (recommended)". A text input field is set to "100", indicating the number of days before passwords expire. The URL in the browser bar is https://admin.microsoft.com/Adminportal/Home#/Settings/SecurityPrivacy/:/Settings/L1/Password... .

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

The screenshot shows the Microsoft 365 admin center interface. On the left, the navigation menu is visible with 'Roles' selected and 'Role assignments' highlighted. In the main area, the 'Role assignments' page is displayed under the 'Azure AD' tab. A list of roles is shown, with 'Service Support Administrator' selected and checked. A modal window titled 'Add users' is open over the list, showing a search result for 'Grady Archie'. The user's name and email ('Grady Archie' and 'GradyA@nol121.onmicrosoft.com') are listed with a checkbox next to it. Other users listed in the dropdown include 'Arm Valanchai (THCS)' and 'Ken (THCS)'. The 'Assigned' tab is selected in the modal window.

SC-900

SECURITY
COMPLIANCE
IDENTITY



With On-Prem 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.



SC-900

SECURITY
COMPLIANCE
IDENTITY



Recommendations ...



Name ↑	Max score ↑	Current score ↑	Potential score increase ↑	Status ↑	Unhealthy resources
Enable MFA	10	0.00	+ 20%	● Unassigned	1 of 1 resources
Secure management ports	8	0.00	+ 16%	● Unassigned	1 of 1 resources
Apply system updates	6	0.00	+ 12%	● Unassigned	1 of 1 resources
Intermediate vulnerabilities	6	0.00	+ 12%	● Unassigned	1 of 1 resources
Manage access and permissions	4	4.00	Completed	0 of 1 resources	

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

Microsoft Defender for Cloud | Security posture

Showing 2 subscriptions

Search (Ctrl+ /) Secure score over time Governance report (preview) Guides & Feedback

General

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

Azure environment

Secure score 8% SECURE SCORE

Environment

Management groups 0 Subscriptions 1

Unhealthy resources 2/4 Recommendations 17

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	8%	2 of 2	View recommendations >

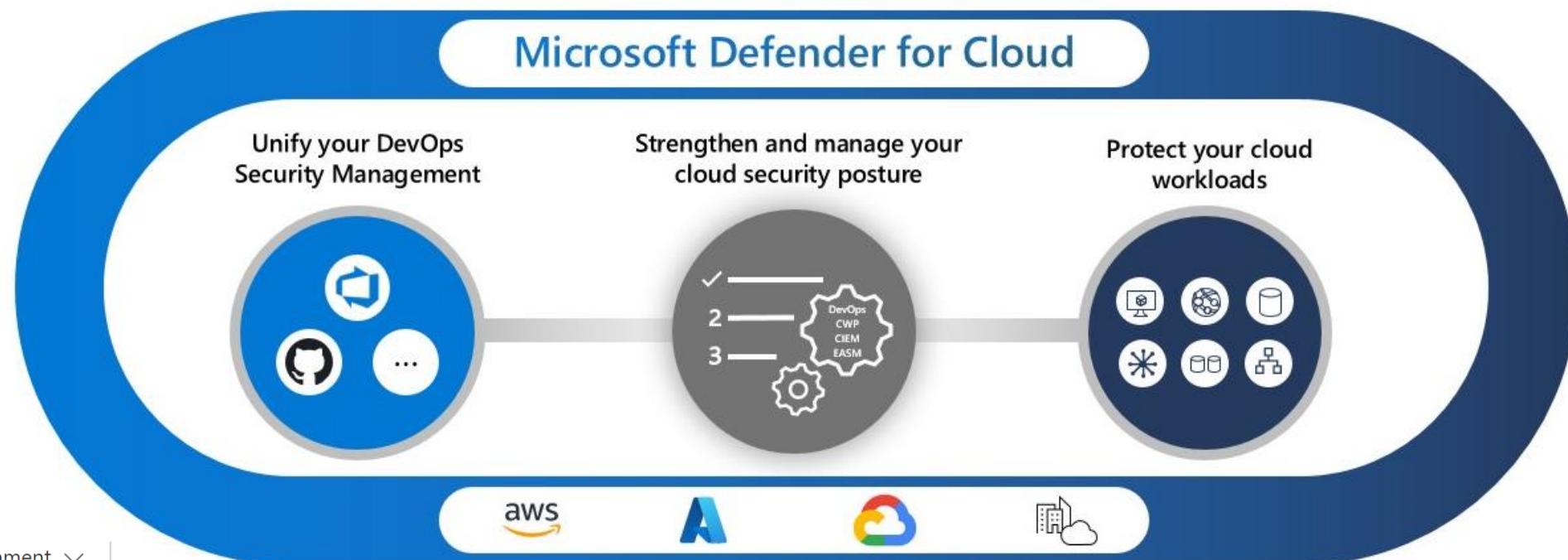
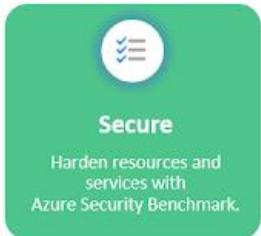




Azure
Security
Technologies



Defender
for Cloud (MDC)



DevSecOps

Code Pipeline Sec

CSPM

Foundation (FREE)
Defender (Premium)

CWPP

ITGeist

mvp skill
change the world by contributions

M>

THCS

Spark Tech Thailand

DevOps environments in Defender for Cloud

Home > Microsoft Defender for Cloud

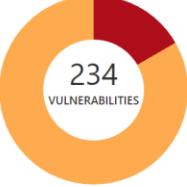
Microsoft Defender for Cloud | DevOps Security (Preview) X

Showing 2 subscriptions | PREVIEW

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)
- Workbooks
- Community
- Diagnose and solve problems

Security Overview

DevOps security vulnerabilities (39 High, 195 Medium, 0 Low) 

Vulnerability Type	Count
High	39
Medium	195
Low	0

DevOps security results

Category	Count
Code scanning vulnerabilities	169
Exposed Secrets	18
OSS vulnerabilities	31
Recommendations	28

DevOps coverage

Connector Type	Count
Github Connectors	1
Azure DevOps Connectors	1

Total 30 

Resource Types == Github Repository, Azure DevOps Repository

Subscription	Pull request status	Total exposed secrets	OSS vulnerabilities	Total code scanning vulnerabilities
ASE_SG_Demo	N/A	Unhealthy (1)	1	65
RS_ramontest	N/A	Unhealthy (1)	0	65
DfDDemo	N/A	Unhealthy (4)	17	16
Toy-Website	N/A	Unhealthy (2)	0	0
Contoso Hotels	On	Unhealthy (1)	N/A	0
RepositoriesSampleContent	N/A	Healthy	0	0
Toy-Website	On	Healthy	N/A	0
DfD Demo	On	Healthy	N/A	0

Page 1 of 1

Cloud workload protection

Microsoft Defender for Cloud | Overview

Showing 59 subscriptions

Search (Ctrl+ /) Subscriptions What's new

General

- Overview
- Getting started
- Recommendations
- Security alerts**
- Inventory
- Community

Cloud Security

- Secure Score
- Regulatory compliance
- Workload protections
- Firewall Manager

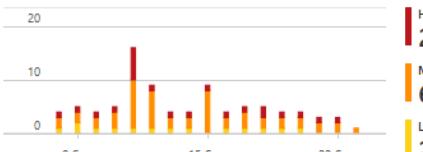
Management

- Environment settings
- Security solutions
- Workflow automation

59 Azure subscriptions **1** AWS accounts **4** GCP projects **161** Active recommendations **121** Security alerts

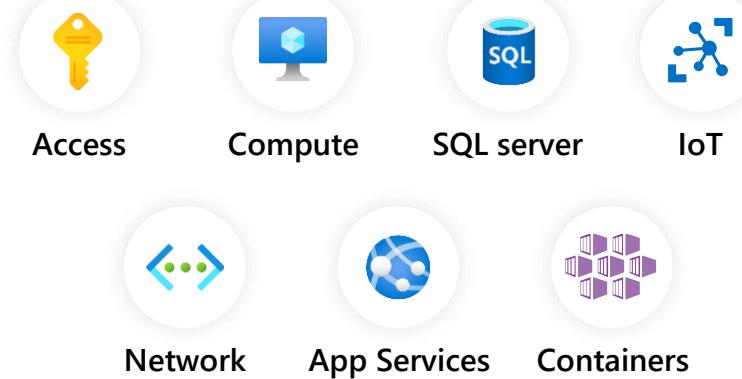
Secure score
Current secure score
60% 3626 POINTS
COMPLETED Controls 1/16
COMPLETED Recommendations 29/190
[Improve your secure score >](#)

Regulatory compliance
Current compliance by passed controls
UKO and U... 0/7
SOC TSP 1/13
NIST SP 80... 2/23
HIPAA HITR... 2/22
NIST SP 80... 3/29
[Improve your compliance >](#)

Workload protections
Resource coverage 95% For full protection, enable 10 resource plans
Alerts by severity

[Enhance your threat protection capabilities >](#)

Inventory
Unmonitored VMs 60 To better protect your organization, we recommend installing agents
Total Resources 3900
Unhealthy (2936) Healthy (679) Not applicable (285)
[Explore your resources >](#)

Evaluated categories



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

Evaluated categories



Access



Compute



SQL server



IoT



Network



App Services



Containers

Manage and Assign Security Alerts

Security alerts

Refresh Change status Open query Suppression rules Security alerts map (Preview) Create sample alerts

Active alerts 644 Affected resources 34

Active alerts by severity

High (166) Medium (414) Low (64)

Search by ID, title, or affected resource Status == Active Severity == Low, Medium, High Time == Last month

Severity	Alert title	Affected resource	Activity start time (UTC+2)	MITRE ATT&CK® tactics
High	Suspicious process executed [seen ...]	CH-VictimVM00-Dev	11/22/20, 3:00 AM	Credential Access
High	Suspicious process executed [seen ...]	CH-VictimVM00	11/22/20, 1:00 AM	Credential Access
High	Suspicious process executed [seen ...]	dockervm-redhat	11/21/20, 3:00 AM	Credential Access
High	Suspicious process executed [seen ...]	dockeroniaasdemo	11/21/20, 1:00 AM	Credential Access
High	Suspicious process executed [seen ...]	samplecrmwebblobstor...	11/20/20, 7:00 AM	Credential Access
High	Suspicious process executed	dockervm-redhat	11/20/20, 6:00 AM	Credential Access
High	Suspicious process executed	dockervm-redhat	11/20/20, 5:00 AM	Credential Access
High	Microsoft Defender for Cloud test ale...	ASC-AKS-CLOUD-TALK	11/20/20, 3:00 AM	Persistence
High	Exposed Kubernetes dashboard det...	ASC-WORKLOAD-PRO...	11/20/20, 12:00 AM	Initial Access
High	Suspicious process executed [seen ...]	CH-VictimVM00-Dev	11/19/20, 7:00 PM	Credential Access

No grouping

High Exposed Kubernetes dashboard detected ASC-AKS-CLOUD-TALK 11/05/20, 1:58 PM

High Microsoft Defender for Cloud test alert... ASC-AKS-CLOUD-TALK 11/04/20, 11:50 AM

High Exposed Kubernetes dashboard detect... ASC-AKS-CLOUD-TALK 10/26/20, 10:44 PM

Search by ID, title, or affected resource Status == Active Severity == High Time == Last month

Excluded Kubernetes dashboard detected

High Active 11/05/20, 13:58

Alert description

Kubernetes audit log analysis detected exposure of the Kubernetes Dashboard by a LoadBalancer service. Exposed dashboard allows an unauthenticated access to the cluster management and poses a security threat.

Affected resource

ASC-AKS-CLOUD-TALK Kubernetes service
ASC DEMO Subscription

MITRE ATT&CK® tactics

- Initial Access

View full details Take action

< Previous Page 1 of 17 Next >



Defender for Cloud (MDC)

Cloud Security Posture Management (CPSM)

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

Visual Studio Enterprise Subscription

Save Settings & monitoring

Settings

Defender plans

Email notifications

Workflow automation

Integrations

Continuous export

...

Select Defender plan

Enable all

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >	N/A	Full	<input checked="" type="checkbox"/> On
Defender CSPM	Free (during preview) Details >	N/A	Partial	<input type="checkbox"/> Off

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



Defender
for Cloud (MDC)



Azure
Policy

Cloud Security Posture Management (CPSM)

Policy | Compliance

Search



Assign policy

Assign initiative



Refresh

Overview

2 selected

All definition types

All compliance states

Filter by name or ID...

Getting started

Compliance

Remediation

Events

Authoring

Definitions

Assignments

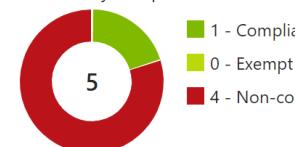
Exemptions

Overall resource compliance

20%

1 out of 5

Resources by compliance state



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 (subscription)	Visual Studio Enterpr...	✗ Non-compliant	25% (1 out of 4)	3	10
----------------------------	--------------------------	-----------------	------------------	---	----

ASC Default (subscription)	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

mvpSkill
change the world by contributions

M>

THCS

Spark Tech Thailand



Defender for Cloud (MDC)

Add Multicloud Environment with “Native” (agentless) Connector

Microsoft Defender for Cloud | Environment settings
Showing 2 subscriptions

Search Add environment Refresh Guides

Amazon Web Services Multi-cloud account manage

Cloud rules

Assign owners and set expected timeframes for recommendations

2 Azure subscriptions 0 AWS accounts

Search by name Environments == All

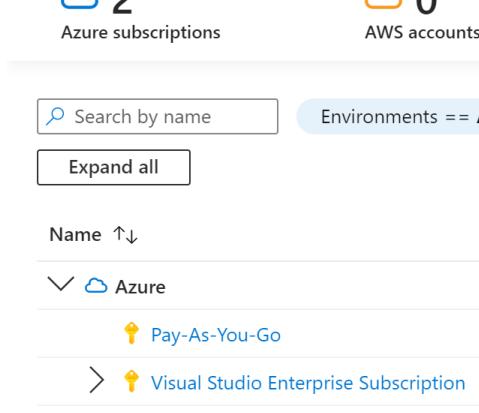
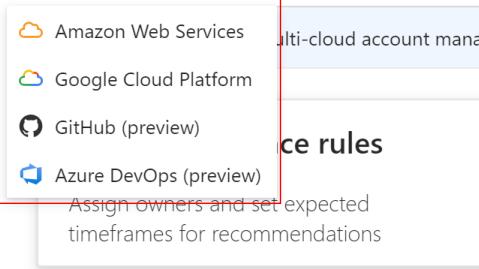
Expand all

Name ↑

✓ Azure Pay-As-You-Go Visual Studio Enterprise Subscription

Management

Environment settings Security solutions Workflow automation



Home > Microsoft Defender for Cloud | Environment settings >

AWS

Add account

Amazon Web Services

① Account details ② Select plans ③ Configure access ④ Review and generate

Enter a descriptive name for the cloud account connector and choose where to save the connector resource.

Connector name *

AWSenvTest

Onboard *

Management account Single account

Subscription *

Visual Studio Enterprise N. Virginia Sarah Hansakul

Resource group *

SarahLog Add widget Account ID: 36...1

Location *

West US 2 Account

AWS account Id *

3...1 Organization

Excluded accounts

Service Quotas Create new Service Quotas

Billing Dashboard Insert accounts to exclude Billing Dashboard

Security credentials Security credentials

ITGeist

mvpSkill
change the world by contributions

M>

THCS

Spark Tech Thailand



Defender for Cloud (MDC)

Add Multicloud Environment with “Native” (agentless) Connector

Home > Microsoft Defender for Cloud | Environment settings >

Add account

Amazon Web Services

✓ Account details

2 Select plans

3 Configure access

4 Review and generate

Select plans

i 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

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.

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

ITGeist

mvp skill
change the world by contributions

M>

THCS

Spark Tech Thailand



Add Multicloud Environment with “Native” (agentless) Connector

Home > Microsoft Defender for Cloud | Environment settings >

Add account

Amazon Web Services

Account details Select plans Configure access

Click to download the CloudFormation template

Click to download the CloudFormation template

Create Stack in AWS

First, deploy the CloudFormation template on the master account you wish to onboard. Next, deploy the CloudFormation StackSet.

1. Click 'Go to AWS'
2. In AWS, Select 'Create stack', 'With new resources (standard)'
3. Choose 'Upload a template file', 'Choose file' and select the downloaded template
4. Click 'Next' and 'Create stack'
5. **Navigate to CloudFormation 'StackSets'**
6. Click 'Create StackSet'
7. Choose 'Upload a template file', 'Choose file' and select the downloaded template
8. Click 'Next' and 'Submit'

[Go to AWS](#)

The screenshot shows the AWS CloudFormation StackSets page. At the top, there's a search bar with 'stackSets'. On the left, a sidebar lists 'Services (7)', 'Features (10)', 'Resources (New)', 'Blogs (428)', 'Documentation (10,501)', and 'Knowledge Articles (30)'. The main content area has a heading 'CloudFormation > StackSets'. Below it, a table shows 'StackSets (0)' with a 'Create StackSet' button highlighted with a red box. The 'Top features' section includes 'StackSets', 'Resource import', 'Stacks', 'Exports', and 'Designer'.

ITGeist

mvp skill
change the world by contributions

M>

THCS

Spark Tech Thailand

Add Multicloud Environment with “Native” (agentless) Connector

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>

Cancel

Next

Capabilities

AWS



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



Add Multicloud Environment with “Native” (agentless) Connector

Home > Microsoft Defender for Cloud | Environment settings >

GCP

Create GCP connector

Google cloud

Organization details Select plans

3 Configure access

4 Review and generate

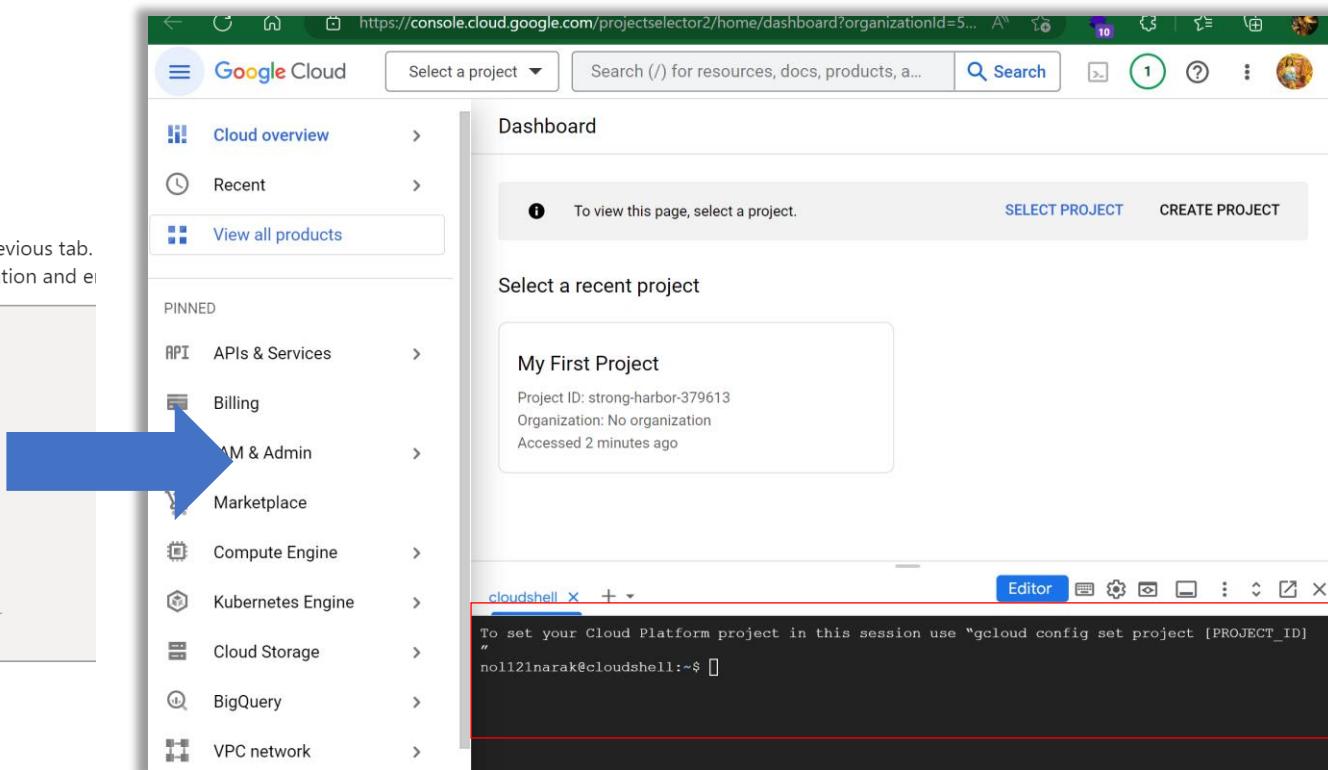
 Copy script to GCP Cloud Shell

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 enable access to the environment.

```
# 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"
WorkloadIdentityPoold="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

mvp skill
change the world by contributions

M>

THCS

Spark Tech Thailand



Similar to VA tool

*Price per Asset



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

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

“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

Confirmation

Custom Attack Surfaces take 24-48 hours to build as we scan our security gr...

Seeds

Type	Seed Name
Org Name	ThaiCySec
Domain	thaicysec.com

Back

Confirm



Attack Surface Summary

Domains

449.9K

Hosts

2.8M

Pages

894.6K

SSL Certs

2.6K

ASNs

68

IP Blocks

720

IP Addresses

2.4M

Contacts

1.2K

Attack Surface Priorities



8

High Severity Observations



4

Medium Severity Observations

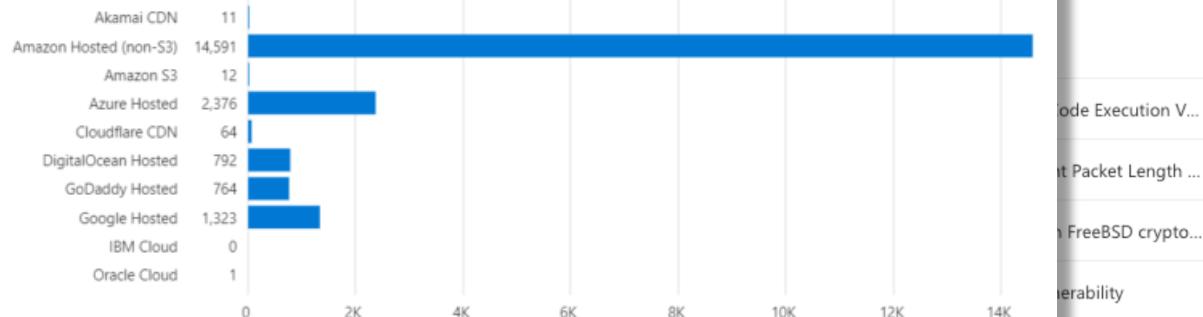


2

Low Severity Observations

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.



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

0

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

0

[All 77 Insights](#)

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

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	

ITGeist

SC-900

SECURITY
COMPLIANCE
IDENTITY

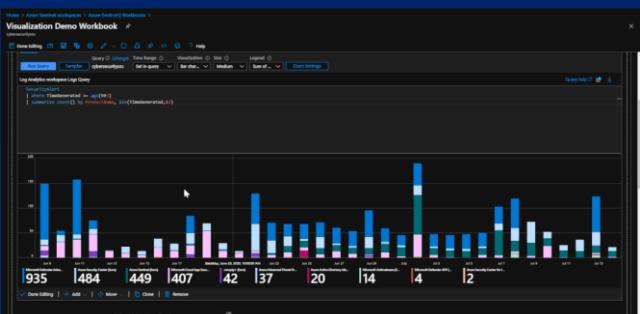


=

SIEM

Sec.Info+Event Mgmt

- Workbook > Visualize Data
 - Kusto Query



+ SOAR

Sec.Orchestrate+AutoRespond

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



https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/0/id/%2Fsubscriptions%2FresourceGroups%2F... Chat Compose

Microsoft Sentinel | Overview

Selected workspace: 'sarahrtestsentinel'

Search Refresh Last 24 hours

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incident
- Workbooks
- Hunting
- Notebooks
- Entity browser

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
AADMANAGEDID: 10
USAGE: 12

No data was found

Data source anomalies

Potential malicious events

POTENTIAL MALICIOUS EVENTS: 0

Democratize ML for your SecOps

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

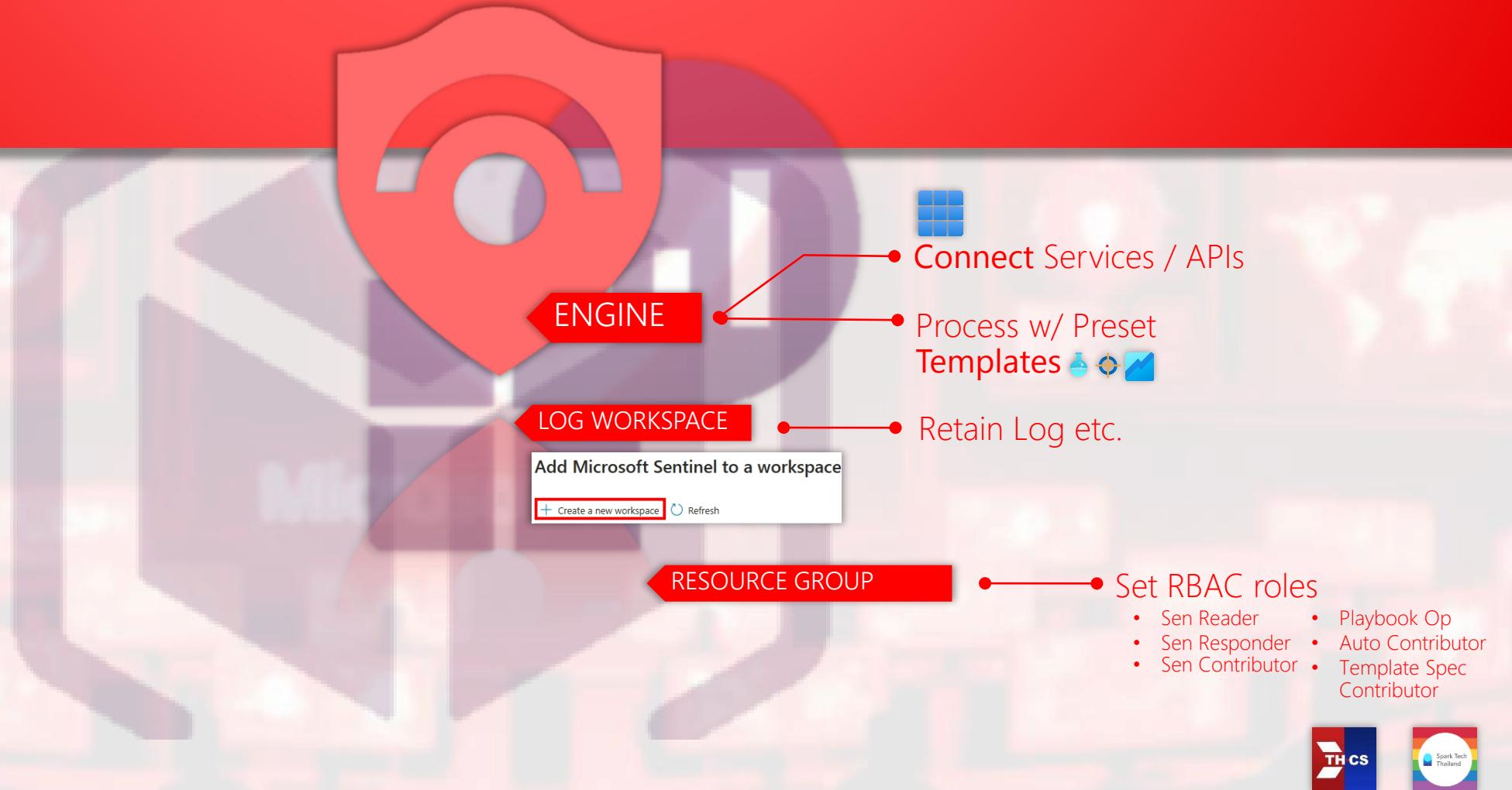
1 [learn.microsoft.com](#)

Stop Responding

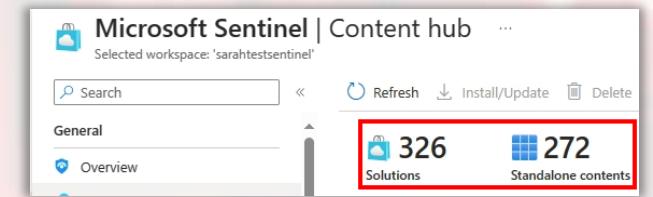
Ask me anything...

0/4000

Simplified Microsoft Sentinel



Simplified Microsoft Sentinel



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

Content is Connector + **TEMPLATES**

w/ Template Spec Contributor
Get "Content"
ENGINE



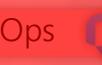
MUST "SAVE" / "CREATE" TO USE

Custom
REPOSITORIES

GitHub



Azure DevOps



Search

Refresh Install/Update Delete 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

326

Solutions

272

Standalone contents

2

Installed

1

Updates

Search...

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

<input type="checkbox"/>	Content title	Content source	Provider
<input type="checkbox"/>	SOC Handbook FEATURED	Solution	Community
<input type="checkbox"/>	Threat Int... FEATURED PREVIEW	Solution	Microsoft
<input type="checkbox"/>	UEBA Essentials FEATURED	Solution	Microsoft
<input type="checkbox"/>	VirusTotal FEATURED	Solution	VirusTotal
<input type="checkbox"/>	Workspace Usage Rep... FEATURED	Standalone	
<input type="checkbox"/>	42Crunch Microsoft Sentinel Connec...	Solution	42Crunch
<input type="checkbox"/>	A client made a web request to a po...	Standalone	
<input type="checkbox"/>	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

Standalone

Workspace Usage Report

sarahtestsentinel

 Auto refresh: Off

Subscription

Visual Studio Enterprise Subscription

Workspace

SarahTestSentinel

Time Range

Last 30 days

Select the data

Basic

Workspace Info

 Latency

Cost Analysis

Microsoft Sentinel

Regular Checks (D)

Log Analytics Workspace Name ↑↓

Resource Group ↑↓

location ↑↓

Data Retention(days) ↑↓

Latency ↑↓

SarahTestSentinel

sentineltest

eastus2

30

Group: Workspace info: SarahTestSentinel

Status for Last 30 days, Billable Tables have an average use of:

Search

Table Name ↑↓ IsBillable ↑↓ Table S

AADNonInteractiveUserSignInLogs

True

AADManagedIdentitySignInLogs

True

SignInLogs

True

AuditLogs

True

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

Status
Not savedDescription
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

Workbooks

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

Standalone



or Last 30 days

Workspace Usage Report - sarahtestsentinel

sarahtestsentinel



Workspace Usage Report

Change Log

Use this report to analyze 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, minimum and maximum values

Standalone

Microsoft Sentinel | Content hub

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

Workspace Usage Report - sarahtestsentinel

sarahtestsentinel

Standalone

Done Editing Open F Settings P Power BI D Refresh A Alert S Share Latency C Cost Analysis M Microsoft Sentinel

Workspace Usage Report

Change Log

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

Version	Description
v1.1	Added Events Per Second (EPS) to Workspace Info Tab.

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

Workspace Usage Report - sarahtestsentinel

sarahtestsentinel

Edit Open F Refresh A Alert S Share Latency C Cost Analysis M Microsoft Sentinel

Sarah! Subscription? My beauty, Workspace?

Visual Studio Enterprise Subscription SarahTestSentinel

Time Range Last 30 days

Workspace Info Latency Cost Analysis Microsoft Sentinel

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

Done Editing Open F Settings P Power BI D Refresh A Alert S Share Latency C Cost Analysis M Microsoft Sentinel

1 Editing parameters item: parameters - 1

Settings Advanced Settings Style </> Advanced Editor

Add Parameter Standard Style

Required? Parameter name Display name

DefaultSubscription_Internal Sarah! Subscription?

Subscription Workspace My beauty, Workspace?

resourceGroup TimeRange Time Range

TimeRange Last 30 days

Latency

Cost Analysis

Microsoft Sentinel

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

Simplified Microsoft Sentinel



ENGINE

w/ Template Spec Contributor
In Subscription RBAC level
Get "Content"

Data Connector



OOTB

CONTENT HUB

Solution

All-in-"One Click"

- Workbook
- Hunting Query
- Analytic Rule
- Watchlist
- Parser
- Playbook

Azure Activity

Microsoft Provider | Microsoft Support | 2.0.6 Version

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](#)

Content type ①

Analytics rule	12	Data connector	1	Hunting query	14
Workbook	1				

Category ①

IT Operations

Pricing ①

Free

Actions ▾

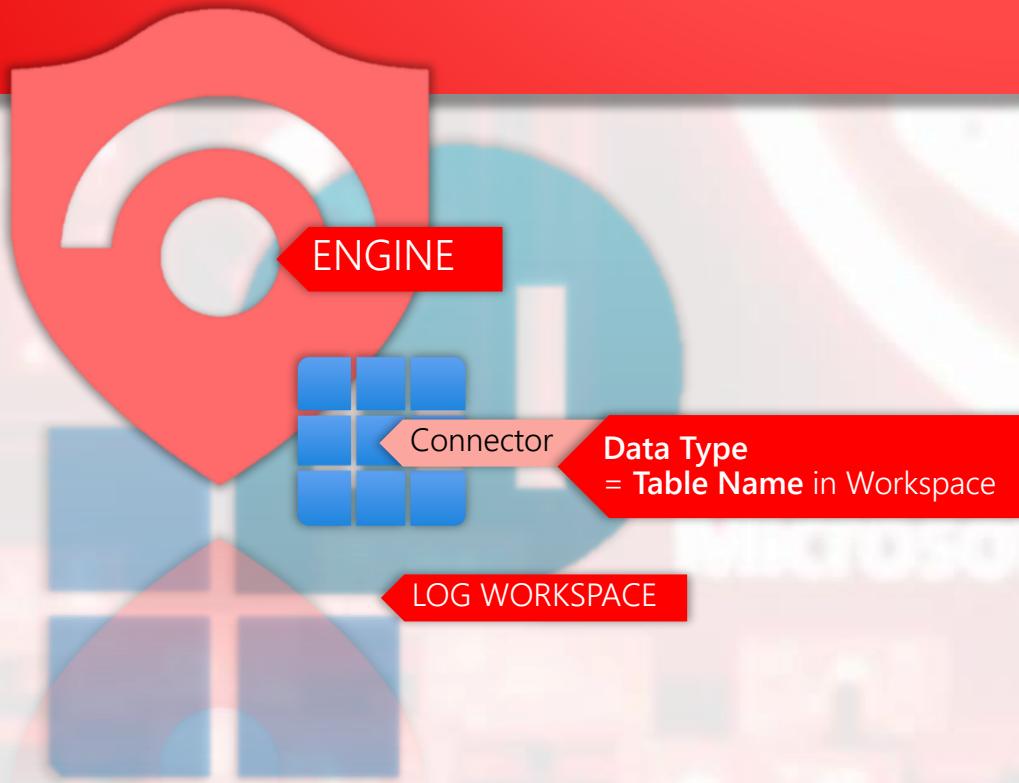
Manage

Install

[View details](#)



Simplified Microsoft Sentinel



Microsoft Sentinel | Data connectors

Selected workspace: 'saratestsentinel'

3 Connectors, 2 Connected

Azure Activity

Status	Connector name
Connected	Azure Activity Microsoft
Connected	Microsoft 365 Defender Microsoft

AzureActivity 17

Data types: AzureActivity 11/7/2023, 2:46:27 PM

Logs

New Query 1*

```
1 AzureActivity
2 | summarize Time = max(TimeGenerated)
3 | where isnoteempty(Time)
```

Results

Time [UTC]
11/7/2023, 7:46:27.291 AM

Time [UTC] 2023-11-07T07:46:27.2915605Z

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

Workbook

Category ⓘ

IT Operations

Pricing ⓘ

Free

Manage

Actions

View details

Content name

Azure Activity	Connector	1 item	Data connector	2.0.0
NRT Azure Active Directory Hybrid Health AD FS New Server	Templates	--	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				

Created content Content type Version

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 Rules

1 Active rules
More content at Content hub
LEARN MORE About analytics rules

Rules by severity

High (1)	Medium (0)	Low (0)	Informational (0)								
Active rules Rule templates Anomalies											
<table border="1"> <thead> <tr> <th>Severity</th> <th>Name</th> <th>Rule type</th> <th>Data source</th> </tr> </thead> <tbody> <tr> <td>Medium</td> <td>NRT Azure Act...</td> <td>NRT</td> <td>Azure Activ</td> </tr> </tbody> </table>				Severity	Name	Rule type	Data source	Medium	NRT Azure Act...	NRT	Azure Activ
Severity	Name	Rule type	Data source								
Medium	NRT Azure Act...	NRT	Azure Activ								
<p>Description: This detection uses AzureActivity logs (Administrative category) to identify the creation or update of a server instance in an</p> <p>Note: You haven't used this template yet. You can use it to create analytics rules.</p> <p>Create rule</p>											



Azure Activity



W 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 ⓘ

Analytics rule

Data connector

Hunting query

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 Cloud Shell User

--

Analytics rule

2.0.2

Creation of expensive computes in Azure

--

Analytics rule

2.0.1

Resource non-compliant operation in Azure

--

Analytics rule

2.0.2

Suspicious Azure deployment

--

Analytics rule

2.0.2

NRT Creation of expensive computes in Azure

--

Analytics rule

2.0.1

Azure Active Directory Hybrid Health AD FS Suspicious Application

--

Analytics rule

2.0.1

Suspicious number of resource creation or deployment activities

--

Analytics rule

2.0.3

Azure Active Directory Hybrid Health AD FS New Server

--

Analytics rule

2.0.1

Azure Active Directory Hybrid Health AD FS Service Delete

--

Analytics rule

2.0.1

Mass Cloud resource deletions Time Series Anomaly

--

Analytics rule

2.0.2

Suspicious granting of permissions to an account

--

Analytics rule

2.0.1

Azure Network Security Group NSG Administrative Operations

--

Hunting query

2.0.1

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



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



If no Incident to study

Just **Create!**

The screenshot shows the Microsoft Sentinel Content Hub interface. It displays several pre-built content items:

- Azure Activity**: Microsoft Support, Version 2.0.6.
- Note: The** (partially visible note about issues pertaining to the solution).
- Diagnostic Settings**: Microsoft Support, Version 2.0.6.
- Data Connectors: 1, Workbooks: 1, Analytic Rules: 12, Hunting Queries: 14**: Summary statistics for the hub.
- Analytics rule**: 12 items.
- Data connector**: 1 item.
- Hunting query**: 14 items.
- Workbook**: 1 item.

At the bottom, there are buttons for **Manage**, **Actions**, and **Install**. The **Pricing** information indicates it is **Free**.



Simplified Microsoft Sentinel

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'sarahsentinel'

Search

Create incident (Preview)

4 Open incidents

General

Overview

Create incident (Preview)

Title *

Suspicious Login from Beautiful person Detected

Description

Login attempts from Sarah followed by a successful login from an beautiful IP address.

Severity *

High

Status *

New

Owner ⓘ

Sarah

Tags



Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

 Microsoft Sentinel | Incidents

Selected workspace: 'sarahsentinel'

The screenshot shows the Microsoft Sentinel Incident Page. At the top, there are four summary cards: 'Open incidents' (0), 'New incidents' (0), 'Active incidents' (0), and 'Open incidents by severity' (High: 0, Medium: 0, Low: 0, Informational: 0). Below these are search and filter controls, including a search bar ('Search by ID, title, tags, owner or product'), a severity dropdown ('Severity : All'), and a status dropdown ('Status : 2 selected'). A 'More (3)' link is also present. The main table lists incidents with columns for Severity, Incident ID, Title, Alerts, and Incident provider name. One incident is highlighted: 'Suspicious Login from Beautiful person Detected' (Incident ID: 1). The details pane on the right shows the incident's description: 'Login attempts from Sarah followed by a successful login from an beautiful IP address.', alert product names (empty), evidence (empty), last update time (03/27/24, 06:06 PM), creation time (03/27/24, 06:04 PM), entities (empty), incident workbook (empty), tags ('ForAzureConf2024'), and incident link (empty). The 'Delete incident' button in the incident card is highlighted with a red box.

Microsoft Security Community Thailand

https://portal.azure.com/#view/Microsoft_OperationsManagementSuite_Workspace/Logs.ReactView/initiator/ASI_Hunting/scope~/...

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Logs

SarahSentinel

New Query 1*

SarahSentinel

Run Time range : Set in query Save Share New alert rule Export Pin to Format query

Tables Queries Functions ...

Search Filter Group by: Category

Collapse all

- Failed login Count
- Failed MFA challenge
- Failed Signin reasons
- Failures updating Office365- Sharepoint related Sentinel...
- File name extension change
- File upload operation
- Files from malicious sender
- Firewall blocked request count per hour
- Firewall request count by host, path, rule, and action

Save as query Save as function

```
1 // Failed login Count
2 // Resources with most failed lo
3 SigninLogs
4 | where TimeGenerated > ago(30d)
5 | where ResultType !=0
6 | summarize FailedLoginCount=count() by ResourceDisplayName
7 | sort by FailedLoginCount desc nulls last
```

in the query. Overrides time picker in portal.

Results Chart

FailedLoginCount

ResourceDisplayName	FailedLoginCount
Windows Azure Ac...	13
Windows Azure Se...	6
OfficeHome	3
WindowsDefender...	1

Microsoft Sentinel | Hunting

Selected workspace: 'sarahsentinel'



Refresh

New hunt

Create incident



Delete

Colum

General

[Overview \(Preview\)](#)[Logs](#)[News & guides](#)[Search](#)

Threat management

[Incidents](#)[Workbooks](#)[Hunting](#)

1 / 1

Open / total hunts

0

Validated hypotheses

1

Incidents created

Hunts (Preview)

Queries

Livestream

Bookmarks

Search hunts

Add filter

 Hunt name

Status

Hypothesis

 ถึงให้ดูก็ดูไม่ออก

New

Unknown

Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >



ถึงให้ดูก็ดูไม่ออก

Incident number 5

Refresh

Delete incident



Logs



Tasks



Act

Medium

Severity

New

Status

Sarah

Owner

Workspace name
sarahsentinel

Description

หลอกคนเข้ามาเท่าไรในรั้ว ช่องดูขาวที่เธอเป็นอยู่

Incident activity log

Activity logs content : All



Incident was created 04/19/24, 05:29 PM

Incident was created by Sarah





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 ① 3 0

Events

Alerts

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 command...
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

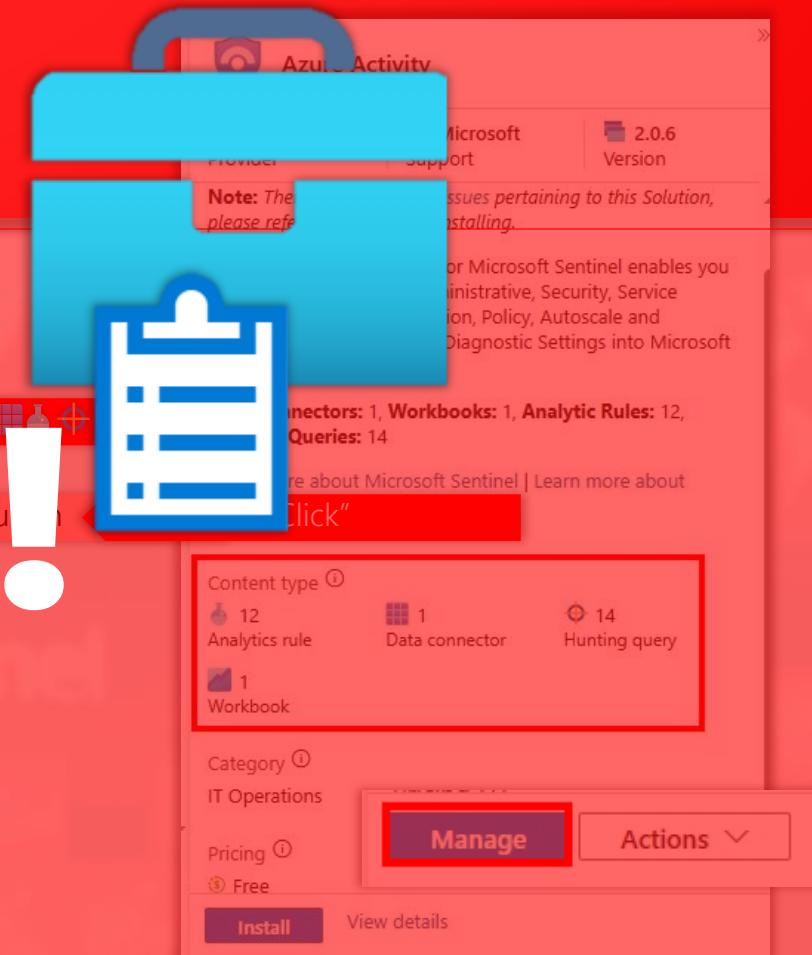
911d039e71583a07320b32bde22f8e22(MD5)
FileHash

bc866cfddda37e24dc2634dc282c7a0e6f55209...
FileHash

Similar incidents

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

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



Simplified Microsoft Sentinel

1. Click the **View full details** button.

2. Click the **Tasks** button.

3. Click the **Add task** button.

4. Enter the task description: **ข่าร่า! กัดมันเลยลูก**.

5. Click the **Save** button.

Incident tasks

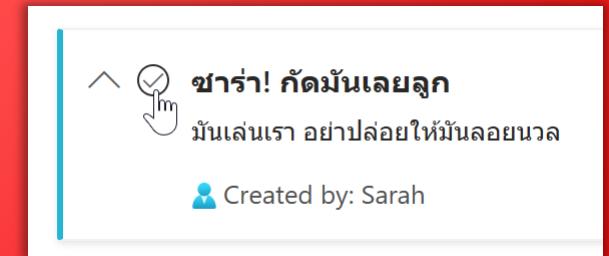
Refresh Add task 3

ข่าร่า! กัดมันเลยลูก 4

Normal B I U S
“ ” ↵ Tx

มันเล่นเรา อย่าปล่อยให้มันล้อຍนวลด

Save Cancel



Incident actions

- Run playbook (Preview)
- Create automation rule
- Create team (Preview)

Incident Team

Team name *
Incident 2: Multi-stage incident involving Execution & Defense

Team description
อาจาร์ย์เคนช่วยด้วย

Add groups and members 1
Admin ThaiCySec
admin@thaicysec.com

Search users and groups

กดเพื่อเริ่มกระบวนการจัดการ



Incident tasks

Home > Microsoft Sentinel | Incidents >



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

Incident tasks

Refresh Add task

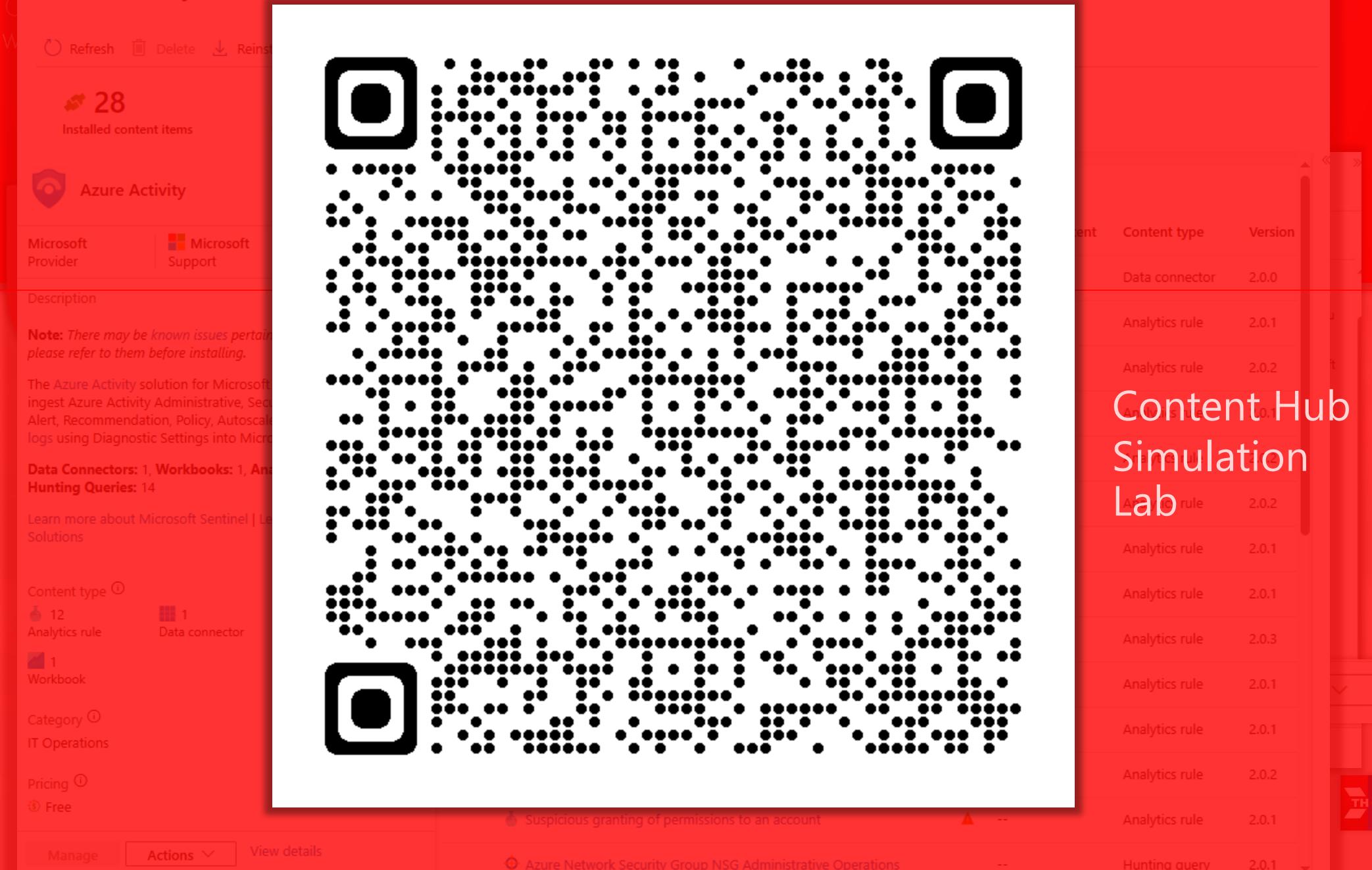
1/1 completed

Search Status : All

✓ ขาร่า! กัดมันเลยลูก

Created by: Sarah

Name	Type
127.0.0.1	IP
ded8fd7f36417f66eb6ada10e0c0d7c0022986e	FileHas
911d039e71583a07320b32bde22f8e22(MD5)	FileHas
bc866cfcd37e24dc2634dc282c7a0e6f55209c	FileHas
6cbce4a295c163791b60fc23d285e6d84f28ee4c	FileHas
7353f60b1739074eb17c5f4dddefe239(MD5)	FileHas
de96a6e69944335375dc1ac238336066889d9ff	FileHas
yellow	Host
aedf41adc7a2d1b9bec091ece86a6fcc1e63e1d2	FileHas
79ef9cc16b1ecf09e424077014473e4b(MD5)	FileHas
e1a139c25d9069ca030bc6c6acdd1be4a8d5d81	FileHas
5fc5d3c811f87bcf1fa10f4aad355879647b1d7d1	FileHas
719a31eeb64b9caeb66e0f992c9ac206(MD5)	FileHas



Cloud Security Center

Home > Microsoft Sentinel | Content hub >

Azure Activity

W... Refresh Delete Reinstall

28 Installed content items 13 Configuration needed

Azure Activity

Search...

MS Sentinel in the Field

Content pack 12 Analytics rule 1 Hunting query 14 Hunting query 1 Workbook Category ① IT Operations Pricing ① Free Manage Actions View details

MS Sentinel Ninja

NFT Creation or expensive compute in Azure

MS Sentinel Ninja

SC-900 Updated (Sentinel 55%)

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

Hunting query 2.0.1

THCS Spark Tech 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

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

- 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
2. Can compare score with organizations like yours
3. Can be improved if follow recommendations for Active Directory
4. Can be improved even using 3rd party software for actions

Yes/No
Yes/No
Yes/No
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



Where can you see Azure Secure Score?

The image shows two screenshots of the Microsoft Azure portal. The left screenshot displays the 'Azure services' dashboard, which includes icons for Create a resource, Monitor, Advisor, Microsoft Defender for Cloud (boxed in blue), Security, Azure AD Connect Health, Subscriptions, Application Insights, Alerts, and More services. The right screenshot shows the 'Microsoft Defender for Cloud | Security posture' blade, which includes sections for General (Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems), Cloud Security (Security posture, Regulatory compliance, Workload protections, Firewall Manager), and Environment (Management groups, Subscriptions, Unhealthy resources, Recommendations). A circular chart indicates a 'Secure score' of 12%.

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

[redacted] 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



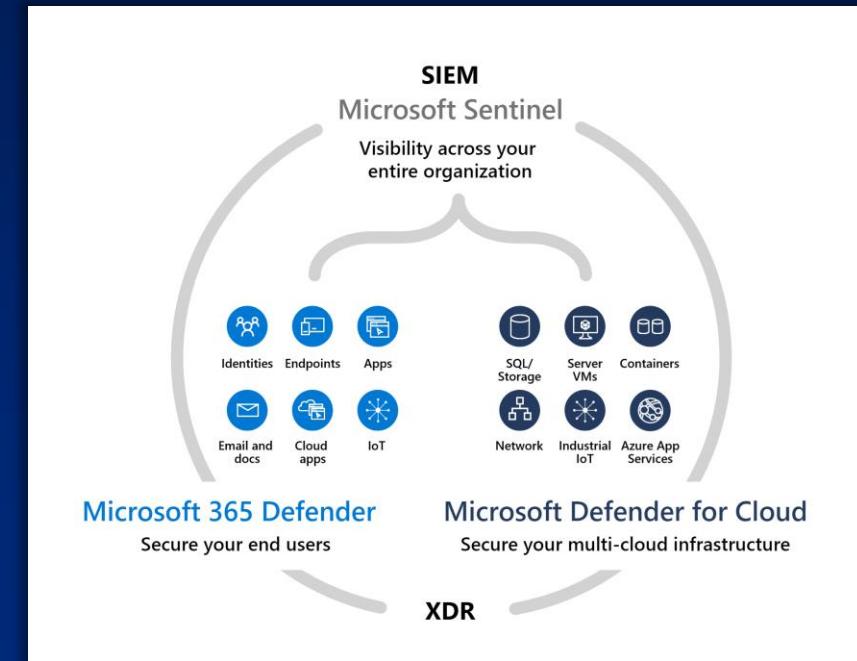
(Azure) Microsoft Sentinel

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

[redacted] 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



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



Which product can be used 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. Privileged 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**