Exam

SC-200

Microsoft Security Operations Analyst

Free demo	40 sample questions
Full exam	392 questions with answers and explanations
Contents	Questions with answers and explanations
Generated	30 October 2026

Exam domains

Domain	Exam weight	Questions
D1 Manage a security operations environment	40–45%	21
D2 Respond to security incidents	35–40%	12
D3 Perform threat hunting	20–25%	7

This is a free demo from Dumpsgate: 40 of the exam's 392 questions. **Get the full SC-200 exam** with every question, answer and explanation.

Question 1

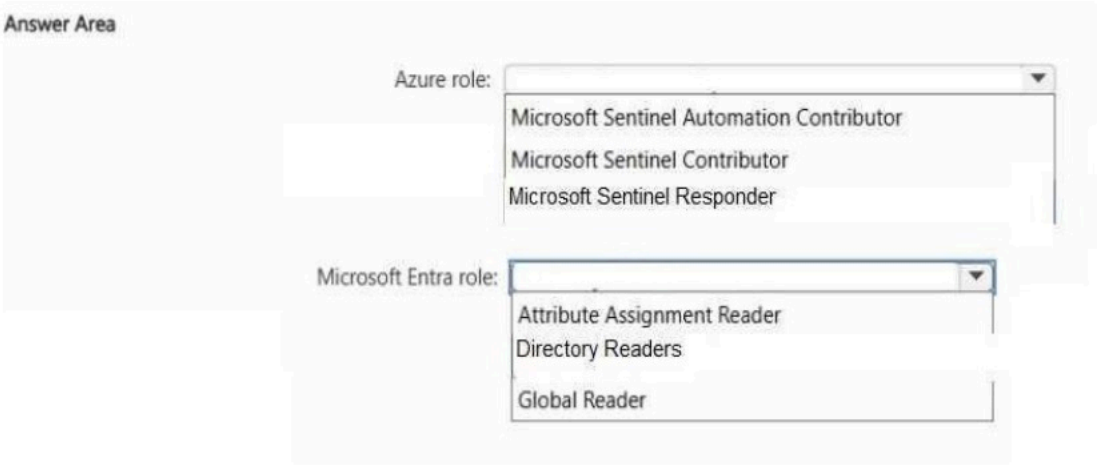
Hotspot (dropdowns) · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named workspace1.

You need to ensure that User1 can triage Microsoft Sentinel incidents in workspace1. The solution must use the principle of least privilege.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Azure role: Microsoft Sentinel Automation Contributor | Microsoft Sentinel Contributor | Microsoft Sentinel Responder

Microsoft Entra role: Attribute Assignment Reader | Directory Readers | Global Reader

Answer

- Azure role: **Microsoft Sentinel Responder**
- Microsoft Entra role: **Directory Readers**

Explanation

Assign Microsoft Sentinel Responder at the workspace scope so User1 can triage incidents without the broader permissions of a contributor role. Directory Readers is the least-privileged Microsoft Entra role among the listed choices that supports the directory information needed when working with Sentinel incidents. Together, these roles meet the incident-triage requirement while following least privilege.

https://learn.microsoft.com/en-us/azure/sentinel/roles
https://learn.microsoft.com/en-us/azure/sentinel/incident-navigate-triage

✗ **Azure role: Microsoft Sentinel Automation Contributor** Microsoft Sentinel Automation Contributor This role is intended for managing Sentinel automation, rather than providing the incident-triage permissions User1 needs. It does not meet the requirement as the appropriate least-privilege incident role.

https://learn.microsoft.com/en-us/azure/sentinel/roles
https://learn.microsoft.com/en-us/azure/sentinel/automation/automate-responses-with-playbooks

Free demo · full exam: 392 questions

https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules

✗ **Azure role: Microsoft Sentinel Contributor** Microsoft Sentinel Contributor
Contributor permissions are broader than needed for triaging incidents and include capabilities beyond those required by this scenario. Microsoft Sentinel Responder is the narrower suitable role.

https://learn.microsoft.com/en-us/azure/sentinel/roles

✓ **Azure role: Microsoft Sentinel Responder** Microsoft Sentinel Responder
The Responder role is designed to investigate and respond to incidents, including triage, without granting the broader management permissions associated with Contributor. Assign it to User1 for workspace1.

https://learn.microsoft.com/en-us/azure/sentinel/roles
https://learn.microsoft.com/en-us/azure/sentinel/incident-navigate-triage

✗ **Microsoft Entra role: Attribute Assignment Reader** Attribute Assignment Reader
This role provides read access related to attribute assignments, not the directory-reading permissions needed for working with incident-related directory information in Sentinel. Directory Readers is the appropriate choice from the listed options.

https://learn.microsoft.com/en-us/azure/sentinel/roles
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles?WT.mc_id=MVP_319025

✓ **Microsoft Entra role: Directory Readers** Directory Readers
Directory Readers provides read access to directory information that can be needed when triaging Sentinel incidents. It grants the required directory access without using the broader Global Reader role.

https://learn.microsoft.com/en-us/azure/sentinel/roles
https://learn.microsoft.com/en-us/azure/sentinel/incident-navigate-triage

✗ **Microsoft Entra role: Global Reader** Global Reader
Global Reader grants read access across a wide range of Microsoft Entra and Microsoft 365 settings, exceeding what is needed for incident triage. Directory Readers is the more limited suitable role.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles?WT.mc_id=MVP_319025

Dumpsgate

Question 2

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have two Microsoft Entra tenants named Tenantl and Tenant2. Each tenant is linked to an Azure subscription. Tenant! contains a group named Group1. Tenant2 contains a group named Group2.

You need to implement Microsoft Sentinel for each tenant. The solution must meet the following requirements:

- Ensure that Group1 can manage security incidents for Tenantl and Tenant2 in a single workspace.
- Ensure that Group2 can manage security incidents only for Tenant2.
- Minimize the use of guest accounts.
- Minimize administrative effort.
- Minimize costs.

What should you include in the solution?

A. one workspace and Privileged Identity Management (PIM)
B. one workspace and multiple role-based access control (RBAC) role assignments
C. two workspaces and Azure Lighthouse
D. two workspaces and granular delegated admin privileges (GDAP)

Answer: C. two workspaces and Azure Lighthouse

Explanation

Use one Microsoft Sentinel workspace in each tenant, then use Azure Lighthouse to delegate access to Tenant2's workspace to Group1 in Tenant1. Group1 can manage incidents across both workspaces without requiring guest accounts, while Group2 retains access only to Tenant2's workspace. Lighthouse provides cross-tenant resource delegation, and two workspaces preserve each tenant's separate workspace boundary; this avoids creating a shared workspace that cannot satisfy the tenant-specific access requirements.

https://learn.microsoft.com/en-us/azure/lighthouse/concepts/cross-tenant-management-experience
https://learn.microsoft.com/en-us/azure/lighthouse/how-to/manage-sentinel-workspaces
https://learn.microsoft.com/en-us/azure/lighthouse/concepts/azure-delegated-resource-management
https://learn.microsoft.com/en-us/azure/sentinel/multiple-tenants-service-providers
https://learn.microsoft.com/en-us/azure/lighthouse/overview
https://learn.microsoft.com/en-us/azure/lighthouse/how-to/onboard-customer

✗ **A** one workspace and Privileged Identity Management (PIM)
A single workspace cannot provide the required tenant-specific separation and access: Group2 must be limited to Tenant2, while Group1 must manage incidents in both tenants. PIM can govern activation of eligible roles, but it does not provide the cross-tenant resource delegation needed here.

https://learn.microsoft.com/en-us/azure/lighthouse/concepts/cross-tenant-management-experience
https://learn.microsoft.com/en-us/azure/lighthouse/how-to/manage-sentinel-workspaces

✗ **B** one workspace and multiple role-based access control (RBAC) role assignments
Multiple RBAC assignments can scope permissions within a workspace, but they do not make a workspace in one tenant serve as a workspace in both tenants with the required tenant-specific access. This also does not address cross-tenant access without adding guest accounts or another delegation mechanism.

https://learn.microsoft.com/en-us/azure/lighthouse/concepts/cross-tenant-management-experience

Free demo · full exam: 392 questions

https://learn.microsoft.com/en-us/azure/lighthouse/how-to/manage-sentinel-workspaces

✓ **C** two workspaces and Azure Lighthouse
Create a Sentinel workspace in each tenant and use Azure Lighthouse to delegate access to Tenant2's workspace to Group1 from Tenant1. Group1 can then manage incidents in both workspaces, while Group2 can retain access only to Tenant2's workspace; Lighthouse avoids the need to add Group1 as guest users in Tenant2.

https://learn.microsoft.com/en-us/azure/lighthouse/concepts/cross-tenant-management-experience
https://learn.microsoft.com/en-us/azure/lighthouse/how-to/manage-sentinel-workspaces
https://learn.microsoft.com/en-us/azure/lighthouse/concepts/azure-delegated-resource-management
https://learn.microsoft.com/en-us/azure/sentinel/multiple-tenants-service-providers
https://learn.microsoft.com/en-us/azure/lighthouse/overview
https://learn.microsoft.com/en-us/azure/lighthouse/how-to/onboard-customer

✗ **D** two workspaces and granular delegated admin privileges (GDAP)
Two workspaces support the tenant separation, but GDAP is not the Azure resource delegation mechanism for granting Group1 access to manage Sentinel workspaces across tenants. Azure Lighthouse is the cross-tenant delegation option suited to this requirement.

https://learn.microsoft.com/en-us/azure/lighthouse/how-to/manage-sentinel-workspaces
https://learn.microsoft.com/en-us/azure/lighthouse/concepts/azure-delegated-resource-management
https://learn.microsoft.com/en-us/azure/lighthouse/overview

Dumpsgate

Question 3

Hotspot (dropdowns) · Domain: D1 Manage a security operations environment › Configure automation for Microsoft Defender XDR and Microsoft Sentinel

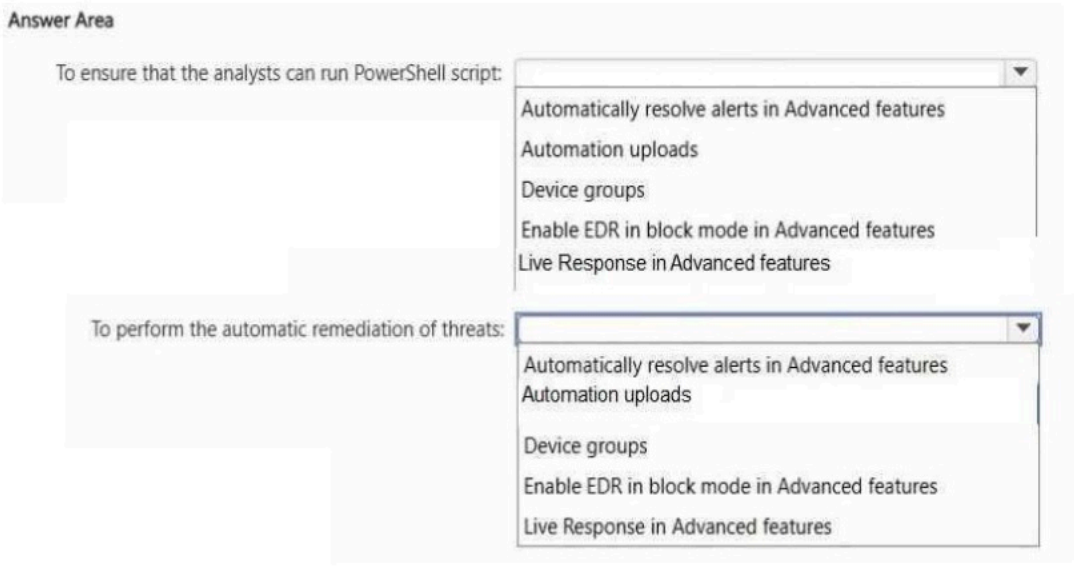
You have a Microsoft 365 subscription. The subscription contains 500 Windows 11 devices that are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

- Ensure that security operation analysts can run PowerShell scripts on client computers.
- Perform the automatic remediation of threats on client computers

Which Endpoints settings should you configure in the Microsoft Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



To ensure that the analysts can run PowerShell script: Automatically resolve alerts in Advanced features | Automation uploads | Device groups | Enable EDR in block mode in Advanced features | Live Response in Advanced features

To perform the automatic remediation of threats: Automatically resolve alerts in Advanced features | Automation uploads | Device groups | Enable EDR in block mode in Advanced features | Live Response in Advanced features

Answer

- To ensure that the analysts can run PowerShell script: **Live Response in Advanced features**
- To perform the automatic remediation of threats: **Enable EDR in block mode in Advanced features**

Explanation

Enable Live Response in Advanced features so security operations analysts can connect to client devices and run PowerShell scripts. Enable EDR in block mode in Advanced features to let Defender for Endpoint

Free demo · full exam: 392 questions

block and remediate threats detected by EDR, including when Microsoft Defender Antivirus is not the primary antivirus. These settings address the two requirements directly.

https://learn.microsoft.com/defender-endpoint/live-response
https://learn.microsoft.com/en-us/defender-endpoint/edr-block-mode-faqs
https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features
https://learn.microsoft.com/en-us/defender-endpoint/live-response-command-examples

✗ **Box 1: Automatically resolve alerts in Advanced features** Automatically resolve alerts in Advanced features
This setting controls whether alerts are automatically marked as resolved; it does not enable analysts to run PowerShell scripts on client computers. It also is not the setting that enables EDR block-mode remediation.

https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features

✗ **Box 1: Automation uploads** Automation uploads
Automation uploads controls whether files collected during automated investigations can be uploaded for analysis. It does not provide analysts with PowerShell access or enable EDR block mode.

https://learn.microsoft.com/en-us/defender-endpoint/manage-automation-file-uploads

✗ **Box 1: Device groups** Device groups
Device groups organize devices and can be used to manage access and settings by group. They do not enable the Live Response capability analysts need to run scripts.

https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features
https://learn.microsoft.com/en-us/defender-endpoint/advanced-features

✗ **Box 1: Enable EDR in block mode in Advanced features** Enable EDR in block mode in Advanced features
EDR in block mode helps block and remediate threats identified by EDR, so it addresses the second requirement. It does not enable analysts to run PowerShell scripts; that requires Live Response.

https://learn.microsoft.com/en-us/defender-endpoint/edr-block-mode-faqs
https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features

✓ **Box 1: Live Response in Advanced features** Live Response in Advanced features
Enable Live Response to let authorized security operations analysts remotely investigate devices and run supported commands, including PowerShell scripts. This satisfies the requirement to run scripts on client computers.

https://learn.microsoft.com/defender-endpoint/live-response
https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features
https://learn.microsoft.com/en-us/defender-endpoint/live-response-command-examples

✗ **Box 2: Automatically resolve alerts in Advanced features** Automatically resolve alerts in Advanced features
Automatically resolving alerts changes their alert status; it does not automatically remediate threats on the devices. The requirement calls for EDR block-mode threat blocking and remediation.

https://learn.microsoft.com/en-us/defender-endpoint/edr-block-mode-faqs
https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features

✗ **Box 2: Automation uploads** Automation uploads
This setting governs uploading files collected by automated investigations, not automatic remediation of threats. It does not enable EDR block mode.

https://learn.microsoft.com/en-us/defender-endpoint/manage-automation-file-uploads

✗ **Box 2: Device groups** Device groups
Device groups provide a way to organize and manage devices, but selecting this setting alone does not enable automatic threat remediation. EDR in block mode is the relevant setting for that requirement.

https://learn.microsoft.com/en-us/defender-endpoint/edr-block-mode-faqs
https://learn.microsoft.com/en-us/defender-endpoint/advanced-features

✓ **Box 2: Enable EDR in block mode in Advanced features** Enable EDR in block mode in Advanced features
Enable EDR in block mode so Defender for Endpoint can block and remediate threats detected by EDR. This meets the requirement for automatic threat remediation on client computers.

https://learn.microsoft.com/en-us/defender-endpoint/edr-block-mode-faqs

Free demo · full exam: 392 questions

https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features

✗ **Box 2: Live Response in Advanced features** Live Response in Advanced features
Live Response allows analysts to investigate devices and run commands, but it is not the setting for automatic remediation of EDR-detected threats. The required setting is EDR in block mode.

https://learn.microsoft.com/defender-endpoint/live-response
https://learn.microsoft.com/en-us/defender-endpoint/edr-block-mode-faqs
https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features

---

Question 4

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft 365 subscription that uses Microsoft Security Copilot. You plan to configure a custom GPT plugin for Copilot. Which GPT model should you use?

A. davinci-002
B. gpt-35-turbo
C. of-mini
D. gpt-4o

Answer: D. gpt-4o

Explanation

For a custom GPT plugin in Microsoft Security Copilot, use the GPT-4o model. The plugin guidance identifies GPT-4o as the model to use for this configuration, making option D the correct choice. [2]

https://learn.microsoft.com/en-us/copilot/security/plugin-gpt

✗ **A** davinci-002
davinci-002 is not the GPT model specified for configuring a custom GPT plugin in Security Copilot. Use GPT-4o for this scenario.

https://learn.microsoft.com/en-us/copilot/security/plugin-gpt

✗ **B** gpt-35-turbo
gpt-35-turbo is not the model specified in the Security Copilot custom GPT plugin guidance. The required choice here is GPT-4o.

https://learn.microsoft.com/en-us/copilot/security/plugin-gpt

✗ **C** of-mini
of-mini is not the model identified for configuring a custom GPT plugin in Security Copilot. The plugin guidance calls for GPT-4o instead.

https://learn.microsoft.com/en-us/copilot/security/plugin-gpt

✓ **D** gpt-4o
GPT-4o is the model specified for a custom GPT plugin in Microsoft Security Copilot. Therefore, it meets the scenario's configuration requirement.

https://learn.microsoft.com/en-us/copilot/security/plugin-gpt

---

Question 5

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft 365 subscription that uses Microsoft Security Copilot. You have the files shown in the following table.

Name	Size
File1.docx	4 MB
File2.pdf	2 MB
File3.txt	128 KB

Each file contains a copy of your company's compliance policy.

You need to ensure that Security Copilot responses are informed by the compliance policy. Which files can be uploaded to Security Copilot?

A. File1.docxonly
B. File3.txt only
C. Filet.docx and File3.txt only
D. File2.pdf and File3.txt only
E. File1.doocFile2.pdf, andFile3.txt

Answer: D. File2.pdf and File3.txt only

Explanation

Security Copilot can use the 2-MB PDF and the 128-KB TXT file, but not the DOCX file. Therefore, File2.pdf and File3.txt are the files that meet the upload requirements and can provide the compliance policy as context for Security Copilot responses.

https://learn.microsoft.com/sv-se/copilot/security/upload-file

✗ **A** File1.docx only
File1.docx is a DOCX file, which is not an eligible file type for this Security Copilot upload scenario. Uploading it alone would not make the policy available to inform responses.

https://learn.microsoft.com/sv-se/copilot/security/upload-file

✗ **B** File3.txt only
The TXT file is eligible, but this choice leaves out File2.pdf, which can also be uploaded. Since the question asks which files can be uploaded, this is incomplete.

https://learn.microsoft.com/sv-se/copilot/security/upload-file

✗ **C** File1.docx and File3.txt only
File3.txt is eligible, but File1.docx is not an eligible file type for this upload scenario. This choice also omits the eligible PDF file.

https://learn.microsoft.com/sv-se/copilot/security/upload-file

✓ **D** File2.pdf and File3.txt only
The PDF and TXT files are supported upload types, and their listed sizes—2 MB and 128 KB—are within the upload limit. Both can therefore provide the compliance policy as context for Security Copilot

responses.
https://learn.microsoft.com/sv-se/copilot/security/upload-file

✗ **E** File1.docx, File2.pdf, and File3.txt
Although File2.pdf and File3.txt can be uploaded, File1.docx is not an eligible file type for this scenario. Including it makes this choice incorrect.
https://learn.microsoft.com/sv-se/copilot/security/upload-file

Question 6

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a custom workbook that will calculate the average time it takes to close security incidents. The solution must minimize administrative effort.

Which built-in Microsoft Sentinel workbook template should you select?

A. Incident Overview
B. Workspace Usage Report
C. Investigation Insights
D. Security operations efficiency

Answer: D. Security operations efficiency

Explanation

Select D, Security operations efficiency. This built-in workbook is designed to measure SOC performance, including incident-handling metrics such as average time to close incidents, so it meets the requirement without building the calculations from scratch. That makes it the lowest-effort choice for this scenario.
https://learn.microsoft.com/en-us/azure/sentinel/top-workbooks
https://learn.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics

✗ **A** Incident Overview
This workbook provides an overview of incident activity, rather than focusing on SOC efficiency metrics such as the average time to close incidents. It is therefore not the best built-in template for the requested calculation.
https://learn.microsoft.com/en-us/azure/sentinel/top-workbooks

✗ **B** Workspace Usage Report
This workbook focuses on workspace usage, such as data and resource consumption, not the time taken to resolve security incidents. It does not directly meet the requested incident-closure metric.
https://learn.microsoft.com/en-us/azure/sentinel/top-workbooks

✗ **C** Investigation Insights
This workbook is intended to provide insights into incident investigations, not to report the SOC efficiency metric requested here: average incident closure time. The Security operations efficiency template is the more direct fit.
https://learn.microsoft.com/en-us/azure/sentinel/incident-investigation

✓ **D** Security operations efficiency
This template is intended to assess security operations performance and includes incident metrics such

as the average time to close incidents. Selecting it provides the requested calculation with minimal administrative effort, rather than requiring a custom workbook to be built from scratch.

https://learn.microsoft.com/en-us/azure/sentinel/top-workbooks
https://learn.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics

---

Question 7

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft Sentinel workspace named Workspace1 that contains the AzureActivity table.

You need to configure the retention period for the AzureActivity table. The solution must meet the following requirements:

- Maximize the period during which you can run interactive queries.
- Minimize retention costs.

To what should you set the retention period? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. 30 days
B. 90 days
C. 180 days
D. 2 years

Answer: B. 90 days

Explanation

Set the AzureActivity table retention period to 90 days. This is the longest period available for interactive querying without extending retention into a higher-cost period, so it meets both requirements: maximize interactive query time while minimizing retention costs.

https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive?trk=article-ssr-frontend-pulse_little-text-block
https://learn.microsoft.com/en-us/azure/sentinel/billing

✗ **A** 30 days
Thirty days would reduce retention costs, but it does not maximize the period during which you can run interactive queries. The table can retain data interactively for longer without extending beyond 90 days.

https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive?trk=article-ssr-frontend-pulse_little-text-block

✓ **B** 90 days
Ninety days provides the longest interactive-query period while avoiding the additional retention costs associated with keeping data for longer. It therefore satisfies both requirements.

https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive?trk=article-ssr-frontend-pulse_little-text-block
https://learn.microsoft.com/en-us/azure/sentinel/billing

✗ **C** 180 days

Keeping the data for 180 days exceeds the 90-day interactive-query period. The additional retention is not needed to maximize interactive queries and would increase retention costs.

https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive?trk=article-ssr-frontend-pulse_little-text-block
https://learn.microsoft.com/en-us/azure/sentinel/billing

✗ **D** 2 years
Two years would retain the data far beyond the 90-day interactive-query period, adding retention costs without extending the time available for interactive queries.

https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive?trk=article-ssr-frontend-pulse_little-text-block
https://learn.microsoft.com/en-us/azure/sentinel/billing

Question 8

Yes / No · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have the Azure subscriptions shown in the following table.

Name	Resource group
Sub1	RG1
Sub2	RG2, RG3

Dumpsgate

Name	Resource group
Sub1	RG1
Sub2	• RG2 • RG3

Name	Role
User1	Security Operator
User2	Security Administrator
User3	Global Administrator

User	Role	Scope
User1	Owner	Sub1
User2	Reader	Sub2
User3	Owner	RG2

Answer Area

Statements	Yes	No
User1 can add an additional capacity to Capacity1.	○	○
User2 can view the capacity usage information of Capacity2.	○	○
User3 can configure additional plugins in Capacity2.	○	○

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Role
User1	Security Operator
User2	Security Administrator
User3	Global Administrator

The users have the Azure roles shown in the following table.

User	Role	Scope
User1	Owner	Sub1
User2	Reader	Sub2
User3	Owner	RG2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statement	Yes	No
User1 can add an additional capacity to Capacity1.	☐	☐
User2 can view the capacity usage information of Capacity2.	☐	☐
User3 can configure additional plugins in Capacity2.	☐	☐

Answer

- User1 can add an additional capacity to Capacity1. **Yes**
- User2 can view the capacity usage information of Capacity2. **No**
- User3 can configure additional plugins in Capacity2. **No**

Explanation

User1 is an Owner at the Sub1 subscription scope, which includes resources in that subscription, so User1 can add capacity to Capacity1. User2 has only the Reader role on Sub2, which does not provide the permissions needed to view Capacity2's capacity-usage information. User3's Owner role is scoped to RG2 and does not grant the permissions required to configure additional plugins in Capacity2.

✓ **Statement 1** User1 can add an additional capacity to Capacity1.
User1 is an Owner on Sub1, so the role applies to resources within that subscription, including Capacity1. That scope grants the required management access to add capacity.

✗ **Statement 2** User2 can view the capacity usage information of Capacity2.
User2 has the Reader role on Sub2, which is read-only access to Azure resources and does not grant the required access to view this capacity-usage information. Therefore, the statement is false.

✗ **Statement 3** User3 can configure additional plugins in Capacity2.
User3's Owner role applies only to RG2, not to resources in RG3. In addition, the role assignments shown do not grant the required permission to configure plugins in Capacity2, so the statement is false.

Question 9

Multiple choice · Domain: D1 Manage a security operations environment › Ingest data into the Microsoft Sentinel SIEM and platform

You have a Microsoft 365 E5 subscription.

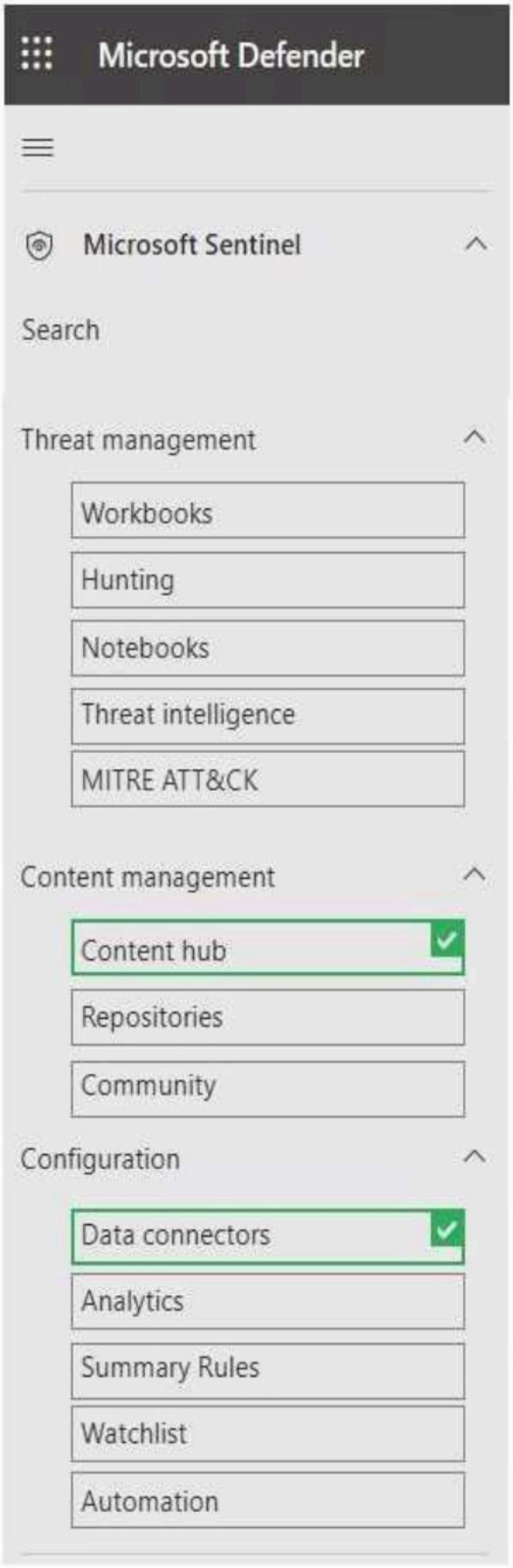
You need to configure Microsoft Sentinel to collect logs from Microsoft Entra.

Which two nodes should you use in the Microsoft Defender portal? To answer, select the appropriate nodes in the answer area.

NOTE: Each correct answer is worth one point.

Free demo · full exam: 392 questions

Answer Area


Microsoft Defender
Microsoft Sentinel
Search
Threat management
Workbooks
Hunting
Notebooks
Threat intelligence
MITRE ATT&CK
Content management
Content hub
Repositories
Community
Configuration
Data connectors
Analytics
Summary Rules
Watchlist
Automation

A. Content hub
B. Data connectors
C. Analytics
D. Repositories

Answer

- A. **Content hub**
- B. **Data connectors**

Explanation

To collect Microsoft Entra logs, first use Content hub to find and install the relevant Microsoft Sentinel content or solution, then use Data connectors to configure the connection that brings the logs into Sentinel. Analytics is for creating or managing detection rules, and Repositories is not the node used to connect a log source. [1][3][4]

https://learn.microsoft.com/azure/sentinel/sentinel-solutions-catalog
https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources
https://learn.microsoft.com/en-us/azure/sentinel/configure-data-connector

✓ **A** Content hub
Content hub is where you find and install Sentinel solutions and related content, including content for Microsoft Entra. It is therefore the appropriate first node when preparing the required log-collection capability. [1][5]

https://learn.microsoft.com/azure/sentinel/sentinel-solutions-catalog
https://learn.microsoft.com/en-us/azure/sentinel/sentinel-solutions

✓ **B** Data connectors
Data connectors is the node used to connect a data source to Sentinel and configure its ingestion. Use it to set up collection of Microsoft Entra logs. [3][4]

https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources
https://learn.microsoft.com/en-us/azure/sentinel/configure-data-connector

✗ **C** Analytics
Analytics is used to create and manage detection rules based on data in Sentinel, not to configure the connection that collects Microsoft Entra logs. It does not meet the requirement to set up log ingestion. [3]

https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources

✗ **D** Repositories
Repositories is not the node for installing Sentinel solutions or configuring a data-source connection. To collect Microsoft Entra logs, use Content hub and Data connectors instead. [1][3]

https://learn.microsoft.com/azure/sentinel/sentinel-solutions-catalog
https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources

Free demo · full exam: 392 questions

Question 10

Multiple choice · Domain: D1 Manage a security operations environment › Ingest data into the Microsoft Sentinel SIEM and platform

You have an on-premises virtual machine named VM1 that runs Windows Server. You have a Microsoft Sentinel workspace named Workspacel. You install the Azure Connected Machine agent on VM1. You need to collect events from VM1 and send the events to Workspacel. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

A. From the Microsoft Defender portal, add the Windows Security Events via AMA data connector.
B. From the Microsoft Defender portal, add the Syslog via AMA data connector.
C. On VM1, install the Log Analytics agent.
D. On VM1, enable the Azure Monitor Agent extensions.
E. On VM1, install the Microsoft Monitonng Agent.
F. From the Microsoft Defender portal, create a data collection rule (DCR) that targets VM1.

Answer

- A. **From the Microsoft Defender portal, add the Windows Security Events via AMA data connector.**
- F. **From the Microsoft Defender portal, create a data collection rule (DCR) that targets VM1.**

Explanation

VM1 runs Windows Server, so Microsoft Sentinel's Windows Security Events via AMA connector is the appropriate connector for Windows Security events. The DCR must then target the Azure Arc-enabled VM. Microsoft documents that the connector's setup process includes creating a DCR and adding Azure Arc-enabled servers as resources. Microsoft Learn You do not need to select a separate manual AMA-extension installation action when the DCR is created through the Azure portal: Microsoft states that when a DCR is created and a machine is added as a resource, Azure Monitor Agent installs automatically if necessary.

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

Free demo · full exam: 392 questions

Question 11

Yes / No · Domain: D1 Manage a security operations environment › Configure detections

You have a custom Microsoft Defender XDR detection rule that includes the following KQL query.

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA2
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, RecipientEmailAddress, Enti
```



For each of the following statements, select Yes if True. Otherwise select No.

NOTE: Each correct selection is worth one point.

Statement	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEmailAddress column.	☐	☐
The custom detection rule can be used to restrict app execution automatically based on the DeviceId column.	☐	☐
The custom detection rule can be used to automate the deletion of a file based on the SHA256 column.	☐	☐

Answer

- The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEmailAddress column. **Yes**
- The custom detection rule can be used to restrict app execution automatically based on the DeviceId column. **No**
- The custom detection rule can be used to automate the deletion of a file based on the SHA256 column. **No**

Explanation

The query returns email-related fields, including RecipientEmailAddress and ReportId, so the rule can target delivered messages for deletion. DeviceId identifies a device, but restricting app execution is a file-focused response action, not an action performed on a device based on that column. Although SHA256 identifies a file, the rule cannot automate file deletion as a response action.

https://learn.microsoft.com/defender-xdr/custom-detection-rules
https://learn.microsoft.com/en-us/defender-xdr/m365d-response-actions-notifications

✓ **Statement 1** The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEmailAddress column.
Yes. The query includes RecipientEmailAddress and ReportId for delivered email events, which provide the email-related information needed for the rule's email deletion response action. The statement is therefore supported by the columns returned by this query.

https://learn.microsoft.com/defender-xdr/custom-detection-rules
https://learn.microsoft.com/en-us/defender-xdr/m365d-response-actions-notifications

✗ **Statement 2** The custom detection rule can be used to restrict app execution automatically based on the DeviceId column.
No. DeviceId identifies a device, but restricting app execution is a file-focused response action and is not enabled by the DeviceId column alone. The query does not make this action available simply by returning a device identifier.

https://learn.microsoft.com/defender-xdr/custom-detection-rules
https://learn.microsoft.com/en-us/defender-xdr/m365d-response-actions-notifications

✗ **Statement 3** The custom detection rule can be used to automate the deletion of a file based on the SHA256 column.
No. SHA256 identifies the file, but that does not make automated file deletion an available custom detection response action. Returning the hash in the query is not sufficient to enable the stated deletion action.

https://learn.microsoft.com/defender-xdr/custom-detection-rules
https://learn.microsoft.com/en-us/defender-xdr/m365d-response-actions-notifications

Free demo · full exam: 392 questions

Question 12

Hotspot (dropdowns) · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft Sentinel workspace named Workspaces1.

The AzureActivity table in Workspace1 has the following retention periods:

- Interactive: 180 days
- Total: 180 days

You need to modify the retention periods to meet the following requirements:

- Minimize the costs associated with storing data in the table.
- Maximize the period during which the table data remains available.

How should you configure each retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Interactive: 30 days | 60 days | 90 days | 120 days

Total: 60 days | 90 days | 180 days | 2 years

Answer

- Interactive: **90 days**
- Total: **2 years**

Explanation

Set Interactive retention to 90 days to use the shortest available interactive period for AzureActivity, which helps minimize storage costs. Set Total retention to 2 years to keep the data available for the longest period offered; the time beyond interactive retention can be retained in lower-cost archive storage. Together, these settings minimize cost while maximizing how long the table data remains available.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/sentinel/billing-reduce-costs

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal
https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive

✗ **Box 1: 30 days** Interactive: 30 days
This is shorter than the 90-day minimum interactive retention available for the AzureActivity table, so it is not a valid configuration for this table. The shortest supported interactive period is 90 days.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal

✗ **Box 1: 60 days** Interactive: 60 days
A 60-day interactive period is below the table's 90-day minimum and is not a supported setting for AzureActivity. Choose the shortest supported period instead to control interactive-storage costs.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal

✓ **Box 1: 90 days** Interactive: 90 days
This is the shortest supported interactive retention period for AzureActivity, so it minimizes the time data is kept in the more readily accessible interactive tier. Data can still remain available longer through the total retention setting.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/sentinel/billing-reduce-costs
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal

✗ **Box 1: 120 days** Interactive: 120 days
This keeps data in interactive retention longer than the 90-day minimum. Because the requirement is to minimize storage costs, 120 days is not preferable when 90 days is supported.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/sentinel/billing-reduce-costs
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal

✗ **Box 2: 60 days** Total: 60 days
Total retention cannot be shorter than the selected 90-day interactive period, and this option would also make the data available for less time than the maximum offered. It does not satisfy the availability requirement.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal

✗ **Box 2: 90 days** Total: 90 days
This would retain the data only for the interactive period and would not maximize the period during which it remains available. The 2-year option extends availability beyond interactive retention.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal
https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive

✗ **Box 2: 180 days** Total: 180 days
This retains the data for longer than 90 days but not for the maximum period offered. Selecting 2 years better meets the requirement to maximize availability.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal
https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive

✓ **Box 2: 2 years** Total: 2 years
This is the longest total retention period in the choices, so it maximizes how long the table data remains available. Retaining data beyond interactive retention in archive helps avoid keeping it in the costlier interactive tier for the entire period.

https://learn.microsoft.com/en-us/azure/sentinel/manage-data-overview?WT.mc_id=EM-MVP-4028970
https://learn.microsoft.com/en-us/azure/sentinel/billing-reduce-costs
https://learn.microsoft.com/en-us/azure/sentinel/configure-data-retention-archive

Free demo · full exam: 392 questions

Question 13

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security. Copilot for Security has the default settings configured. You need to ensure that a user named User1 can use Copilot for Security to perform the following tasks:

- Upload files.
- View the usage dashboard.
- Share promptbooks with all users.

The solution must follow the principle of least privilege. Which role should you assign to User1?

A. Security Administrator
B. Cloud Application Administrator
C. Copilot Contributor
D. Copilot Owner

Answer: D. Copilot Owner

Explanation

Assign User1 the Copilot Owner role. With the default Copilot for Security settings, this role provides the capabilities needed to upload files, view the usage dashboard, and share promptbooks with all users, so it satisfies all three requirements. The other listed roles do not provide the required combination of Copilot permissions.

https://learn.microsoft.com/en-us/copilot/security/using-promptbooks
https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/security-copilot/manage-usage

✗ **A** Security Administrator
This Microsoft Entra role is not the Copilot for Security role that grants the required in-product capabilities. It does not meet the scenario's requirements to upload files, view the usage dashboard, and share promptbooks with all users.

https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/security-copilot/manage-usage

✗ **B** Cloud Application Administrator
This role is intended for managing cloud applications, not for granting the required Copilot for Security permissions. It does not provide the needed combination of file upload, usage-dashboard access, and promptbook sharing capabilities.

https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/security-copilot/manage-usage

✗ **C** Copilot Contributor
Copilot Contributor is not sufficient for all the requested tasks under the default settings. In particular, User1 needs the broader permissions required to view the usage dashboard and share promptbooks with all users.

https://learn.microsoft.com/en-us/copilot/security/using-promptbooks
https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/security-copilot/manage-usage

✓ **D** Copilot Owner
Copilot Owner provides the Copilot for Security permissions needed for the requested tasks, including

Free demo · full exam: 392 questions

uploading files, viewing usage information, and sharing promptbooks with all users. It is therefore the least-privilege choice among the options that satisfies every stated requirement.

https://learn.microsoft.com/en-us/copilot/security/using-promptbooks
https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/security-copilot/manage-usage

Question 14

Hotspot (dropdowns) · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft Sentinel workspace.

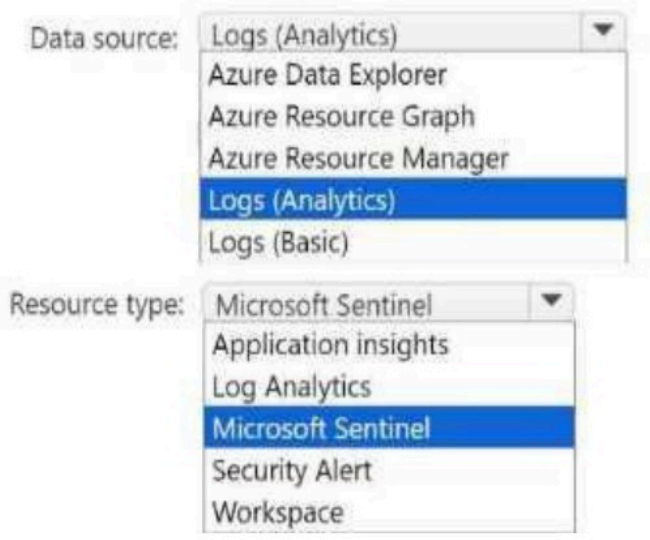
You have a KQL query. The query returns Microsoft Sentinel incidents that are stored in the SecurityIncident table and occurred during the last 90 days.

You need to create a Microsoft Sentinel workbook that will include a visualization of the query.

To what should you set Data source and Resource type for the workbook? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Data source: Azure Data Explorer | Azure Resource Graph | Azure Resource Manager | Logs (Analytics) | Logs (Basic)

Resource type: Application insights | Log Analytics | Microsoft Sentinel | Security Alert | Workspace

Answer

- Data source: **Logs (Analytics)**
- Resource type: **Microsoft Sentinel**

Free demo · full exam: 392 questions

Dumpsgate

Question 15

Single choice · Domain: D1 Manage a security operations environment › Ingest data into the Microsoft Sentinel SIEM and platform

You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1 and 100 virtual machines that run Windows Server.

You need to configure the collection of Windows Security event logs for ingestion to WS1. The solution must meet the following requirements:

- Capture a full user audit trail including user sign-in and user sign-out events.
- Minimize the volume of events.
- Minimize administrative effort.

Which event set should you select?

A. All events
B. Custom
C. Minimal
D. Common

Answer: D. Common

Explanation

Select Common. The Common event set includes the Windows sign-in and sign-out events needed for a user audit trail while collecting fewer events than All. It is a predefined set, so it requires less administration than building and maintaining a Custom selection. [1][2]

https://learn.microsoft.com/azure/sentinel/windows-security-event-id-reference
https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✗ **A** All events
All events would capture sign-in and sign-out activity, but it also collects events beyond the required audit trail, increasing ingestion volume. That conflicts with the requirement to minimize the volume of events.

https://learn.microsoft.com/azure/sentinel/windows-security-event-id-reference
https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✗ **B** Custom
A custom selection could be configured to include sign-in and sign-out events, but choosing and maintaining that selection requires more administrative effort than using a predefined set. It does not best meet the requirement to minimize administration.

https://learn.microsoft.com/azure/sentinel/windows-security-event-id-reference
https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✗ **C** Minimal
Minimal is a predefined, lower-volume set, but it does not provide the full user audit trail required here, including both sign-in and sign-out events. Common is the appropriate predefined set for that coverage without collecting all events.

https://learn.microsoft.com/azure/sentinel/windows-security-event-id-reference
https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✓ **D** Common
Common is a predefined event set that includes the sign-in and sign-out activity needed for a user audit

Free demo · full exam: 392 questions

trail while avoiding the extra volume produced by collecting all events. Using it also avoids the effort of designing and maintaining a custom event selection.

https://learn.microsoft.com/azure/sentinel/windows-security-event-id-reference
https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

---

Question 16

Hotspot (dropdowns) · Domain: D1 Manage a security operations environment › Ingest data into the Microsoft Sentinel SIEM and platform

You have an Azure subscription named Sub1. Sub1 contains a Microsoft Sentinel workspace named SW1 and a virtual machine named VM1 that runs Windows Server. SW1 collects security logs from VM1 by using the Windows Security Events via AMA connector.

You need to limit the scope of events collected from VM1. The solution must ensure that only audit failure events are collected.

How should you complete the filter expression for the connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
Security!*[ [Blank 1][Blank 2][Keywords='0x8010000000000000']]
```

Answer Area



Blank 1 in Security!*[[Blank 1]: EventData | Keywords | System

Blank 2 in Security!*[[Blank 1][Blank 2]: EventData | Keywords | System

Answer

- Blank 1 in Security!*[[Blank 1]: **System**
- Blank 2 in Security!*[[Blank 1][Blank 2]: **Keywords**

Explanation

Select System for Blank 1 and Keywords for Blank 2 to form a filter on the event's System section and its Keywords field. The value `0x8010000000000000` identifies audit failure events, so this filter limits collection to those events as required. [1]

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✗ **Blank 1: EventData** EventData
EventData refers to the event's payload fields, not the System section that contains the event Keywords field used by this filter. It would not apply the supplied keyword value at the required location.

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✗ **Blank 1: Keywords** Keywords
Keywords is the field to test, but it is not the enclosing event section in this expression. The filter must first select System, then specify Keywords within it.

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✓ **Blank 1: System** System
System is the event section that contains the Keywords field. Choosing it lets the expression apply the audit-failure keyword filter to the event metadata.

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✗ **Blank 2: EventData** EventData
EventData is not the field that carries the audit-failure keyword value. Selecting it would not test the event's Keywords against `0x8010000000000000`.

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✓ **Blank 2: Keywords** Keywords
Keywords is the field that identifies the audit-failure event category in this filter. With System selected in Blank 1, this produces the required check for `0x8010000000000000`.

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

✗ **Blank 2: System** System
System is the enclosing section, not the field being compared with the keyword value. Blank 1 already selects this section; Blank 2 must select Keywords.

https://learn.microsoft.com/en-us/azure/sentinel/connect-services-windows-based

Dumpsgate

Question 17

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft 365 B5 subscription that contains a user named User1. The subscription uses Microsoft 365 Copilot for Security. Copilot for Security uses the Sentinel plugin. User1 is assigned the Copilot Contributor role.

During an investigation, User1 submits a prompt and receives a notification that Copilot for Security cannot respond to requests because the security compute unit (SCU) usage is nearing the provisioned capacity limit.

You need to ensure that User1 can use Copilot for Security to generate a successful response.

What should User1 do?

A. Open a second Copilot for Security session and submit the prompt.
B. Wait one hour and resubmit the prompt.
C. Run the Microsoft Sentinel Optimization Workbook.
D. Update the provisioned SCUs.

Answer: D. Update the provisioned SCUs.

Explanation

The notification indicates that Copilot for Security is constrained by the provisioned security compute unit (SCU) capacity, so opening another session or waiting does not address the capacity limit. Increasing the

provisioned SCUs provides additional capacity for Copilot to process User1's prompt and generate a response. The Sentinel Optimization Workbook is not a way to increase Copilot for Security SCU capacity.

https://learn.microsoft.com/security-copilot/manage-usage
https://learn.microsoft.com/en-us/copilot/security/security-compute-units-capacity

✗ **A** Open a second Copilot for Security session and submit the prompt.
A second session does not increase the provisioned SCU capacity; it would still be subject to the same capacity constraint. The notification identifies capacity as the problem, not the session User1 is using.

https://learn.microsoft.com/security-copilot/manage-usage
https://learn.microsoft.com/en-us/copilot/security/security-compute-units-capacity

✗ **B** Wait one hour and resubmit the prompt.
Waiting does not raise the provisioned SCU limit. The stated issue is that usage is nearing the provisioned capacity limit, so User1 needs more capacity rather than simply retrying later.

https://learn.microsoft.com/security-copilot/manage-usage
https://learn.microsoft.com/en-us/copilot/security/security-compute-units-capacity

✗ **C** Run the Microsoft Sentinel Optimization Workbook.
The Sentinel Optimization Workbook is not the control for increasing the SCUs provisioned for Copilot for Security. The scenario calls for addressing Copilot's SCU capacity limit directly.

https://learn.microsoft.com/en-us/copilot/security/security-compute-units-capacity
https://learn.microsoft.com/en-us/cloud-computing/finops/toolkit/workbooks/optimization

✓ **D** Update the provisioned SCUs.
Increasing the provisioned SCUs addresses the capacity limit identified in the notification and gives Copilot for Security more compute capacity to process the prompt. This is the relevant action for enabling a successful response.

https://learn.microsoft.com/security-copilot/manage-usage
https://learn.microsoft.com/en-us/copilot/security/security-compute-units-capacity

Question 18

Single choice · Domain: D1 Manage a security operations environment › Configure detections

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. The subscription contains 500 Windows 11 devices that are onboarded to Microsoft Defender for Endpoint You discover unauthorized changes to the membership of the Administrators group on the devices. You need to configure a solution that meets the following requirements:

- Every hour, check the Administrators group membership of each endpoint.
- When a change to the Administrators group membership is detected, create an incident in Microsoft Defender XDR.

What should you create first?

A. a device group
B. a detection rule
C. an alert tuning rule
D. an advanced hunting query

Answer: D. an advanced hunting query

Dumpsgate

Question 19

Single choice · Domain: D1 Manage a security operations environment › Configure the Microsoft Sentinel SIEM and platform

You have a Microsoft 365 E5 subscription that contains two users named Userl and User2 and From the Copilot for Security portal, User1 starts a session and creates the following prompts:

- Prompt1: Provides access to the Entra plugin
- Prompt2: Provides access to the Intune plugin
- Prompt3: Provides access to the Entra plugin

User1 shares the session with User2.

User2 does NOT have access to Microsoft Intune.

For which prompts can User2 view results during the shared session?

A. Prompt1 only
B. Prompt1 and Prompt2 only
C. Prompt3 only
D. Prompt1 and Prompt3 only
E. Prompt1, Prompt2, and Prompt3

Answer: D. Prompt1 and Prompt3 only

Explanation

User2 can view results for prompts that use a plugin they're authorized to access. Prompt1 and Prompt3 use the Entra plugin, while Prompt2 uses the Intune plugin, and User2 does not have access to Intune. Therefore, User2 can view the results for Prompt1 and Prompt3 only.

https://learn.microsoft.com/en-us/copilot/security/manage-plugins?tabs=securitycopilotplugin
https://learn.microsoft.com/en-us/intune/intune-service/copilot/security-copilot
https://learn.microsoft.com/copilot/security/use-plugins

✗ **A** Prompt1 only
Prompt1 uses the Entra plugin, so User2 can view its results. But Prompt3 also uses the Entra plugin and is viewable for the same reason, so this choice leaves out a prompt User2 can access.

https://learn.microsoft.com/en-us/copilot/security/manage-plugins?tabs=securitycopilotplugin
https://learn.microsoft.com/copilot/security/use-plugins

✗ **B** Prompt1 and Prompt2 only
Prompt1 is viewable because it uses the Entra plugin. Prompt2 uses the Intune plugin, and User2 does not have access to Intune, so User2 cannot view its results; this choice also omits Prompt3, which uses Entra.

https://learn.microsoft.com/en-us/copilot/security/manage-plugins?tabs=securitycopilotplugin
https://learn.microsoft.com/en-us/intune/intune-service/copilot/security-copilot
https://learn.microsoft.com/copilot/security/use-plugins

✗ **C** Prompt3 only
Prompt3 uses the Entra plugin and is viewable, but Prompt1 also uses Entra and is viewable. This choice incorrectly excludes Prompt1.

https://learn.microsoft.com/en-us/copilot/security/manage-plugins?tabs=securitycopilotplugin
https://learn.microsoft.com/copilot/security/use-plugins

✓ **D** Prompt1 and Prompt3 only
Both Prompt1 and Prompt3 use the Entra plugin, so User2 can view their results in the shared session.

Free demo · full exam: 392 questions

Prompt2 uses the Intune plugin, which User2 cannot access, so its results are not viewable by User2.

https://learn.microsoft.com/en-us/copilot/security/manage-plugins?tabs=securitycopilotplugin
https://learn.microsoft.com/en-us/intune/intune-service/copilot/security-copilot
https://learn.microsoft.com/copilot/security/use-plugins

✗ **E** Prompt1, Prompt2, and Prompt3
Prompt1 and Prompt3 use Entra and are viewable by User2. Prompt2 uses Intune, but User2 does not have access to Intune, so User2 cannot view its results.

https://learn.microsoft.com/en-us/copilot/security/manage-plugins?tabs=securitycopilotplugin
https://learn.microsoft.com/en-us/intune/intune-service/copilot/security-copilot
https://learn.microsoft.com/copilot/security/use-plugins

Question 20

Single choice · Domain: D1 Manage a security operations environment › Configure detections

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. All endpoint devices are onboarded to Microsoft Defender for Endpoint.

You have an Azure subscription that contains a Microsoft Sentinel workspace named Workspace 1.

All Microsoft Defender XDR events are ingested into Workspace1.

You have a Microsoft Entra tenant.

You create a KQL query named query1 that searches device logs for a known vulnerability.

You need to ensure that query1 runs every hour. The solution must minimize administrative effort.

What should you configure?

A. an automation rule
B. automated investigation and response (AIR)
C. a watchlist
D. a custom detection rule

Answer: D. a custom detection rule

Explanation

Configure a custom detection rule in Microsoft Defender XDR using query1. Custom detection rules let you turn an advanced hunting query into a recurring detection, and an hourly schedule meets the requirement for query1 to run every hour with minimal administrative effort. The ingested Defender XDR data and onboarded endpoints provide the context for detecting the known vulnerability.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide
https://learn.microsoft.com/defender-xdr/custom-detection-rules
https://learn.microsoft.com/en-us/defender-xdr/custom-detections-overview/?wt.mc_id=SEC-MVP-5005030
https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-defender-use-custom-rules

✗ **A** an automation rule
Sentinel automation rules automate actions on incidents, such as changing incident properties or triggering playbooks; they do not schedule and run a KQL query every hour. They therefore do not meet the query execution requirement.

https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules
https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules

Free demo · full exam: 392 questions

✗ **B** automated investigation and response (AIR)
AIR investigates alerts and can take remediation actions; it is not the feature for scheduling query1 to run hourly. A custom detection rule is designed to run a hunting query on a recurring schedule.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide
https://learn.microsoft.com/defender-xdr/custom-detection-rules
https://learn.microsoft.com/en-us/defender-xdr/custom-detections-overview/?wt.mc_id=SEC-MVP-5005030

✗ **C** a watchlist
A watchlist stores reference data that can be used in queries, such as lists of known values. It does not schedule or execute query1, so it would not satisfy the hourly-run requirement.

https://learn.microsoft.com/en-us/azure/sentinel/watchlists
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/watchlist
https://learn.microsoft.com/en-us/azure/sentinel/watchlists-create?tabs=azure-portal

✓ **D** a custom detection rule
A custom detection rule can use an advanced hunting query such as query1 and run it on a recurring schedule. Configure it to run hourly so the vulnerability search is automated without manually rerunning the query.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide
https://learn.microsoft.com/defender-xdr/custom-detection-rules
https://learn.microsoft.com/en-us/defender-xdr/custom-detection-manage
https://learn.microsoft.com/en-us/defender-xdr/custom-detections-overview/?wt.mc_id=SEC-MVP-5005030
https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-defender-use-custom-rules

---

Question 21

Single choice · Domain: D1 Manage a security operations environment › Configure automation for Microsoft Defender XDR and Microsoft Sentinel

Your on-premises network contains two Active Directory Domain Services (AD DS) domains named contoso.com and fabrikam.com. Contoso.com contains a group named Group1. Fabrikam.com contains a group named Group2.

You have a Microsoft Sentinel workspace named WS1 that contains a scheduled query rule named Rule1. Rule1 generates alerts in response to anomalous AD DS security events. Each alert creates an incident.

You need to implement an incident triage solution that meets the following requirements:

- Security incidents from contoso.com must be assigned to Group1.
- Security incidents from fabrikam.com must be assigned to Group2.
- Administrative effort must be minimized.

What should you include in the solution?

A. one automation rule assigned to Rule1
B. a playbook that is triggered by the creation of an incident
C. two automation rules assigned to Rule1
D. a playbook that is triggered by the creation of an alert

Answer: C. two automation rules assigned to Rule1

Explanation

Use two automation rules associated with Rule1, with each rule matching incidents for one AD DS domain and assigning them to the corresponding group. Automation rules can be scoped to a specific analytics rule and apply incident actions such as assigning an owner, so this avoids building and maintaining a custom playbook. Separate rules are needed because the two domains require different assignment targets.

https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules
https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules

✗ **A** one automation rule assigned to Rule1
A single rule can apply an assignment action to matching incidents, but the scenario requires different groups for incidents from contoso.com and fabrikam.com. One rule would not provide the separate domain-specific assignments required.

https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules
https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules

✗ **B** a playbook that is triggered by the creation of an incident
A playbook could implement conditional assignment logic, but it requires creating and maintaining a workflow for this task. Automation rules provide the needed incident assignment actions with less administrative effort.

https://learn.microsoft.com/en-us/azure/sentinel/automation/run-playbooks
https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules
https://learn.microsoft.com/en-us/azure/sentinel/automation/automate-responses-with-playbooks

✓ **C** two automation rules assigned to Rule1
Create one rule to assign contoso.com incidents to Group1 and another to assign fabrikam.com incidents to Group2. Automation rules can be associated with an analytics rule and can apply incident actions, meeting both routing requirements without a custom playbook.

https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules
https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules

✗ **D** a playbook that is triggered by the creation of an alert
The required action is to assign incidents to different groups, and the question specifies that each alert creates an incident. An alert-triggered playbook is not the least-administrative approach; automation rules can handle incident assignment directly and be associated with Rule1.

https://learn.microsoft.com/en-us/azure/sentinel/automation/run-playbooks
https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules
https://learn.microsoft.com/en-us/azure/sentinel/automation/playbook-triggers-actions

Question 22

Multiple choice · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender XDR

You have a Microsoft 365 E5 subscription.

You need to configure Microsoft Defender XDR automatic attack disruption to use signals generated by Microsoft Defender for Cloud Apps.

Which two actions should you perform for Defender for Cloud Apps in the Microsoft Defender portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Deploy Cloud Discovery user enrichment.
B. Turn on app governance.
C. From Information protection, enable file monitoring.
D. Add a log collector for automatic log upload.
E. Enable the Microsoft 365 connector.

Answer

- B. **Turn on app governance.**
- E. **Enable the Microsoft 365 connector.**

Explanation

Enable app governance so Defender for Cloud Apps can generate governance signals about OAuth-enabled apps, and enable the Microsoft 365 connector so the relevant Microsoft 365 activity is connected to Defender for Cloud Apps. These are the two actions required for Defender for Cloud Apps signals to be available to automatic attack disruption in this scenario.

https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started
https://learn.microsoft.com/hr-hr/defender-xdr/configure-attack-disruption
https://learn.microsoft.com/en-us/defender-cloud-apps/protect-office-365
https://learn.microsoft.com/en-us/defender-xdr/automatic-attack-disruption

✗ **A** Deploy Cloud Discovery user enrichment.
Cloud Discovery user enrichment adds user context to discovered cloud-app traffic; it does not enable app governance or connect Microsoft 365 signals for automatic attack disruption.

✓ **B** Turn on app governance.
App governance monitors and governs OAuth-enabled apps and can produce signals about suspicious app activity. Turning it on provides a required Defender for Cloud Apps signal source for automatic attack disruption.

https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started
https://learn.microsoft.com/hr-hr/defender-xdr/configure-attack-disruption
https://learn.microsoft.com/en-us/defender-xdr/automatic-attack-disruption

✗ **C** From Information protection, enable file monitoring.
File monitoring is an information-protection capability for monitoring files in cloud apps. It is not the app-governance or Microsoft 365 connector setup required here.

https://learn.microsoft.com/en-us/defender-cloud-apps/protect-office-365

✗ **D** Add a log collector for automatic log upload.
A log collector is used to upload network traffic logs for Cloud Discovery. It does not configure the app-governance signal source or the Microsoft 365 connector for this scenario.

✓ **E** Enable the Microsoft 365 connector.
Enabling the Microsoft 365 connector connects Microsoft 365 activity to Defender for Cloud Apps. This

Free demo · full exam: 392 questions

supplies the Microsoft 365 data needed for Defender for Cloud Apps signals to be used by Defender XDR automatic attack disruption.

https://learn.microsoft.com/hr-hr/defender-xdr/configure-attack-disruption
https://learn.microsoft.com/en-us/defender-cloud-apps/protect-office-365
https://learn.microsoft.com/en-us/defender-xdr/automatic-attack-disruption

Dumpsgate

Question 23

Drag and drop · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender XDR

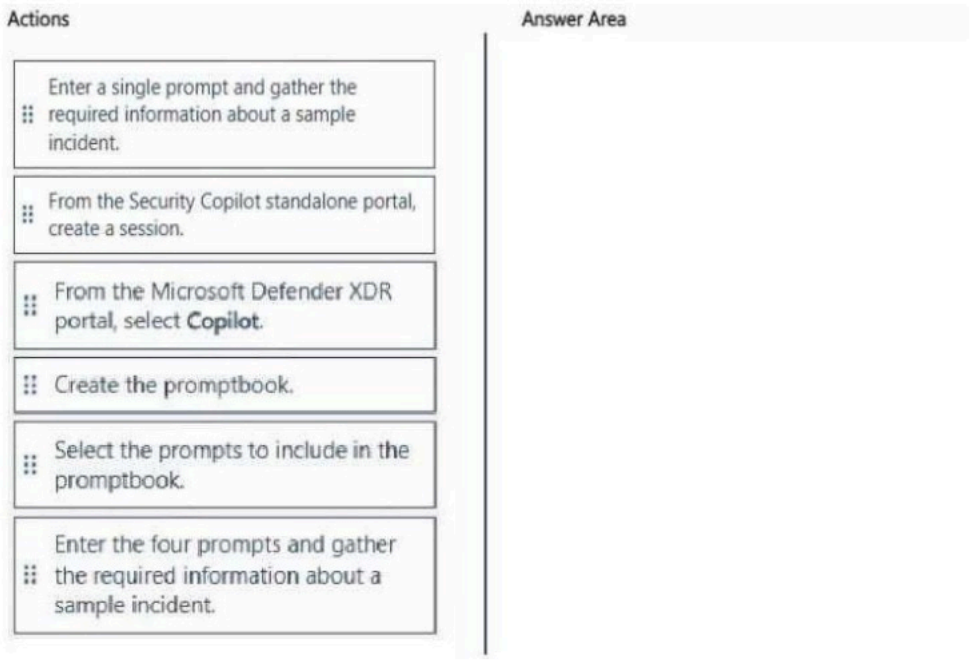
You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You have an Azure subscription that uses Microsoft Security Copilot.

You need to create a custom promptbook in Security Copilot that will gather the following information about an incident ID:

- An incident summary
- Threat intelligence on the identified threat actors
- A detailed analysis of the users affected by the incident.
- A detailed analysis of the devices affected by the incident

Which four 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.



Items:

- A. Enter a single prompt and gather the required information about a sample incident.
- B. From the Security Copilot standalone portal, create a session.
- C. From the Microsoft Defender XDR portal, select Copilot.
- D. Create the promptbook.
- E. Select the prompts to include in the promptbook.
- F. Enter the four prompts and gather the required information about a sample incident.

Place them on:

1. Step 1
2. Step 2
3. Step 3
4. Step 4

Answer

- Step 1 → **C. From the Microsoft Defender XDR portal, select Copilot.**
- Step 2 → **D. Create the promptbook.**
- Step 3 → **E. Select the prompts to include in the promptbook.**
- Step 4 → **F. Enter the four prompts and gather the required information about a sample incident.**

Explanation

Open Security Copilot from the Microsoft Defender XDR portal, where it can use the incident context needed for this task. Create a promptbook, choose the prompts for the incident summary, threat intelligence, and affected-user and device analyses, then run those four prompts against a sample incident to gather the required information. A standalone session or a single prompt would not create and populate the requested four-prompt promptbook.

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot?view=o365-worldwide
https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/en-us/defender-xdr/security-copilot-in-microsoft-365-defender

✗ **Enter a single prompt and gather the required information about a sample incident.** Enter a single prompt and gather the required information about a sample incident.
This gathers information with one prompt, but the promptbook must include four prompts to address the incident summary, threat actors, affected users, and affected devices. The sequence instead selects the prompts for the promptbook and then runs all four against a sample incident.

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot?view=o365-worldwide

✗ **From the Security Copilot standalone portal, create a session.** From the Security Copilot standalone portal, create a session.
A standalone session is not the specified entry point for this sequence. The correct action is to open Copilot from the Microsoft Defender XDR portal, which provides the relevant Defender context for investigating an incident.

https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/en-us/defender-xdr/security-copilot-in-microsoft-365-defender

✓ **From the Microsoft Defender XDR portal, select Copilot.** From the Microsoft Defender XDR portal, select Copilot.
This is the first step: open Copilot from Defender XDR so the workflow is connected to the security environment containing the incident. After opening Copilot, create the promptbook and configure its prompts.

https://learn.microsoft.com/en-us/copilot/security/navigating-security-copilot
https://learn.microsoft.com/en-us/defender-xdr/security-copilot-in-microsoft-365-defender

✓ **Create the promptbook.** Create the promptbook.
Once Copilot is open from Defender XDR, create the promptbook that will hold the reusable incident-investigation prompts. The prompts are selected for inclusion after the promptbook is created.

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot?view=o365-worldwide

✓ **Select the prompts to include in the promptbook.** Select the prompts to include in the promptbook.
The promptbook needs prompts covering all four requested outputs: a summary, threat intelligence, affected users, and affected devices. Select those prompts before running them on a sample incident.

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot?view=o365-worldwide
https://learn.microsoft.com/en-us/security-copilot/prompting-tips

✓ **Enter the four prompts and gather the required information about a sample incident.** Enter the four prompts and gather the required information about a sample incident.
After selecting the prompts, enter and run the four prompts against a sample incident to verify that they gather the required information. This final step tests the promptbook's prompts against the scenario's incident-analysis requirements.

Free demo · full exam: 392 questions

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot?view=o365-worldwide
https://learn.microsoft.com/en-us/security-copilot/prompting-tips

Question 24

Single choice · Domain: D2 Respond to security incidents › Investigate Microsoft 365 activities to identify threats

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.

You delete users from the subscription.

You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.

What should you use?

A. an access review in Microsoft Entra
B. a file policy in Microsoft Defender for Cloud Apps
C. an insider risk management policy in Microsoft Purview
D. an alert policy in Microsoft Defender for Office 365

Answer: C. an insider risk management policy in Microsoft Purview

Explanation

Use an insider risk management policy in Microsoft Purview. Insider risk management can identify risky activity such as a user downloading many SharePoint documents, including activity that occurred before the user was deleted, and generate an alert based on the policy. The other choices do not provide this combination of retrospective activity detection and insider-risk alerting.

✗ **A** an access review in Microsoft Entra
Access reviews are used to periodically review whether users should retain access to resources. They do not detect or alert on a deleted user's earlier pattern of downloading numerous SharePoint documents.

https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview?WT.mc_id=AZ-MVP-33518
https://learn.microsoft.com/en-us/entra/id-governance/manage-user-access-with-access-reviews

✗ **B** a file policy in Microsoft Defender for Cloud Apps
A file policy in Defender for Cloud Apps focuses on file-related conditions and actions, rather than evaluating a user's prior activity as insider risk. The requirement is to be alerted about numerous downloads in the month before account deletion.

✓ **C** an insider risk management policy in Microsoft Purview
Insider risk management policies can detect risky user activities, including downloading many files from SharePoint, and raise alerts for investigation. This is suited to identifying suspicious activity in the period before a user's account was deleted.

✗ **D** an alert policy in Microsoft Defender for Office 365
Defender for Office 365 alert policies address alerts related to its protection and security workloads, not insider-risk analysis of SharePoint document download activity before account deletion. Use Purview insider risk management for this scenario.

Question 25

Single choice · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender XDR

You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security. You have a Copilot for Security workspace that uses the following plugins:

- Microsoft Entra
- Microsoft Defender XDR

From the Microsoft Defender portal, you use Copilot for Security to investigate a reported incident.

You need to run a promptbook that will include information from Microsoft Entra ID Protection in the investigation. What should you do first?

A. From the Microsoft Defender portal, create an incident report
B. From the Microsoft Defender portal, create an advanced hunting query.
C. Open the investigation in the Copilot for Security standalone experience.
D. Open the investigation in Microsoft Sentinel.

Answer: C. Open the investigation in the Copilot for Security standalone experience.

Explanation

Open the investigation in the Copilot for Security standalone experience first. The scenario requires a promptbook to include Microsoft Entra ID Protection information, and the standalone experience supports access to the broader Copilot for Security experience and its plugins; the embedded Microsoft Defender portal experience does not provide the needed path for this investigation. [1] [10]

https://learn.microsoft.com/copilot/security/experiences-security-copilot
https://learn.microsoft.com/en-us/copilot/security/using-promptbooks

✗ **A** From the Microsoft Defender portal, create an incident report
Creating an incident report does not change which Copilot for Security experience is being used or enable the promptbook to use Microsoft Entra ID Protection information. The required first step is to open the investigation in the standalone experience.

https://learn.microsoft.com/copilot/security/experiences-security-copilot
https://learn.microsoft.com/en-us/copilot/security/using-promptbooks

✗ **B** From the Microsoft Defender portal, create an advanced hunting query.
An advanced hunting query is not the step that makes Entra ID Protection information available to a promptbook. You must first open the investigation in the standalone Copilot for Security experience, where the relevant plugin functionality can be used.

https://learn.microsoft.com/copilot/security/experiences-security-copilot
https://learn.microsoft.com/copilot/security/use-plugins

✓ **C** Open the investigation in the Copilot for Security standalone experience.
The standalone experience is the required starting point for running a promptbook that needs information from Microsoft Entra ID Protection in this scenario. It provides access to Copilot for Security's broader plugin and promptbook capabilities, beyond the embedded Defender portal experience.

https://learn.microsoft.com/copilot/security/experiences-security-copilot
https://learn.microsoft.com/copilot/security/use-plugins
https://learn.microsoft.com/en-us/copilot/security/using-promptbooks

✗ **D** Open the investigation in Microsoft Sentinel.
Opening the investigation in Sentinel is not required to access Microsoft Entra ID Protection information through the configured Copilot for Security plugins. The needed step is to use the Copilot for Security standalone experience.

Free demo · full exam: 392 questions

https://learn.microsoft.com/copilot/security/experiences-security-copilot
https://learn.microsoft.com/copilot/security/use-plugins

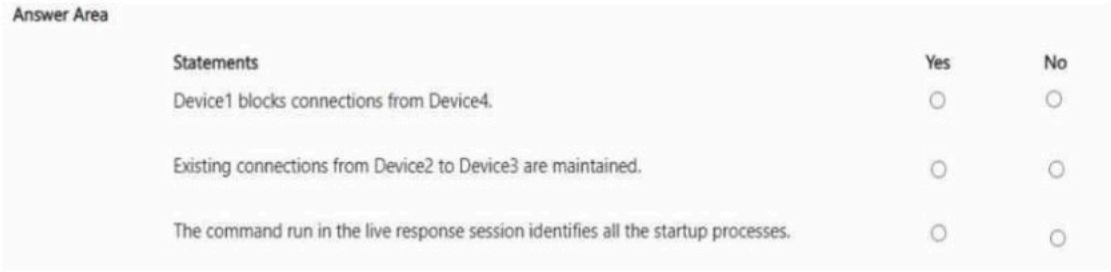
Question 26

Yes / No · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender for Endpoint

You have a Microsoft 365 subscription that uses Microsoft Defender XDR and Microsoft Defender for Endpoint. The subscription contains the devices shown in the following table.

Name	Microsoft Defender status	Operating system
Device1	Onboarded	Windows
Device2	Onboarded	Windows
Device3	Onboarded	Windows
Device4	Network discovered	Other

Name	Microsoft Defender status	Operating system
Device1	Onboarded	Windows
Device2	Onboarded	Windows
Device3	Onboarded	Windows
Device4	Network discovered	Other



You discover the following forensic data:

- During the startup of Device1, a connection is established to Device2 via port 5555.
- Device2 connects to Device3 by using port 5555.
- Device4 connects to Device1 by using port 5555.

You perform the following actions:

- Initiate a live response session on Device1 and run the processes command.
- From Devices in the Microsoft Defender portal, isolate Device1 and Device2.

For each of the following statements, select Yes if True. Otherwise select No.

NOTE: Each correct selection is worth one point.

Statements:

1. Device1 blocks connections from Device4.
2. Existing connections from Device2 to Device3 are maintained.

3. The command run in the live response session identifies all the startup processes.

Statement	Yes	No
Device1 blocks connections from Device4.	☐	☐
Existing connections from Device2 to Device3 are maintained.	☐	☐
The command run in the live response session identifies all the startup processes.	☐	☐

Answer

- Device1 blocks connections from Device4. **Yes**
- Existing connections from Device2 to Device3 are maintained. **No**
- The command run in the live response session identifies all the startup processes. **No**

Explanation

Isolating Device1 blocks its network connections, including the connection from Device4 over port 5555. Isolating Device2 interrupts its connection to Device3, so that existing connection is not maintained. The live response `processes` command lists running processes; it does not identify all startup processes.

https://learn.microsoft.com/en-us/defender-endpoint/live-response-command-examples
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/isolate-machine

✓ **Statement 1** Device1 blocks connections from Device4.
Device1 is isolated, which blocks its network connections other than permitted Defender connectivity. Device4's connection to Device1 over port 5555 is therefore blocked; Device4 being network discovered does not make that connection an exception.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/isolate-machine

✗ **Statement 2** Existing connections from Device2 to Device3 are maintained.
Device2 is isolated, so its connection to Device3 is not maintained as an ordinary network connection. Isolation restricts the device's network connectivity, even though the connection existed before isolation.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/isolate-machine

✗ **Statement 3** The command run in the live response session identifies all the startup processes.
The live response `processes` command displays running processes; it does not identify all processes configured to start at startup. The statement claims broader startup-process identification than the command provides.

https://learn.microsoft.com/en-us/defender-endpoint/live-response-command-examples

Free demo · full exam: 392 questions

Question 27

Yes / No · Domain: D2 Respond to security incidents › Investigate Microsoft 365 activities to identify threats

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online. You identify the suspicious emails shown in the following table.

Name	From	Subject	Date received	Attachment
Email1	prizes@contoso.com	You have WON a free gold coin	1/1/2024	File1.docx
Email2	hrhr@contoso.com	Update your benefits in the Contoso HR portal	1/1/2024	None
Email3	benefits@contoso.com	You have WON a free gold coin	1/1/2024	None

Name	From	Subject	Date received	Attachment
Email1	prizes@contoso.com	You have WON a free gold coin	1/1/2024	File1.docx
Email2	hrhr@contoso.com	Update your benefits in the Contoso HR portal	1/1/2024	None
Email3	benefits@contoso.com	You have WON a free gold coin	1/1/2024	None

Name	Location	KQL query
Search1	Exchange mailboxes	(c:c)(filetype=docx) (senderauthor=prizes@contoso.com)
Search2	Exchange mailboxes	(c:c)(-subjecttitle=benefits) (from=hrhr@contoso.com)
Search3	Exchange mailboxes	(c:c)(subjecttitle=won) (from=benefits@contoso.com)

Answer Area

Statements	Yes	No
Search1 will include Email1.	○	○
Search2 will include Email2.	○	○
Search3 will include Email3.	○	○
	○	○

In the Microsoft Purview portal, you create the content searches shown in the following table.

Name	Location	KQL query
Search1	Exchange mailboxes	(c:c) (filetype=docx) (senderauthor=prizes@contoso.com)
Search2	Exchange mailboxes	(c:c)(-subjecttitle=benefits) (from=hrhr@contoso.com)
Search3	Exchange mailboxes	(c:c)(subjecttitle~won) (from=benefits@contoso.com)

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer

- Search1 will include Email1. **Yes**
- Search2 will include Email2. **No**
- Search3 will include Email3. **Yes**

Explanation

Search1 matches Email1 because it has a DOCX attachment and was sent by prizes@contoso.com. Search2 excludes Email2 because its subject contains “benefits,” which conflicts with the negative subject condition. Search3 matches Email3 because its subject contains “WON” and its sender is benefits@contoso.com.

https://learn.microsoft.com/en-us/purview/edisc-condition-builder

✓ **Statement 1** Search1 will include Email1.
Search1 requires a DOCX file type and the sender prizes@contoso.com. Email1 has a File1.docx attachment and that sender, so it meets both conditions.

https://learn.microsoft.com/en-us/purview/edisc-condition-builder

✗ **Statement 2** Search2 will include Email2.
Search2 requires the sender to be hrhr@contoso.com, which Email2 satisfies. However, the negative subject condition excludes messages whose subject contains “benefits,” and Email2’s subject is “Update your benefits in the Contoso HR portal.”

https://learn.microsoft.com/en-us/purview/edisc-condition-builder

✓ **Statement 3** Search3 will include Email3.
Search3 requires the subject to contain “won” and the sender to be benefits@contoso.com. Email3’s subject contains “WON,” and its sender matches, so it meets both conditions.

https://learn.microsoft.com/en-us/purview/edisc-condition-builder

Question 28

Single choice · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender for Endpoint

You have a Microsoft 365 E5 subscription that contains a device named Device1. From the Microsoft Defender portal, you discover that an alert was triggered for Device1. From the Device inventory page, you isolate Device1. You need to collect a list of installed programs on Device1. What should you do?

A. Run an advanced hunting query against the DeviceTvmInfoGathering table.
B. Initiate a live response session and run the processes command.
C. Run an advanced hunting query against the DeviceTvmSoftwareInventory table.
D. Run an advanced hunting query against the DeviceProcessEvents table.

Answer: C. Run an advanced hunting query against the DeviceTvmSoftwareInventory table.

Explanation

Free demo · full exam: 392 questions

To collect installed programs, query the `DeviceTvmSoftwareInventory` table, which contains software inventory information for devices. This directly addresses the requirement to list programs installed on Device1; process activity or a list of currently running processes would not provide that inventory.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicetvmsoftwareinventory-table
https://learn.microsoft.com/en-us/defender-vulnerability-management/tvm-software-inventory

✗ **A** Run an advanced hunting query against the DeviceTvmInfoGathering table.
This table is not the software inventory table needed to retrieve installed programs. Use `DeviceTvmSoftwareInventory` for device software inventory instead.

https://learn.microsoft.com/defender-xdr/advanced-hunting-schema-tables

✗ **B** Initiate a live response session and run the processes command.
The `processes` command returns process information, such as processes running on the device, rather than a list of installed programs. The requirement is to collect software inventory, not current process activity.

https://learn.microsoft.com/en-us/defender-endpoint/live-response-command-examples

✓ **C** Run an advanced hunting query against the DeviceTvmSoftwareInventory table.
The intended table is `DeviceTvmSoftwareInventory`, which provides information about software installed on devices. Querying it is the appropriate way to collect the installed-program list for Device1.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicetvmsoftwareinventory-table
https://learn.microsoft.com/en-us/defender-vulnerability-management/tvm-software-inventory

✗ **D** Run an advanced hunting query against the DeviceProcessEvents table.
`DeviceProcessEvents` contains process creation and other process-related events, not a complete inventory of installed programs. A program being recorded as a process event does not establish that this table provides the requested installed-software list.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-deviceprocessevents-table

Dumpsgate

Question 29

Hotspot (dropdowns) · Domain: D2 Respond to security incidents › Investigate Microsoft 365 activities to identify threats

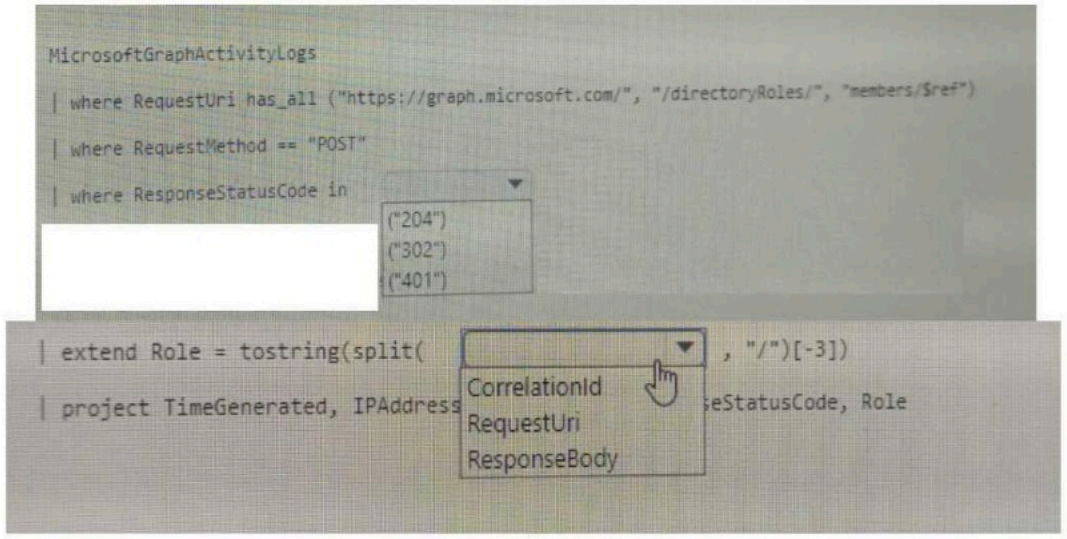
You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.

You need to query Microsoft Graph activity logs to identify changes to the roles in contoso.com.

How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
MicrosoftGraphActivityLogs
| where RequestUri has_all ("https://graph.microsoft.com/", "/directoryRoles/", "members/$r
| where RequestMethod == "POST"
| where ResponseStatusCode in [Blank 1]
| extend Role = tostring(split([Blank 2], "/")[-3])
| project TimeGenerated, IPAddress, ResponseStatusCode, Role
```



Blank 1 (where ResponseStatusCode in ...): ("204") | ("302") | ("401")

Blank 2 (extend Role = tostring(split(..., "/")[-3])): CorrelationId | RequestUri | ResponseBody

Answer

- Blank 1 (where ResponseStatusCode in ...): **("204")**
- Blank 2 (extend Role = tostring(split(..., "/")[-3])): **RequestUri**

Explanation

A successful POST that adds a member to a directory role returns HTTP 204, so that is the response code to filter for. The role ID is embedded in the request URI between `/directoryRoles/` and `/members/$ref`; splitting that URI on `/` and selecting the third element from the end extracts it as `Role`.

https://learn.microsoft.com/en-us/graph/api/directoryrole-post-members?view=graph-rest-1.0
https://learn.microsoft.com/en-us/graph/microsoft-graph-activity-logs-overview

✓ **Blank 1: ("204")** ("204")
The query filters for successful POST requests that add a member to a directory role. The directory-role members API returns 204 when the operation succeeds.
https://learn.microsoft.com/en-us/graph/api/directoryrole-post-members?view=graph-rest-1.0

✗ **Blank 1: ("302")** ("302")
A 302 response indicates a redirect, not the success response for adding a directory-role member. Filtering on it would not identify the successful changes requested here.
https://learn.microsoft.com/en-us/graph/api/directoryrole-post-members?view=graph-rest-1.0

✗ **Blank 1: ("401")** ("401")
A 401 response indicates an unauthorized request, not a successful role membership change. It therefore does not identify completed changes to the role.
https://learn.microsoft.com/en-us/graph/api/directoryrole-post-members?view=graph-rest-1.0

✗ **Blank 2: CorrelationId** CorrelationId
A correlation ID is not the URL path containing the directory role ID. Splitting it on `/` would not extract the role ID needed for the `Role` column.

✓ **Blank 2: RequestUri** RequestUri
The request URI contains the path `/directoryRoles/{role-id}/members/$ref`. Splitting that path on `/` and selecting the element three positions from the end yields the role ID.
https://learn.microsoft.com/en-us/graph/api/directoryrole-post-members?view=graph-rest-1.0
https://learn.microsoft.com/en-us/graph/microsoft-graph-activity-logs-overview

✗ **Blank 2: ResponseBody** ResponseBody
The role ID is identified in the request path, not by splitting the response body. Using `ResponseBody` would not reliably extract the role ID required by this query.
https://learn.microsoft.com/en-us/graph/api/directoryrole-post-members?view=graph-rest-1.0

Question 30

Single choice · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender for Endpoint

You have a Microsoft 365 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

The timeline of Device1 includes three files named File1.ps1, File2.exe, and File3.dll.

You need to submit files for deep analysis in Microsoft Defender XDR.

Which files can you submit?

A. File1.ps1 only
B. File2.exe only
C. File3.dll only
D. File2.exe and File3.dll only
E. File1.ps1 and File2.exe only
F. File1.ps1, File2.exe, and File3.dll

Answer: D. File2.exe and File3.dll only

Explanation

For deep analysis from Device1's timeline, Microsoft Defender XDR supports submitting executable files such as .exe and .dll files. File2.exe and File3.dll meet that requirement, while File1.ps1 is a PowerShell script and is not eligible for this submission workflow. Therefore, the correct choice is D.

https://learn.microsoft.com/en-us/unified-secops/submission-guide

✗ **A** File1.ps1 only
A .ps1 file is a PowerShell script, not one of the executable file types supported for deep analysis submission from the device timeline. It therefore cannot be submitted through the workflow described.

https://learn.microsoft.com/en-us/unified-secops/submission-guide

✗ **B** File2.exe only
File2.exe is an eligible executable file, but it is not the only eligible file in the timeline. File3.dll can also be submitted.

https://learn.microsoft.com/en-us/unified-secops/submission-guide

✗ **C** File3.dll only
File3.dll is an eligible executable file, but it is not the only eligible file in the timeline. File2.exe can also be submitted.

https://learn.microsoft.com/en-us/unified-secops/submission-guide

✓ **D** File2.exe and File3.dll only
Both .exe and .dll files are supported for deep analysis submission from the device timeline. File1.ps1 is a script and is not eligible, so this is the complete set of files that can be submitted.

https://learn.microsoft.com/en-us/unified-secops/submission-guide

✗ **E** File1.ps1 and File2.exe only
File2.exe is eligible, but File1.ps1 is not supported for this deep analysis submission workflow. This option also incorrectly omits the eligible File3.dll.

https://learn.microsoft.com/en-us/unified-secops/submission-guide

✗ **F** File1.ps1, File2.exe, and File3.dll
File2.exe and File3.dll are eligible, but File1.ps1 is not supported for deep analysis submission from the device timeline. Including all three files makes this choice incorrect.

https://learn.microsoft.com/en-us/unified-secops/submission-guide

Question 31

Single choice · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender XDR

You need to update the threat intelligence list to include the entities.

Which entities can you add on the Incident page?

A. 175.45.176.99 only
B. Host1 only
C. Used only
D. 175.45.176.99 and Host1 only
E. Host1 and User1 only
F. 175.45.176.99, Host1, and User1

Answer: A. 175.45.176.99 only

Explanation

The Incident page supports adding the IP address entity 175.45.176.99 to the threat intelligence list. Host1 and User1 are not entities that can be added through this workflow, so the IP address alone is the correct choice. [1]

https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

✓ **A** 175.45.176.99 only
The Incident page workflow supports adding the IP address entity to threat intelligence. Host1 and User1 are not supported for this action, so this is the only correct choice.

https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

✗ **B** Host1 only
Host1 is a host entity, not the IP address entity supported by this Incident page workflow for adding to threat intelligence.

https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

✗ **C** Used only
This option does not identify the supported IP address, 175.45.176.99. The supported entity in the scenario is the IP address alone.

https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

✗ **D** 175.45.176.99 and Host1 only
Although 175.45.176.99 can be added, Host1 cannot be added through this workflow. Including Host1 makes this choice incorrect.

https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

✗ **E** Host1 and User1 only
Neither Host1 nor User1 is the supported IP address entity. The Incident page workflow allows adding 175.45.176.99, which this option omits.

https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

✗ **F** 175.45.176.99, Host1, and User1
The IP address can be added, but Host1 and User1 cannot be added through this workflow. The choice therefore includes unsupported entities.

https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

Dumpsgate

Question 32

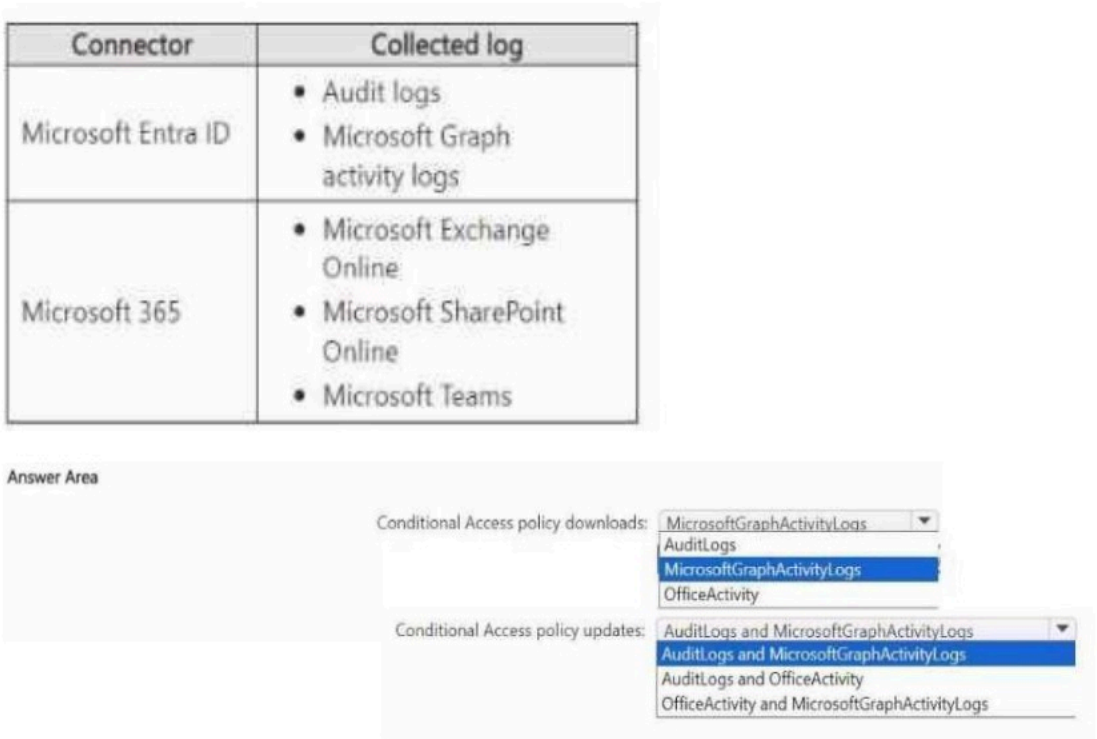
Hotspot (dropdowns) · Domain: D2 Respond to security incidents › Investigate Microsoft 365 activities to identify threats

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You have a Microsoft Sentinel workspace.

Microsoft Sentinel connectors are configured as shown in the following table.

Connector	Collected log
Microsoft Entra ID	Audit logs; Microsoft Graph activity logs
Microsoft 365	Microsoft Exchange Online; Microsoft SharePoint Online; Microsoft Teams



You use Microsoft Sentinel to investigate suspicious Microsoft Graph API activity related to Conditional Access policies. You need to search for the following activities:

- Downloads of the Conditional Access policies by using PowerShell
- Updates to the Conditional Access policies by using the Microsoft Entra admin center

Which tables should you query for each activity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Conditional Access policy downloads: AuditLogs | MicrosoftGraphActivityLogs | OfficeActivity

Conditional Access policy updates: AuditLogs and MicrosoftGraphActivityLogs | AuditLogs and OfficeActivity | OfficeActivity and MicrosoftGraphActivityLogs

Free demo · full exam: 392 questions

Answer

- Conditional Access policy downloads: **MicrosoftGraphActivityLogs**
- Conditional Access policy updates: **AuditLogs and MicrosoftGraphActivityLogs**

Explanation

Query MicrosoftGraphActivityLogs for Conditional Access policy downloads performed through PowerShell because these are Microsoft Graph API requests. For policy updates made in the Microsoft Entra admin center, query both AuditLogs and MicrosoftGraphActivityLogs: AuditLogs records the directory change, while MicrosoftGraphActivityLogs provides the related Graph API activity. OfficeActivity is for Microsoft 365 services such as Exchange, SharePoint, and Teams, not these Entra activities.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-policy-changes-audit-log
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-analyze-activity-logs-with-microsoft-graph

✗ **Box 1: AuditLogs** Conditional Access policy downloads — AuditLogs
AuditLogs is useful for reviewing changes to Conditional Access policies, but it is not the appropriate table for searching the Graph API requests that downloaded the policies through PowerShell. For that request activity, query MicrosoftGraphActivityLogs.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-policy-changes-audit-log
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-analyze-activity-logs-with-microsoft-graph

✓ **Box 1: MicrosoftGraphActivityLogs** Conditional Access policy downloads — MicrosoftGraphActivityLogs
PowerShell downloads of Conditional Access policies use Microsoft Graph API requests. MicrosoftGraphActivityLogs captures Microsoft Graph activity, making it the appropriate table for finding those requests.

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-analyze-activity-logs-with-microsoft-graph

✗ **Box 1: OfficeActivity** Conditional Access policy downloads — OfficeActivity
OfficeActivity contains activity for Microsoft 365 services such as Exchange Online, SharePoint Online, and Teams. It does not provide the Graph API request telemetry needed to find these Entra Conditional Access policy downloads.

https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/officeactivity

✓ **Box 2: AuditLogs and MicrosoftGraphActivityLogs** Conditional Access policy updates — AuditLogs and MicrosoftGraphActivityLogs
An update made in the Microsoft Entra admin center is a directory change that is recorded in AuditLogs. Querying MicrosoftGraphActivityLogs as well provides the associated Microsoft Graph API activity, so both tables are needed for the specified investigation.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-policy-changes-audit-log
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-analyze-activity-logs-with-microsoft-graph

✗ **Box 2: AuditLogs and OfficeActivity** Conditional Access policy updates — AuditLogs and OfficeActivity
AuditLogs can show the Conditional Access policy change, but OfficeActivity records Microsoft 365 workload activity rather than the Microsoft Graph activity relevant to this Entra admin center update. Use MicrosoftGraphActivityLogs alongside AuditLogs instead.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-policy-changes-audit-log
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/officeactivity
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-analyze-activity-logs-with-microsoft-graph

✗ **Box 2: OfficeActivity and MicrosoftGraphActivityLogs** Conditional Access policy updates — OfficeActivity and MicrosoftGraphActivityLogs
MicrosoftGraphActivityLogs provides the Graph API activity, but OfficeActivity does not record the Entra directory audit event showing the Conditional Access policy change. AuditLogs is needed alongside MicrosoftGraphActivityLogs.

Free demo · full exam: 392 questions

https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-policy-changes-audit-log
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/officeactivity
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-analyze-activity-logs-with-microsoft-graph

Question 33

Hotspot (dropdowns) · Domain: D2 Respond to security incidents › Respond to alerts and incidents in Microsoft Defender for Endpoint

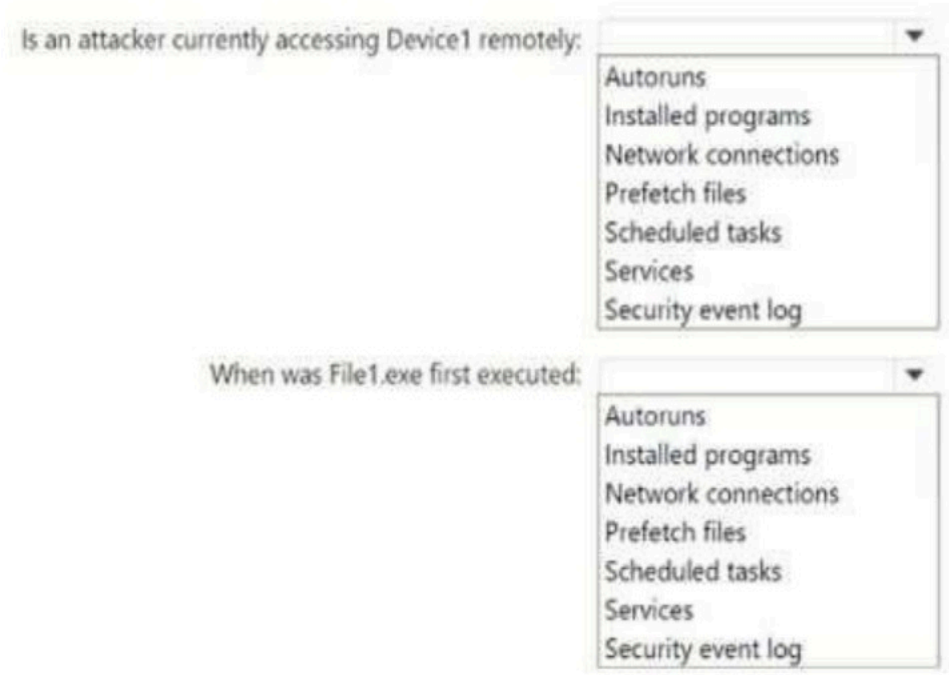
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

You investigate Device1 for malicious activity and discover a suspicious file named File1.exe. You collect an investigation package from Device1.

You need to review the following forensic data points:

- Is an attacker currently accessing Device1 remotely?
- When was File1.exe first executed?

Which folder in the investigation package should you review for each data point? To answer, select the appropriate options in the answer area.



Is an attacker currently accessing Device1 remotely?: Autoruns | Installed programs | Network connections | Prefetch files | Scheduled tasks | Services | Security event log

When was File1.exe first executed?: Autoruns | Installed programs | Network connections | Prefetch files | Scheduled tasks | Services | Security event log

Answer

- Is an attacker currently accessing Device1 remotely?: **Network connections**
- When was File1.exe first executed?: **Prefetch files**

Explanation

Review **Network connections** to determine whether Device1 has active remote connections, which can indicate that an attacker is currently accessing it remotely. Review **Prefetch files** to find execution artifacts for File1.exe and determine when it was first run. These folders address the two distinct forensic questions in the investigation package. [3]

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 1: Autoruns** Is an attacker currently accessing Device1 remotely? — Autoruns
Autoruns shows programs configured to run automatically, such as startup entries; it does not show whether a remote connection is active now.

https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns?trk=article-ssr-frontend-pulse_little-text-block

✗ **Box 1: Installed programs** Is an attacker currently accessing Device1 remotely? — Installed programs
The installed-programs data can help identify software on Device1, but it does not indicate whether an attacker is currently connected remotely.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✓ **Box 1: Network connections** Is an attacker currently accessing Device1 remotely? — Network connections
Network connections are the relevant data for checking whether Device1 currently has remote connections that could indicate active remote access.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 1: Prefetch files** Is an attacker currently accessing Device1 remotely? — Prefetch files
Prefetch files can provide evidence that an executable ran, but they do not show whether an attacker is currently accessing Device1 remotely.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 1: Scheduled tasks** Is an attacker currently accessing Device1 remotely? — Scheduled tasks
Scheduled tasks show configured tasks and their execution schedule; they do not establish whether a remote attacker is connected now.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 1: Services** Is an attacker currently accessing Device1 remotely? — Services
Services data can help identify services running on the device, but it does not directly show current remote connections.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 1: Security event log** Is an attacker currently accessing Device1 remotely? — Security event log
Security event logs may contain historical security events, but the Network connections data is the appropriate source for checking current remote access.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 2: Autoruns** When was File1.exe first executed? — Autoruns
Autoruns identifies entries configured to start automatically; it does not provide the execution timestamp needed for File1.exe.

https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns?trk=article-ssr-frontend-pulse_little-text-block

✗ **Box 2: Installed programs** When was File1.exe first executed? — Installed programs
Installed-programs data concerns software installation, not when this executable was first run.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 2: Network connections** When was File1.exe first executed? — Network connections
Network connections can help investigate remote access, but they do not provide the first-execution time

Free demo · full exam: 392 questions

for File1.exe.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✓ **Box 2: Prefetch files** When was File1.exe first executed? — Prefetch files
Prefetch files contain execution artifacts that can be reviewed to determine when File1.exe was run, making this the appropriate folder for the first-execution question.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 2: Scheduled tasks** When was File1.exe first executed? — Scheduled tasks
Scheduled tasks can show whether a task is configured to launch a program, but that does not establish when File1.exe was first executed.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 2: Services** When was File1.exe first executed? — Services
Services data describes services on the device; it is not the appropriate source for the first-execution time of File1.exe.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

✗ **Box 2: Security event log** When was File1.exe first executed? — Security event log
The security event log records security-related events, but Prefetch files are the relevant execution artifacts for determining when File1.exe was first run.

https://learn.microsoft.com/en-us/defender-endpoint/collect-diagnostic-data

Dumpsgate

Question 34

Hotspot (dropdowns) · Domain: D3 Perform threat hunting › Detect threats by using Microsoft Defender XDR

You have a Microsoft 365 subscription.

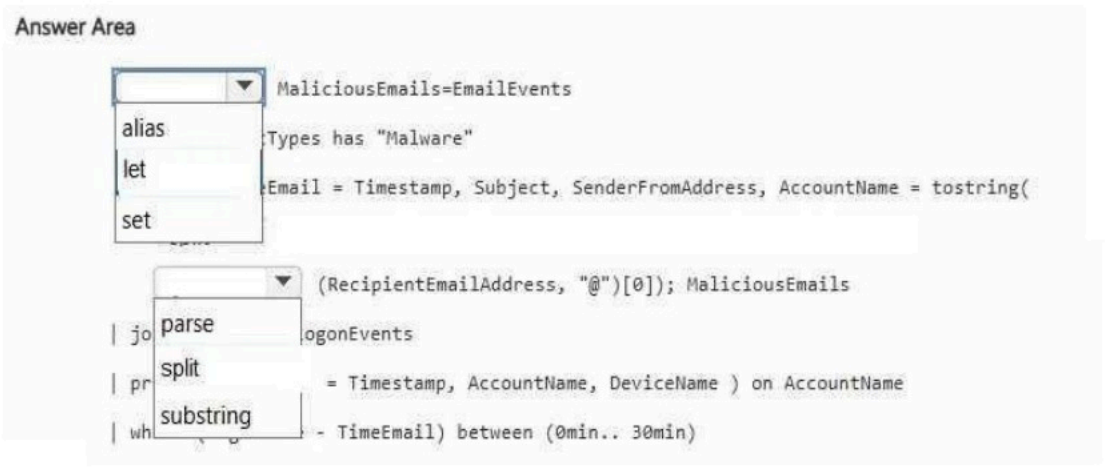
You plan to use Microsoft Defender XDR to hunt for email-related threats.

You need to identify sign-ins performed by users within 30 minutes of the users receiving a known malicious email.

How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
[Blank 1] MaliciousEmails=EmailEvents
| where ThreatTypes has "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName = tostring(
    [Blank 2] (RecipientEmailAddress, "@")[0]); MaliciousEmails
| join ( IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName ) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 30min)
```



Blank 1 (before MaliciousEmails=EmailEvents): alias | let | set

Blank 2 (before (RecipientEmailAddress, "@")[0]): parse | split | substring

Answer

- Blank 1 (before MaliciousEmails=EmailEvents): **let**
- Blank 2 (before (RecipientEmailAddress, "@")[0]): **split**

Explanation

Use `let` to define `MaliciousEmails` as the result of the `EmailEvents` query so it can be referenced later in the query. Use `split` on `RecipientEmailAddress` with `@` as the delimiter, then select element `[0]` to obtain the account name used to join the email events to sign-in events. The join and time filter then identify sign-ins occurring from 0 to 30 minutes after the malicious email timestamp.

https://learn.microsoft.com/en-us/kusto/query/split-function?view=microsoft-fabric
https://learn.microsoft.com/en-us/kusto/query/let-statement?view=azure-data-explorer

✗ **Blank 1: alias** alias
`alias` is not the KQL statement used here to define a named result set. The query needs `let` so that `MaliciousEmails` can be assigned the `EmailEvents` results and referenced later.

https://learn.microsoft.com/en-us/kusto/query/let-statement?view=azure-data-explorer

✓ **Blank 1: let** let
`let` defines the `MaliciousEmails` name and binds it to the `EmailEvents` query results. This lets the later query refer to `MaliciousEmails` when projecting and joining the email data.

https://learn.microsoft.com/en-us/kusto/query/let-statement?view=azure-data-explorer

✗ **Blank 1: set** set
`set` configures query options; it does not define the named tabular value `MaliciousEmails` needed by the later query. `let` is the appropriate statement for that assignment.

https://learn.microsoft.com/en-us/kusto/query/let-statement?view=azure-data-explorer

✗ **Blank 2: parse** parse
`parse` is not the function needed to divide the email address at the `@` delimiter and select the portion before it. The expression requires a function that returns the address components as an array.

✓ **Blank 2: split** split
`split(RecipientEmailAddress, "@")` divides the recipient address into components at the `@` delimiter. Index `[0]` selects the first component, which the query converts to a string for `AccountName`.

https://learn.microsoft.com/en-us/kusto/query/split-function?view=microsoft-fabric

✗ **Blank 2: substring** substring
`substring` selects characters by position and length; it does not split the address at the `@` delimiter into an array whose first element can be selected with `[0]`. `split` matches the expression shown in the query.

Dumpsgate

Question 35

Hotspot (dropdowns) · Domain: D3 Perform threat hunting › Detect threats by using Microsoft Defender XDR

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

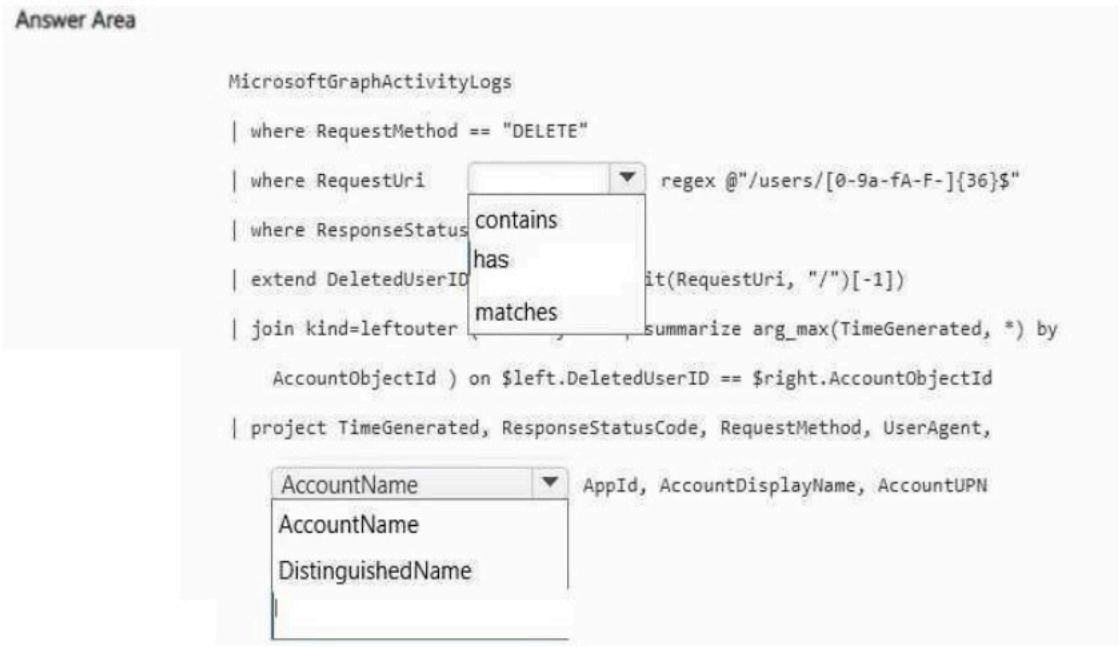
You plan to investigate suspicious activity in the subscription by using Microsoft Graph activity logs.

You need to search for requests to delete resources from the subscription and identify the users that initiated the requests.

How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
MicrosoftGraphActivityLogs
| where RequestMethod == "DELETE"
| where RequestUri [Blank 1] regex @"/users/[0-9a-fA-F-]{36}$"
| where ResponseStatusCode == "204"
| extend DeletedUserID = tostring(split(RequestUri, "/")[-1])
| join kind=leftouter (IdentityInfo | summarize arg_max(TimeGenerated, *) by AccountObjectI
| project TimeGenerated, ResponseStatusCode, RequestMethod, UserAgent, [Blank 2] AppId, Acc
```



Blank 1 (RequestUri [Blank 1] regex @"/users/[0-9a-fA-F-]{36}$"): contains | has | matches

Blank 2 (project … UserAgent, [Blank 2] AppId, AccountDisplayName, AccountUPN): AccountName | DistinguishedName

Answer

- Blank 1 (RequestUri [Blank 1] regex @"/users/[0-9a-fA-F-]{36}$"): **matches**
- Blank 2 (project … UserAgent, [Blank 2] AppId, AccountDisplayName, AccountUPN): **AccountName**

Dumpsgate

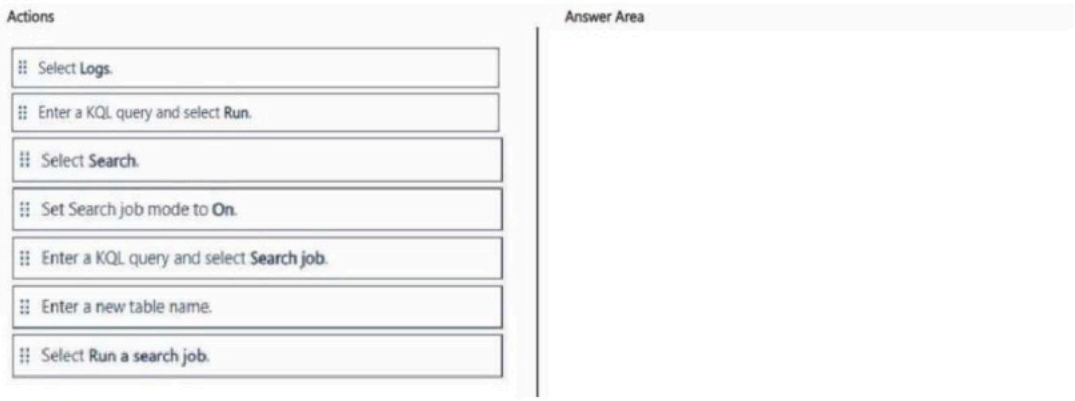
Question 36

Drag and drop · Domain: D3 Perform threat hunting › Detect threats by using the Microsoft Sentinel platform

You have a Microsoft Sentinel workspace named Workspace1.

You need to run a KQL query as a search job.

Which five actions should you perform in Workspace 1 in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Items:

- A. Select Logs.
- B. Enter a KQL query and select Run.
- C. Select Search.
- D. Set Search job mode to On.
- E. Enter a KQL query and select Search job.
- F. Enter a new table name.
- G. Select Run a search job.

Place them on:

1. Step 1
2. Step 2
3. Step 3
4. Step 4
5. Step 5

Answer

- Step 1 → **C. Select Search.**
- Step 2 → **D. Set Search job mode to On.**
- Step 3 → **E. Enter a KQL query and select Search job.**
- Step 4 → **F. Enter a new table name.**
- Step 5 → **G. Select Run a search job.**

Explanation

To run a KQL query as a search job, use the Search workflow rather than the standard Logs query flow. Turn on Search job mode, submit the query with Search job, provide a new table name, and then run the search job. The other listed actions either start a regular query or do not belong to this search-job

Free demo · full exam: 392 questions

sequence.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

✗ **Select Logs.** Select Logs.
This opens the standard Logs query experience, but the required sequence begins by selecting Search to create a search job.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

✗ **Enter a KQL query and select Run.** Enter a KQL query and select Run.
Selecting Run executes a regular query, not the search-job workflow. For a search job, submit the query using Search job after enabling Search job mode.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

✓ **Select Search.** Select Search.
This starts the search workflow needed to run the KQL query as a search job. It is the first action in the required sequence.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

✓ **Set Search job mode to On.** Set Search job mode to On.
Enabling Search job mode configures the Search experience to submit the query as a search job. This follows selecting Search and comes before entering the query.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

✓ **Enter a KQL query and select Search job.** Enter a KQL query and select Search job.
This submits the KQL query using the search-job action rather than running it as a standard query. It follows enabling Search job mode.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

✓ **Enter a new table name.** Enter a new table name.
A new table name is required as part of setting up the search job output. Enter it after submitting the query and before running the job.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

✓ **Select Run a search job.** Select Run a search job.
This is the final action that starts the configured search job after the query and new table name have been provided.

https://learn.microsoft.com/en-us/azure/sentinel/search-jobs

Dumpsgate

Question 37

Hotspot (dropdowns) · Domain: D3 Perform threat hunting › Detect threats by using Microsoft Defender XDR

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You discover a malicious process that was initiated by a file named File1exe on a device named Device1.

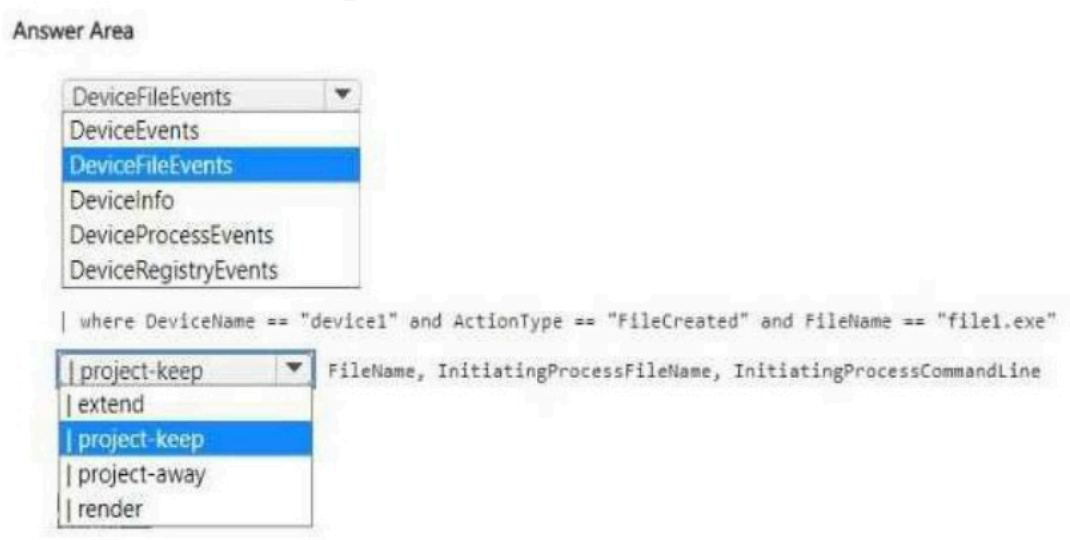
You need to create a KQL query that will identify when File1.exe was created. The solution must meet the following requirements:

- Return the FileName, InitiatingProcessFileName, and InitiatingProcessCommandLine columns.
- Minimize the volume of data returned.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
[Blank 1]
| where DeviceName == "device1" and ActionType == "FileCreated" and FileName == "file1.exe"
| [Blank 2] FileName, InitiatingProcessFileName, InitiatingProcessCommandLine
```



Blank 1 (table before | where DeviceName == "device1"): DeviceEvents | DeviceFileEvents | DeviceInfo | DeviceProcessEvents | DeviceRegistryEvents

Blank 2 (operator before FileName, InitiatingProcessFileName, InitiatingProcessCommandLine): extend | project-keep | project-away | render

Answer

- Blank 1 (table before | where DeviceName == "device1"): **DeviceFileEvents**
- Blank 2 (operator before FileName, InitiatingProcessFileName, InitiatingProcessCommandLine): **project-keep**

Explanation

Use the DeviceFileEvents table because the query filters for a file creation action and needs file-event fields such as FileName and initiating process details. Then use project-keep to retain only FileName,

InitiatingProcessFileName, and InitiatingProcessCommandLine, minimizing the columns returned as required.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table
https://learn.microsoft.com/defender-xdr/advanced-hunting-schema-tables

✗ **Blank 1: DeviceEvents** DeviceEvents
DeviceEvents is not the specific table for file activity; this query needs the file event record for the FileCreated action and its file and initiating-process columns.

https://learn.microsoft.com/defender-xdr/advanced-hunting-schema-tables

✓ **Blank 1: DeviceFileEvents** DeviceFileEvents
DeviceFileEvents contains file creation activity and the FileName and initiating-process fields used by the query. It is therefore the appropriate table for identifying when File1.exe was created.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table
https://learn.microsoft.com/defender-xdr/advanced-hunting-schema-tables

✗ **Blank 1: DeviceInfo** DeviceInfo
DeviceInfo contains device information rather than per-file event records. It cannot provide the matching FileCreated event and the requested initiating-process details.

https://learn.microsoft.com/defender-xdr/advanced-hunting-schema-tables
https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-deviceinfo-table

✗ **Blank 1: DeviceProcessEvents** DeviceProcessEvents
DeviceProcessEvents is intended for process events, while the query filters on ActionType == "FileCreated" and seeks a file creation event. DeviceFileEvents is the relevant event table.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table
https://learn.microsoft.com/defender-xdr/advanced-hunting-schema-tables

✗ **Blank 1: DeviceRegistryEvents** DeviceRegistryEvents
DeviceRegistryEvents records registry activity, not file creation activity. It does not fit the FileCreated filter in this query.

https://learn.microsoft.com/defender-xdr/advanced-hunting-schema-tables

✗ **Blank 2: extend** extend
extend adds or calculates columns; it does not restrict the output to the three requested columns. That would not minimize the returned columns.

✓ **Blank 2: project-keep** project-keep
project-keep retains only the named columns, so the result contains FileName, InitiatingProcessFileName, and InitiatingProcessCommandLine. This meets the requested output and reduces the returned data.

✗ **Blank 2: project-away** project-away
project-away removes the named columns from the result, which would discard the three columns the query must return. It does not select only those requested fields.

https://learn.microsoft.com/en-us/kusto/query/project-away-operator

✗ **Blank 2: render** render
render is used to display query results as a visualization, not to retain only specified columns. It does not satisfy the requirement to limit the returned columns.

Free demo · full exam: 392 questions

Question 38

Single choice · Domain: D3 Perform threat hunting › Detect threats by using Microsoft Defender XDR

You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1. WS1 has the Azure Activity connector and the Microsoft Entra ID connector configured.

You need to investigate which accounts have the most alerts and any corresponding incident information for each alert. The solution must minimize administrative effort What should you do first in WS1?

A. Enable User and Entity Behavior Analytics (UEBA).
B. From Content hub, install Cloud Identity Threat Protection Essentials.
C. From Content hub, install the Microsoft Purview insider risk management solution.
D. Use User and Entity Behavior Analytics (UEBA) to detect anomalies.

Answer: B. From Content hub, install Cloud Identity Threat Protection Essentials.

Explanation

Install Cloud Identity Threat Protection Essentials from the Content hub first. This Sentinel solution provides the content needed to review which accounts have the most alerts and see associated incident information, avoiding the need to build that view manually. Installing a solution from Content hub is the relevant first step for adding packaged Sentinel content to WS1.

https://learn.microsoft.com/en-us/azure/sentinel/sentinel-solutions

✗ **A** Enable User and Entity Behavior Analytics (UEBA).
UEBA can help identify anomalous user and entity behavior, but enabling it alone does not add the packaged account alert and corresponding incident view requested here. The solution from Content hub is the more direct first step.

https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics

✓ **B** From Content hub, install Cloud Identity Threat Protection Essentials.
This installs the Sentinel solution content suited to investigating identity-related alerts by account and reviewing related incident information. Installing the packaged solution is the lowest-effort first action rather than creating or assembling the investigation view yourself.

https://learn.microsoft.com/en-us/azure/sentinel/sentinel-solutions

✗ **C** From Content hub, install the Microsoft Purview insider risk management solution.
Insider risk management focuses on investigating insider-risk cases and related activities, which is not the requested account-centric view of alerts and their corresponding Sentinel incident information. It is not the appropriate solution for this task.

https://learn.microsoft.com/en-us/purview/purview-sentinel
https://learn.microsoft.com/en-us/purview/insider-risk-management

✗ **D** Use User and Entity Behavior Analytics (UEBA) to detect anomalies.
Detecting anomalies with UEBA is not the requested first step for reviewing accounts with the most alerts and incident details. UEBA can contribute behavioral insights, but it does not replace installing the packaged solution that supplies the needed investigation content.

https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics
https://learn.microsoft.com/en-us/azure/sentinel/ueba-anomalies-on-behaviors

Free demo · full exam: 392 questions

Question 39

Hotspot (dropdowns) · Domain: D3 Perform threat hunting › Detect threats by using Microsoft Defender XDR

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You need to create a hunting query in KQL that meets the following requirements:

- Identifies any devices That received an email containing an attachment named File1.pdf during the last 12 hours and opened the attachment.
- Minimizes the resources required to run the query.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
EmailAttachmentInfo
| where Timestamp > ago(12h)
| where Subject == "Document Attachment" and FileName == "File1.pdf"
| join kind=[Blank 1] (DeviceFileEvents | where Timestamp > ago(12h)) on [Blank 2]
```



Blank 1 (join kind=...): inner | innerunique | rightouter

Blank 2 (join ... on): FileOriginUrl | FilePath | SHA256

Answer

- Blank 1 (join kind=...): **innerunique**
- Blank 2 (join ... on): **SHA256**

Explanation

Use `innerunique` to keep only matching rows while deduplicating the left side of the join, which helps minimize query resources. Join on `SHA256` to correlate the email attachment with the file recorded in `DeviceFileEvents` when it was opened. The time filters on both tables restrict the search to the last 12 hours. [1][2][3]

https://learn.microsoft.com/en-us/kusto/query/join-innerunique?view=azure-data-explorer
https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

✗ **Box 1: inner** inner

An `inner` join returns matching rows, but it does not deduplicate the left-side rows as `innerunique` does by default. Since the query must minimize resources, `innerunique` is the better choice here.

https://learn.microsoft.com/en-us/kusto/query/join-innerunique?view=azure-data-explorer

✓ **Box 1: innerunique** innerunique
`innerunique` returns matching rows and deduplicates the left side of the join. That behavior suits this query's requirement to find matching attachment and device-file events while minimizing the work caused by duplicate left-side rows.

https://learn.microsoft.com/en-us/kusto/query/join-innerunique?view=azure-data-explorer

✗ **Box 1: rightouter** rightouter
`rightouter` preserves rows from the right-hand `DeviceFileEvents` input even when there is no matching email attachment. The query is looking for devices whose file events match the specified attachment, so unmatched right-side rows are unnecessary.

https://learn.microsoft.com/en-us/kusto/query/tutorials/join-data-from-multiple-tables

✗ **Box 2: FileOriginUrl** FileOriginUrl
`FileOriginUrl` is a URL value, not the attachment's content hash. Joining on it does not directly correlate the email attachment with the same file recorded in the device file events.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

✗ **Box 2: FilePath** FilePath
`FilePath` describes where a file is located on a device, whereas the email attachment record is matched to the device event by file identity. A path is not the appropriate shared key for correlating these records.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

✓ **Box 2: SHA256** SHA256
`SHA256` provides a hash that can identify the attachment's file in both the email attachment and device file event data. Joining on this value correlates the received attachment with the corresponding device event, which indicates that the file was opened.

https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

Dumpsgate

Question 40

Single choice · Domain: D3 Perform threat hunting › Detect threats by using Microsoft Defender XDR

You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security. You plan to run the following code to create a custom Copilot for Security plugin.

```
<code segment>
SkillGroups:
- Format: <target>
Skills:
```

You need to specify a format and complete the code segment. Which format should you use for the <target> variable?

A. API
B. GPT
C. KQL
D. SQL

Answer: C. KQL

Explanation

The code defines a skill group with a `Format` field, and the plugin is intended to use KQL skills. Set `<target>` to `KQL` so the custom Copilot for Security plugin interprets the skills as KQL content, as required by the KQL plugin format.

https://learn.microsoft.com/en-us/copilot/security/custom-plugins
https://learn.microsoft.com/id-id/copilot/security/plugin-kql

✗ **A** API
`API` is used for plugins that connect to an API, not for a skill group whose skills are written in KQL. This code segment needs to identify the KQL format.

https://learn.microsoft.com/en-us/copilot/security/plugin-api

✗ **B** GPT
`GPT` identifies a GPT-based plugin format, rather than the KQL format required for these skills. It would not specify the skill format shown in this code segment.

https://learn.microsoft.com/en-us/copilot/security/plugin-gpt

✓ **C** KQL
`KQL` is the format value for a Copilot for Security plugin whose skills use Kusto Query Language. Therefore, `<target>` should be replaced with `KQL`.

https://learn.microsoft.com/id-id/copilot/security/plugin-kql

✗ **D** SQL
The required format is KQL, not SQL. The code is for a KQL skill group, and SQL is not the format value needed here.

https://learn.microsoft.com/id-id/copilot/security/plugin-kql

Free demo · full exam: 392 questions

Dumpsgate

Free demo · full exam: 392 questions