DUMPSBOSS.

Microsoft Security Operations Analyst

Microsoft SC-200

Version Demo

Total Demo Questions: 58

Total Premium Questions: 580

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Mitigate threats by using Microsoft Defender XDR	287
Topic 2, Mitigate threats by using Microsoft Sentinel	259
Topic 3, Mix Questions	34
Total	580

QUESTION NO: 1

You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

A. Create an AWS user for Defender for Cloud.

B. Create an Access control (IAM) role for Defender for Cloud.

C. Configure AWS Security Hub.

D. Deploy the AWS Systems Manager (SSM) agent.

ANSWER: B

Explanation:

Create an Access control (IAM) role for Defender for Cloud. The native AWS connector uses AWS Identity and Access Management (IAM) to establish a secure, delegated trust relationship between Microsoft Defender for Cloud and the AWS account. The IAM role supplies the permissions Defender for Cloud needs to discover AWS resources, assess security posture, and enable the relevant Defender for Cloud plans and data collection capabilities. Rather than relying on persistent user credentials, Defender for Cloud is configured to assume this role through an AWS CloudFormation-based deployment or an equivalent manually configured role, using the required trust policy and permissions. Establishing this role is therefore the foundational AWS-side setup action before the connector can access the account and begin onboarding its security data. Microsoft's AWS onboarding guidance describes creating the necessary AWS CloudFormation stack and IAM roles as part of connecting an AWS account to Defender for Cloud. The role-based approach follows AWS least-privilege and temporary-credential practices while allowing Defender for Cloud to perform the connector's required inventory and security-management operations. See Connect AWS accounts to Defender for Cloud and Connect AWS accounts to Microsoft Defender for Cloud.

QUESTION NO: 2

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

B. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

C. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

D. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

A. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EFC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

B. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EFC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode

C. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EFC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode

D. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EFC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

ANSWER: B C

Explanation:

The commands using `AuditMode` for the ASR rule identified by `D4F940AB-401B-4EFC-AADC-AD5F3C50688A` are correct. This rule, named *Block all Office applications from creating child processes*, is designed to prevent Office applications such as Word, Excel, and PowerPoint from starting child processes. Such child-process creation is a common way for VBA macros to launch command shells, scripts, or additional payloads.

Deploying the rule in audit mode allows the organization to observe activity that the rule would block without disrupting line-of-business macro workflows. Potential rule matches are recorded in Microsoft Defender event telemetry, enabling security administrators to review the affected macros and evaluate the operational impact before changing the rule to enforced mode.

`Add-MpPreference` can add the specified ASR rule and action to Defender preferences, while `Set-MpPreference` can configure the specified ASR rule settings. In both cases, pairing the Office child-process rule ID with `AuditMode` achieves the required assessment. Microsoft recommends evaluating ASR rules in audit mode before enforcement. See Attack surface reduction rules reference and Add-MpPreference documentation.

QUESTION NO: 3

You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

A. Azure Synapse Analytics

B. Azure Databricks

C. Azure Machine Learning

D. Log Analytics workspace

ANSWER: D

Explanation:

Log Analytics workspace is correct because Microsoft Sentinel is enabled on an Azure Log Analytics workspace, which provides the data repository and Kusto Query Language (KQL) query capability used by Sentinel. After Sentinel is onboarded to the workspace and relevant data is collected through connectors, analysts can use the Hunting page to run built-in hunting queries, customize them, or create new KQL queries against the workspace's security data. Hunting is designed to proactively search collected logs for indicators of threats, anomalous activity, and entities of interest; therefore, access to the Sentinel-enabled Log Analytics workspace is the fundamental workspace requirement. A workspace also defines the data boundary that queries operate over, including its retained log data and any configured analytics content. Microsoft's Sentinel documentation states that onboarding Sentinel requires selecting or creating a Log Analytics workspace, and its hunting documentation describes using KQL queries to investigate data in that Sentinel workspace. For implementation details, see Quickstart: Onboard Microsoft Sentinel and Hunting in Microsoft Sentinel.

QUESTION NO: 4 - (DRAG DROP)

DRAG DROP

You have a Microsoft Sentinel workspace that contains the following Advanced Security Information Model (ASIM) parsers:

_Im_ProcessCreate

InProceessCreate

You create a new source-specific parser named vimProcessCreate.

You need to modify the parsers to meet the following requirements:

Call all the ProcessCreate parsers.

Standardize fields to the Process schema.

Which parser should you modify to meet each requirement? To answer, drag the appropriate parsers to the correct requirements. tach parser may be used once, more than once, or not at all You may need to drag the split bar between panes or scroll to view content. NOTE Each correct selection is worth one point.

ANSWER:

Explanation:

Microsoft Sentinel ASIM uses parser layers so that data from many security products can be queried through a consistent schema. The new **vimProcessCreate** parser is source-specific. Its role is to take the native fields emitted by the new data source and map them into the normalized field names, types, and values defined by the ASIM **Process** schema. Updating this parser ensures that the source's process-creation records are standardized before analysts, analytics rules, hunting queries, and other content consume them.

The **imProcessCreate** parser is the unifying parser for the ProcessCreate event type. It acts as the common entry point that calls and combines the available source-specific ProcessCreate parsers, including the new **vimProcessCreate** parser. Adding the new parser to this unifying function makes ProcessCreate queries that use the unified parser include records from the new source alongside the other normalized ProcessCreate sources.

This separation lets source-specific mapping remain focused on the source's native event format while the unifying parser provides a single, schema-level query experience. Microsoft documents that source-specific ASIM parsers normalize source events to an ASIM schema, and that unifying parsers combine source-specific parsers for a schema. See ASIM parsers overview and Microsoft Sentinel normalization and ASIM.

QUESTION NO: 5

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

Name	Operating system
Device1	Windows
Device2	Windows
Device3	Linux
Device4	macOS

You initiate a live response session on each device.

You need to collect a Defender for Endpoint investigation package from each device.

On which devices can you collect the package by running advanced live response commands from the command-line interface (CLI)?

A. Device1 and Device2 only

B. Device1, Device2, and Device3 only

C. Device3 and Device4 only

D. Device1, Device2, Device3, and Device4

ANSWER: B

Explanation:

Device1, Device2, and Device3 only is correct. Microsoft Defender for Endpoint Live Response includes the advanced `collect` command, which collects an investigation package from a supported endpoint and makes the resulting ZIP file available for download from the Live Response session. The command is supported for Windows devices and Linux devices. Therefore, the Windows devices represented by Device1 and Device2, together with the Linux device represented by Device3, can use the CLI-based advanced Live Response command to collect the package.

An investigation package is intended to provide security operations teams with relevant forensic and diagnostic data to support incident investigation. Depending on the platform, its contents can include data such as running processes, scheduled tasks, services, networking details, and relevant security-product information. Collecting it through Live Response is useful when an analyst needs to obtain the evidence directly from an active response session without separately accessing the endpoint.

Microsoft documents the platform availability of Live Response commands, including the advanced `collect` command, in the Live response documentation. For details about package contents and collection workflows, see Collect investigation packages from devices.

QUESTION NO: 6

You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector. You need to create a new near-real-time (NRT) analytics rule that will use the playbook. What should you configure for the rule?

A. the Incident automation settings

B. entity mapping

C. the query rule

D. the Alert automation settings

ANSWER: D

Explanation:

The correct configuration is **the Alert automation settings**. An NRT analytics rule generates an alert when its query detects matching events. Alert automation associates an eligible Microsoft Sentinel playbook with that analytics rule so that the

playbook runs automatically when the rule creates an alert. The playbook must use the Microsoft Sentinel alert trigger, enabling it to receive the alert context generated from Azure Activity data and perform the defined response actions immediately after detection.

Microsoft Sentinel supports automated response configuration as part of analytics-rule creation. In the rule's automated-response experience, the alert automation configuration is where a playbook is selected for direct execution in response to the alerts produced by that rule. This aligns the detection logic, which runs at the NRT cadence, with the response workflow without requiring manual analyst intervention. Microsoft's guidance on responding to threats describes attaching playbooks to analytics rules for alert-triggered automation, while the analytics-rule documentation covers the creation and configuration of NRT rules. See Automate threat responses with playbooks in Microsoft Sentinel and Create near-real-time analytics rules in Microsoft Sentinel.

QUESTION NO: 7

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. You need to implement deception rules. The solution must ensure that you can limit the scope of the rules. What should you create first?

A. device groups

B. device tags

C. honeytoken entity tags

D. sensitive entity tags

ANSWER: B

Explanation:

device tags is correct because Microsoft Defender XDR uses device tags to define the endpoint scope to which a deception rule applies. When creating a deception rule, administrators can select device tags so that the rule deploys deception content only to devices that have the chosen tag or tags. This supports a controlled rollout, such as applying a rule only to server devices, a pilot group, high-value endpoints, or devices in a particular business environment.

Tags must therefore be created and assigned to the intended devices before the deception rule is configured. The rule can then use those existing tags as its targeting criteria. This approach provides granular, operationally manageable scope without requiring the deception configuration to be applied across the entire tenant. Microsoft's deception guidance identifies device tags as the mechanism for scoping deception rules and describes selecting the relevant tagged devices during rule configuration. See Microsoft Defender XDR deception and Manage device tags in Microsoft Defender for Endpoint.

QUESTION NO: 8

You use Azure Defender.

You have an Azure Storage account that contains sensitive information.

You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.

B. Create an Azure logic app that has a manual trigger.

C. Create an Azure logic app that has an Azure Security Center alert trigger.

D. Create an Azure logic app that has an HTTP trigger.

E. From Azure Active Directory (Azure AD), add an app registration.

ANSWER: A C

Explanation:

From Azure Security Center, enable workflow automation, and create an Azure logic app that has an Azure Security Center alert trigger. Workflow automation in Microsoft Defender for Cloud is designed to initiate automated responses when security alerts are generated. It uses automation rules to select relevant Defender for Cloud alerts and invoke a Logic App, enabling a response to be initiated without manual intervention. The automation rule can be scoped and filtered so that alerts associated with suspicious access to the Storage account cause the workflow to run.

The Logic App must use the Microsoft Defender for Cloud alert trigger (formerly the Azure Security Center alert trigger). This trigger supplies the alert context to the playbook when Defender for Cloud creates the alert. The workflow can then use that context in subsequent actions, such as invoking an Azure Automation runbook that executes the required PowerShell, calling an Azure Function, or using another approved script-execution integration. Together, workflow automation provides the event-to-playbook connection, while the alert-triggered Logic App provides the automated response path needed for the PowerShell operation.

For implementation details, see Automate responses to Defender for Cloud alerts and Microsoft Defender for Cloud alerts.

QUESTION NO: 9

Which rule setting should you configure to meet the Microsoft Sentinel requirements?

A. From Set rule logic, turn off suppression.

B. From Analytic rule details, configure the tactics.

C. From Set rule logic, map the entities.

D. From Analytic rule details, configure the severity.

ANSWER: C

Explanation:

From Set rule logic, map the entities. Entity mapping associates fields returned by an analytics rule query with Microsoft Sentinel entity types, such as IP address, account, host, URL, file hash, or cloud application. For a requirement to make a specific source IP address available while navigating and investigating data-access activity, mapping the query's IP-address field to the IP entity creates the required relationship between the alert and that observable.

When the analytic rule generates alerts, Microsoft Sentinel uses the mapping to enrich those alerts with normalized entity information. The mapped IP then appears as an entity in the alert and incident context and can be explored through the investigation graph. This lets an analyst pivot from the alert to information connected with that IP address, review related activity, and use the entity as investigation context during hunting. Entity mapping is configured in the rule's Set rule logic step because it depends on the columns produced by the rule query and identifies which result columns represent each entity identifier.

Microsoft documents entity mapping as the mechanism for integrating recognized entities from scheduled analytics rules into alerts and investigations. See Map data fields to entities in Microsoft Sentinel and Investigate incidents with Microsoft Sentinel.

QUESTION NO: 10

You use Microsoft Defender for Cloud Apps and Microsoft Entra Conditional Access.

You need to prevent users from downloading files from SharePoint Online when they use unmanaged devices. The solution must allow users to view the files in a browser.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a Conditional Access policy that uses Conditional Access App Control.

B. Create a session policy that blocks downloads.

C. Create a file policy that quarantines all SharePoint files.

D. Create a Microsoft Purview retention policy.

E. Enable just-in-time VM access.

ANSWER: A B

Explanation:

Create a **Conditional Access policy that uses Conditional Access App Control**. This redirects applicable browser sessions to Microsoft Defender for Cloud Apps, where the session can be monitored and controlled. The policy can target SharePoint Online and apply conditions that identify unmanaged devices.

Create a **session policy** in Microsoft Defender for Cloud Apps that blocks downloads. Session policies provide real-time controls for browser sessions that are routed through Conditional Access App Control. Blocking downloads while allowing browser access satisfies the requirement to preserve viewing capability without allowing data to be saved to the unmanaged device.

For more information, see Deploy Conditional Access App Control for Microsoft Defender for Cloud Apps and Create session policies in Defender for Cloud Apps.

QUESTION NO: 11

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.

B. Create a hunting query that references the built-in parse.

C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.

D. Build a custom unify parse and include the build- parse version E. Create an analytics rule that includes the built-in parse

ANSWER: A D

Explanation:

Redeploying the built-in parser with **CallerContext=any** and **SourceSpecificParse=any** creates a workspace-level deployment of the parser configuration. This lets the workspace use the deployed parser rather than relying solely on the managed built-in parser update path. ASIM parser deployment parameters control the parser's intended calling context and whether it is used as a source-specific parser, enabling a locally managed parser deployment that can be maintained at the version required by the organization.

Building a custom unifying parser that includes a specific built-in parser version is also a complete solution because the custom unifying parser is customer-managed. The organization can explicitly control which parser implementation and version its ASIM-normalized queries invoke. Analytics rules, hunting queries, and other content can then call that custom parser, preserving predictable normalization behavior even when Microsoft releases newer versions of managed parser content. This approach is particularly useful where change-control processes require testing and approving parser changes before adopting them in production.

Microsoft describes ASIM normalization and the parser model, including unifying and source-specific parsers, in the ASIM normalization documentation and the ASIM parsers overview.

QUESTION NO: 12 - (SIMULATION)

You have a Microsoft 365 E5 subscription.

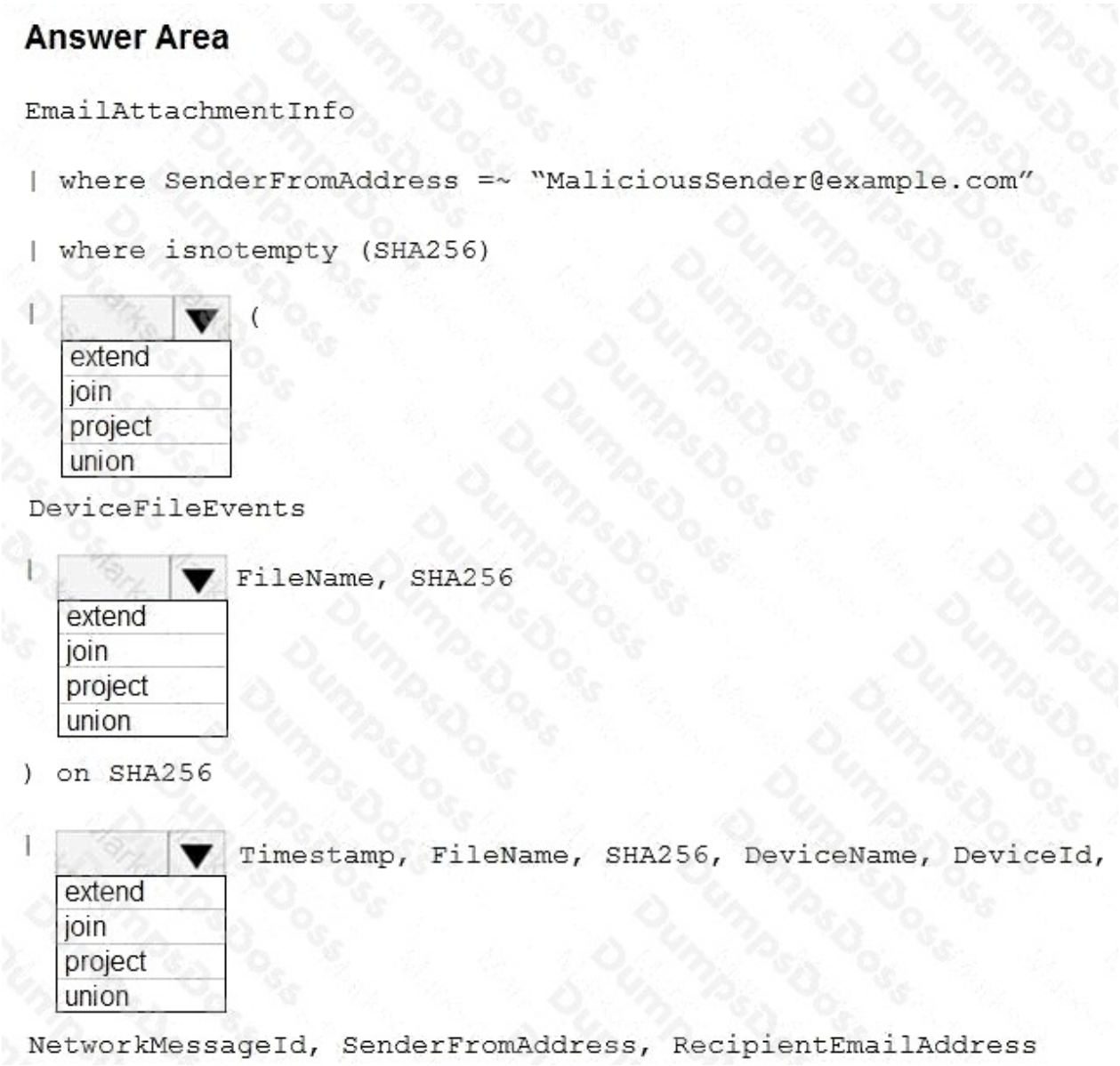
You plan to perform cross-d omain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

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

NOTE: Each correct selection is worth one point.

Answer Area



ANSWER: See the explanation for the answer

Explanation:

Select the operators in this order:

First blank: `join`
Blank inside the `DeviceFileEvents` subquery: `project`
Final blank: `project`

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty(SHA256)
```

```
| join (
    DeviceFileEvents
    | project FileName, SHA256
) on SHA256
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
          NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

`EmailAttachmentInfo` contains attachment metadata, including the SHA256 hash. The `join` correlates that hash with endpoint file events in `DeviceFileEvents`. Use `project` in the subquery and again after the join to return the relevant investigation fields.

QUESTION NO: 13

You have a Microsoft Sentinel workspace.

You need to generate incidents when firewall logs contain IP addresses that match known malicious threat intelligence indicators.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add a threat intelligence data connector.

B. Create an analytics rule that matches firewall events to threat intelligence indicators.

C. Create a hunting query only.

D. Create a workbook that displays firewall events.

E. Create a Microsoft Sentinel bookmark.

ANSWER: A B

Explanation:

Add a **threat intelligence data connector** to ingest the known malicious indicators into Microsoft Sentinel. Threat intelligence connectors ingest indicator data from supported sources, including TAXII feeds and threat intelligence platforms, and make the indicators available for analysis in the workspace.

Create an **analytics rule** that matches firewall-log IP addresses to the ingested indicators. The rule continuously evaluates the relevant firewall table and threat intelligence data, and it generates alerts and incidents when a match is found. Entity mappings can be added to expose the matching IP address as an incident entity.

A hunting query can identify historical matches but does not generate incidents automatically. For more information, see Microsoft Sentinel data connectors reference and Microsoft Sentinel analytics rules.

QUESTION NO: 14

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. user

B. resource group

C. IP address

D. computer

ANSWER: C D

Explanation:

IP address and **computer** are valid components for grouping related alerts into Microsoft Sentinel incidents. Sentinel analytics rules can map values returned by a Kusto query to recognized entity types, including IP and Host entities. The incident-creation experience can then use entity information to group alerts that are associated with the same relevant infrastructure or network endpoint. This reduces duplicate investigations while retaining the individual alerts as evidence within a shared incident.

For SecurityEvent data, the computer name is a natural Host entity value. The query's `HostCustomEntity = Computer` assignment explicitly provides the host value for Sentinel's entity mapping. An IP address returned by the event data can likewise be mapped as an IP entity and used as a shared grouping characteristic. These entity mappings make it possible to correlate repeated alerts involving a single machine or a single network address, even when alerts are generated separately for each matching event.

Microsoft documents entity mapping for analytics rules, including the Host and IP address entity types, and documents alert grouping as an analytics-rule incident setting. See Map data fields to entities in Microsoft Sentinel and Microsoft Sentinel alert grouping.

QUESTION NO: 15

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You need to prevent users from downloading and running additional payloads from the Office VBA macros as additional child processes.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

B. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

C. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

D. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: A B

Explanation:

The correct selections configure the Microsoft Defender Attack Surface Reduction rule named *Block all Office applications from creating child processes*. This rule is specifically designed to stop Office applications, including documents containing VBA macros, from launching child processes such as command shells, script hosts, or download tools that could retrieve and execute a second-stage payload. The applicable ASR rule GUID is `D4F940AB-401B-4EFC-AADC-AD5F3C50688A`. The valid commands use the Defender PowerShell `Set-MpPreference` cmdlet and the correctly named `-AttackSurfaceReductionRules_Ids` parameter to configure that rule. One correct command enables enforcement, while the other configures the rule for auditing so security operations can record relevant activity and assess potential impact before or alongside enforcement. Microsoft documents this rule as protecting against Office-based malware techniques in which malicious macros spawn processes to download or run payloads. ASR rules require Microsoft Defender Antivirus to be active and supported Windows versions. For the rule identifier, supported behavior, and deployment guidance, see Attack surface reduction rules reference. For the PowerShell syntax and ASR preference parameters, see Set-MpPreference.

QUESTION NO: 16

You have a Microsoft 365 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode. You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product Solution: You enable automated investigation and response (AIR) Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Automated investigation and response (AIR) is an alert investigation and remediation capability in Microsoft Defender for Endpoint. It examines alerts, correlates evidence, determines a verdict, and can perform approved remediation actions. However, enabling AIR by itself does not configure the required preventative protection for malware that the primary third-party antivirus product fails to detect.

For devices on which a third-party antivirus solution remains the primary product and Microsoft Defender Antivirus operates in passive mode, Microsoft recommends enabling *EDR in block mode* to add post-breach protection. EDR in block mode allows Microsoft Defender for Endpoint to remediate malicious artifacts that were missed by the non-Microsoft antivirus product, including by quarantining malicious files. It is specifically intended to supplement a primary third-party antivirus solution rather than replace it.

AIR can still add value by automating investigation and response workflows for detected incidents, but it is not the setting that enables this additional malware-blocking layer. The appropriate control to meet the stated protection requirement is EDR in block mode, as described in Microsoft Defender for Endpoint EDR in block mode. Microsoft also documents the passive-mode and third-party antivirus coexistence model in its Defender Antivirus compatibility guidance.

QUESTION NO: 17

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.

You need to enable Microsoft Defender for Servers on the virtual machines.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

A. From Defender for Cloud, enable agentless scanning.

B. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.

C. Onboard the virtual machines to Microsoft Defender for Endpoint.

D. From Defender for Cloud, configure auto-provisioning.

E. From Defender for Cloud, configure the AWS connector.

ANSWER: C E

Explanation:

Configuring the AWS connector in Microsoft Defender for Cloud establishes the multicloud connection between the AWS account and Defender for Cloud. The connector uses the required AWS permissions and CloudFormation deployment to discover AWS resources, including EC2 instances, and lets Defender for Cloud apply Defender plans to the connected AWS environment. This is the foundational step for managing Defender for Servers coverage for workloads hosted in AWS.

Onboarding the virtual machines to Microsoft Defender for Endpoint provides the endpoint detection and response sensor required by Defender for Servers' agent-based protection capabilities. Defender for Servers integrates with Defender for Endpoint to collect endpoint telemetry, detect threats, and support investigation and response for Windows Server workloads. In an AWS deployment, this onboarding can be performed through the supported deployment method for the servers, including an AWS Systems Manager-based deployment where applicable, or by using a supported Defender for Endpoint onboarding package.

Together, the AWS connector supplies the Defender for Cloud multicloud management path, while Defender for Endpoint onboarding supplies protection and security signals from each Windows Server virtual machine. See Connect AWS accounts to Defender for Cloud and Onboard Windows Server devices to Defender for Endpoint.

QUESTION NO: 18

You have a Microsoft Sentinel workspace named Workspace1.

You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser.

What should you create in Workspace1?

A. a watch list

B. an analytic rule

C. a hunting query

D. a workbook

ANSWER: A

Explanation:

The correct answer is **a watch list**. Microsoft Sentinel's built-in unified ASIM parsers can be configured to omit individual built-in, source-specific parsers by using the ASIM disabled-parsers watchlist in the workspace. The unified parser checks this configuration when it runs, allowing the workspace to prevent a specified source-specific parser from contributing normalized results while retaining the standard unified-parser architecture.

This approach is useful when a particular built-in parser is not appropriate for the environment, such as when its source data is not used or when a customized parser is intended to handle that source instead. The exclusion is workspace-specific, so creating and populating the watchlist in Workspace1 controls parser behavior for queries that use the relevant unified ASIM parser in that workspace. This provides a supported configuration mechanism without modifying Microsoft-managed built-in parser content.

Microsoft documents ASIM parser management and the use of a disabled-parsers watchlist for controlling which source-specific parsers are included by unified parsers. For implementation guidance, see Manage ASIM parsers and the general Microsoft Sentinel watchlists documentation.

QUESTION NO: 19

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-e vents in near real time.

What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.

B. Configure the Diagnostics settings in Azure AD to stream to an event hub.

C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

ANSWER: B

Explanation:

Configure the Diagnostics settings in Azure AD to stream to an event hub. Microsoft Entra ID diagnostic settings (Azure AD is now Microsoft Entra ID) can export sign-in logs and other identity log categories to Azure Event Hubs. Event Hubs is designed for high-throughput event ingestion and streaming, allowing a third-party SIEM to consume identity events as they are emitted and apply its own correlation rules and alert logic with low latency. This architecture keeps the SIEM as the destination for analysis while using Azure Event Hubs as the supported transport layer between Microsoft Entra ID and the external platform.

To implement this, create or select an Event Hubs namespace and event hub, then configure a diagnostic setting for the tenant. Select the required sign-in log categories and choose the Event Hubs destination, including the appropriate authorization rule. The SIEM must then be configured with a compatible Event Hubs consumer or connector and consumer group to read the event stream. Microsoft documents streaming Microsoft Entra logs to Event Hubs for integration with external monitoring and analysis systems: Stream Microsoft Entra logs to an event hub. Diagnostic-setting destinations and configuration are also documented at Configure Microsoft Entra diagnostic settings.

QUESTION NO: 20

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

A. And a new scheduled query rule.

B. Add a data connector to Azure Sentinel.

C. Configure a custom Threat Intelligence connector in Azure Sentinel.

D. Modify the trigger in the logic app.

ANSWER: D

Explanation:

Modify the trigger in the logic app. A Microsoft Sentinel playbook is an Azure Logic Apps workflow that Microsoft Sentinel can invoke in response to an alert or incident, either manually from the Sentinel experience or automatically through an automation rule. An existing workflow that uses a generic manual trigger is not configured to receive the alert or incident context that Sentinel passes to a playbook. Therefore, the first required change is to replace the manual trigger with the appropriate Microsoft Sentinel trigger, such as the Microsoft Sentinel incident trigger when the workflow is intended to respond to incidents. This makes the workflow available for use as a Sentinel playbook and supplies it with incident entities and other relevant context. After the trigger is updated, the playbook can be associated with automation rules or run from an incident, subject to the required permissions and connections. Microsoft documents that playbooks are based on Logic Apps workflows and must start with a Microsoft Sentinel trigger to be run from Sentinel. The incident trigger is specifically designed to receive incident details and support response actions such as disabling or blocking a user account. See Create and customize Microsoft Sentinel playbooks and Automate threat response with automation rules.

QUESTION NO: 21 - (SIMULATION)

You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud.

You have an Azure DevOps organization named AzDO1.

You need to integrate Sub! and AzDO1. The solution must meet the following requirements:

• Detect secrets exposed in pipelines by using Defender for Cloud.

• Minimize administrative effort.

ANSWER: See the explanation for the answer

Explanation:

Configure the integration as follows:
In **Microsoft Defender for Cloud**, select **Add an environment** and add the Azure DevOps environment for `AzDO1`.
In **Azure DevOps**, install the **Microsoft Security DevOps** extension.

The Defender for Cloud environment connector onboards the Azure DevOps organization to Defender for DevOps. The Microsoft Security DevOps extension enables the security scanners used in Azure DevOps pipelines, including secret scanning (CredScan). This built-in connector and extension approach requires less administrative effort than creating a custom integration.

QUESTION NO: 22

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

A. SharePoint search

B. a hunting query in Microsoft 365 Defender

C. Azure Information Protection

D. RegEx pattern matching

ANSWER: D

Explanation:

RegEx pattern matching is appropriate because the customer account numbers have a clearly defined, consistent structure: exactly 32 alphanumeric characters. In Microsoft Purview, a data loss prevention policy identifies sensitive content by using sensitive information types. When an organization needs to detect a proprietary identifier that is not adequately covered by a built-in sensitive information type, it can create a custom sensitive information type. A regular expression is used in the custom type to specify the required character pattern, such as a sequence of 32 letters and digits.

After the custom sensitive information type is created and tested, it can be selected as a condition in a DLP policy scoped to SharePoint Online. Purview then evaluates supported SharePoint content for matches and applies the policy's configured protective actions, such as restricting access or notifying users and administrators. For a production policy, the regular expression should be designed carefully to minimize unintended matches; Microsoft also supports adding supporting evidence, such as keywords or checksums, where the identifier format requires greater confidence.

Microsoft documents custom sensitive information type creation and regular-expression-based patterns at Create a custom sensitive information type. DLP's use of sensitive information types is described in Learn about Microsoft Purview DLP.

QUESTION NO: 23

You have a Microsoft 365 B5 subscription that contains two groups named Group! and Group2 and uses Microsoft Copilot for Security. You need to configure Copilot for Security role assignments to meet the following requirements:

Ensure that members of Group1 can run prompts and respond to Microsoft Defender XDR security incidents.

Ensure that members of Group2 can run prompts.

Follow the principle of least privilege.

You remove Everyone from the Copilot Contributor role.

Which two actions should you perform next? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Assign the Copilot Contributor role to Group2.

B. Assign the Security Operator role to Group1.

C. Assign the Copilot Owner role to Group1.

D. Assign the Security Operator role to Group2.

E. Assign the Copilot Owner role to Group2.

ANSWER: A B

Explanation:

Assign the Copilot Contributor role to Group2. This role provides the ability to use Microsoft Copilot for Security, including starting sessions and running prompts, without granting role-management or configuration permissions. Because the default *Everyone* assignment was removed, prompt access must be explicitly granted to the group that needs it. Assigning this role directly to Group2 satisfies its stated requirement while maintaining least-privilege access.

Assign the Security Operator role to Group1. Security Operator is the appropriate Microsoft Defender XDR role for personnel who must investigate and respond to security incidents. It provides the operational permissions needed to work with incidents and related security data, rather than administrative control of Copilot configuration or role assignments. This aligns Group1's incident-response duties with an operational security role and lets its members use Copilot capabilities in the Defender XDR security workflow. Microsoft documents the Copilot roles and their use at Microsoft Security Copilot roles, and documents Defender XDR role-based access controls and built-in security roles at Microsoft Defender XDR RBAC.

QUESTION NO: 24

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

Explanation:

Common is the appropriate Windows Security Events collection preset because it provides a Microsoft-managed, broadly useful security-auditing event set that includes the authentication activity needed to establish a user audit trail, such as successful and failed sign-ins and sign-out-related events. It is intended for common security-monitoring scenarios in Microsoft Sentinel, allowing analysts to retain meaningful security telemetry without collecting the complete Windows Security log.

Using this built-in preset also reduces operational work across the 100 Windows Server virtual machines. The Windows Security Events connector configures collection through an Azure Monitor data collection rule, and selecting a predefined event set avoids the ongoing effort of determining, testing, deploying, and maintaining an individually selected list of event IDs. The Common preset therefore balances coverage for authentication investigations with controlled ingestion volume and centralized administration.

Microsoft documents the Windows Security Events via AMA connector and its predefined event-set choices at Windows Security Events via AMA connector. For details on how Azure Monitor data collection rules collect Windows event logs, see Collect Windows event log data with the Azure Monitor Agent.

QUESTION NO: 25

You have the following environment:

Azure Sentinel

A Microsoft 365 subscription

Microsoft Defender for Identity

An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.

You deploy Microsoft Defender for Identity by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified in Active Directory.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.

B. Modify the permissions of the Domain Controllers organizational unit (OU).

C. Configure auditing in the Microsoft 365 compliance center.

D. Configure Windows Event Forwarding on the domain controllers.

ANSWER: A D

Explanation:

Configuring the Advanced Audit Policy Configuration settings for the domain controllers ensures that Active Directory Domain Services generates the required Security event records when group membership changes occur. In particular, auditing for security group management produces the domain-controller events associated with adding, removing, or changing members of security-enabled groups. These event records provide the authoritative activity data needed to identify modifications affecting sensitive groups.

Configuring Windows Event Forwarding on the domain controllers provides a supported way to collect the relevant Windows Security events and make them available for Defender for Identity event collection. Event forwarding is especially useful where event data must be gathered consistently from domain controllers and processed by the Defender for Identity sensor infrastructure. Together, the audit policy creates the required evidence of sensitive-group changes, while Windows Event Forwarding delivers that evidence for analysis and detection. Microsoft documents the required event collection configuration and the Windows events used by Defender for Identity at Configure Windows event collection and Configure event collection.

QUESTION NO: 26

You have a Microsoft Sentinel workspace that collects Microsoft Entra ID sign-in logs and Windows security events.

You need to identify anomalous activity by users and hosts and investigate the related entities from incidents.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable entity behavior analytics in Microsoft Sentinel.

B. Connect and ingest data sources that contain user and host activity.

C. Create a Microsoft Sentinel watchlist.

D. Enable the Fusion analytics rule only.

E. Create a workbook that contains a sign-in chart.

ANSWER: A B

Explanation:

Enable **entity behavior analytics** in Microsoft Sentinel. UEBA analyzes activity associated with entities, including users, hosts, IP addresses, and applications, to establish behavioral baselines and identify anomalous behavior. It also provides entity pages that help analysts investigate related activity and insights.

Connect and ingest the relevant data sources that provide identity and host activity. Microsoft Entra ID sign-in logs provide user authentication context, while Windows security events provide host and account activity. UEBA requires sufficient source telemetry to build meaningful behavioral profiles and generate investigation insights.

Analytics rules and watchlists can supplement investigations, but they do not independently provide UEBA baselining and entity behavior analysis. For more information, see Microsoft Sentinel UEBA reference and Identify advanced threats with UEBA in Microsoft Sentinel.

QUESTION NO: 27

You have a custom analytics rule to detect threats in Azure Sentinel.

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

A. There are connectivity issues between the data sources and Log Analytics.

B. The number of alerts exceeded 10,000 within two minutes.

C. The rule query takes too long to run and times out.

D. Permissions to one of the data sources of the rule query were modified.

ANSWER: D

Explanation:

Permissions to one of the data sources of the rule query were modified is a possible cause because scheduled analytics rules run their Kusto Query Language (KQL) queries against the Microsoft Sentinel workspace and, where applicable, other authorized resources. If a permissions change removes the rule's ability to read a required table, workspace, or external resource, the query can fail during execution. Repeated execution failures can cause Microsoft Sentinel to automatically disable the analytics rule. Sentinel identifies rules disabled in this way by adding the **AUTO DISABLED** prefix to the rule name, making the condition visible to analysts and administrators.

The appropriate remediation is to review the rule's execution and health information to identify the inaccessible resource or authorization error, restore the required access for the relevant identity and resource, validate that the query runs successfully, and then re-enable the rule. Microsoft Sentinel health monitoring provides operational information about analytics-rule status and issues, while scheduled analytics-rule documentation describes the query-based detection process and rule management. See Microsoft Sentinel health and audit and Create custom analytics rules in Microsoft Sentinel.

QUESTION NO: 28

You have a Microsoft 365 E5 subscription.

Automated investigation and response (AIR) is enabled in Microsoft Defender for Office 365 and devices use full automation in Microsoft Defender for Endpoint.

You have an incident involving a user that received malware-infected email messages on a managed device.

Which action requires manual remediation of the incident?

A. containing the device

B. hard deleting the email message

C. isolating the device

D. soft deleting the email message

ANSWER: C

Explanation:

isolating the device requires manual remediation. Device isolation is a containment action that an authorized security operator initiates from the device page in the Microsoft Defender portal. It disconnects the endpoint from the organization's network while retaining connectivity to Defender for Endpoint services, allowing analysts to investigate and remediate the device. Because this can substantially affect a user's ability to work and access organizational resources, it is an explicit analyst-directed response action rather than a remediation step performed by automated investigation and response.

Full automation in Defender for Endpoint enables automated investigations to assess alerts and take supported remediation actions, such as addressing malicious files and persistence artifacts. Likewise, Defender for Office 365 AIR can investigate malicious email threats and perform email remediation as part of its investigation workflow. In this incident, however, separating the managed endpoint from the network is a deliberate containment decision that must be manually executed after reviewing the investigation context and operational impact.

Microsoft documents the manual isolation workflow and its effect on device connectivity in Isolate devices from the network. For the role of automated investigations and remediation in Defender for Office 365, see Automated investigation and response capabilities.

QUESTION NO: 29

You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant

B. Select Investigate files, and then filter App to Office 365.

C. Select Investigate files, and then select New policy from search

D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings

E. From Settings, select Information Protection, select Files, and then enable file monitoring.

F. Select Investigate files, and then filter File Type to Document.

ANSWER: D E

Explanation:

Enabling file monitoring under Information Protection allows Defender for Cloud Apps to monitor files in connected cloud applications and evaluate file-related activities and sharing exposure. This is the foundation for identifying files that are shared externally and for applying file-policy governance actions, such as removing external collaborators or quarantining a file when the policy conditions are met.

Automatically scanning new files for Azure Information Protection classification labels and content-inspection warnings ensures that newly discovered files are evaluated for their confidentiality classification. The scan makes label and inspection information available as policy criteria, allowing a file policy to target confidential content specifically rather than applying to every externally shared file. Once monitoring and classification scanning are enabled, an administrator can create a file

policy that detects external sharing of appropriately classified files, generates an alert, and invokes the configured governance remediation action.

Microsoft documents file monitoring and file-policy controls in Defender for Cloud Apps information protection policies. Configuration of Azure Information Protection label scanning is described in Azure Information Protection integration.

QUESTION NO: 30

You have an Azure subscription named Sub1 and a M icrosoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connec tor for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer present part of the solution

NOTE: Each correct selection is worth one point.

A. Create custom rule based on the Office 365 connector templates.

B. Create a Microsoft incident creation rule based on Microsoft Defender for Cloud.

C. Create a Microsoft Cloud App Security connector.

D. Create an Azure AD Identity Protection connector.

ANSWER: C D

Explanation:

Fusion is a Microsoft Sentinel analytics capability that detects advanced, multistage attacks by correlating lower-fidelity signals, alerts, and entities from supported Microsoft security products. To identify the stated sequence, the workspace needs a source for risky or suspicious Microsoft Entra ID sign-in detections and a source for anomalous Microsoft 365 activity detections. Creating an Azure AD Identity Protection connector provides Identity Protection alerts, including detections associated with risky sign-ins, to Sentinel. These alerts supply the identity, sign-in, and risk context Fusion uses when building a cross-stage attack story.

Creating a Microsoft Cloud App Security connector provides alerts from Microsoft Cloud App Security, now called Microsoft Defender for Cloud Apps. Defender for Cloud Apps monitors cloud-app behavior, including Microsoft 365 activity, and generates alerts for anomalous or suspicious activity. With both alert sources connected, Fusion can correlate the matching account and related entities across the suspicious sign-in and subsequent cloud-app activity, then create a higher-confidence incident when its multistage correlation logic is satisfied. Microsoft documents Fusion as correlating alerts from multiple sources, and documents the connector used to ingest Defender for Cloud Apps alerts into Microsoft Sentinel. See Fusion detection in Microsoft Sentinel and Connect Microsoft Defender for Cloud Apps to Microsoft Sentinel.

QUESTION NO: 31

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription

B. the Contributor for the subscription

C. the Contributor role for RG1

D. the Owner role for RG1

ANSWER: C

Explanation:

The *Contributor role for RG1* is the appropriate additional role because applying a quick fix in Microsoft Defender for Cloud can require making changes to the affected Azure resources. Examples include changing a resource configuration or deploying a required component to a virtual machine. Although the Security Admin role permits management of Defender for Cloud security settings, policies, and recommendations, remediation actions also require Azure Resource Manager permissions to write to the underlying resources.

Assigning Contributor at the RG1 resource-group scope gives SecAdmin1 permission to create and manage the resource changes needed for the virtual machines contained in that group. This scope includes all 100 virtual machines while limiting the permissions to resources in RG1 rather than extending modification rights throughout the subscription. The Contributor role does not grant permission to manage access assignments, which also helps maintain separation between resource administration and access control.

Microsoft documents that Defender for Cloud remediation requires appropriate permissions on the resources being remediated, and that Azure RBAC roles can be assigned at a resource-group scope. See Microsoft Defender for Cloud permissions and Azure Contributor built-in role.

QUESTION NO: 32

You have a Microsoft Sentinel workspace.

You need to collect Syslog events from 50 Linux servers by using the Syslog via AMA data connector. The solution must use the Azure Monitor Agent.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Install the Azure Monitor Agent on the Linux servers.

B. Create and associate a data collection rule with the Linux servers.

C. Install the Log Analytics agent on the Linux servers.

D. Create an Azure Event Grid subscription.

E. Enable Microsoft Defender Antivirus on the Linux servers.

ANSWER: A B

Explanation:

Installing the **Azure Monitor Agent** on the Linux servers provides the supported agent that collects Syslog events and sends them to Azure Monitor Logs. The agent replaces legacy agent-based collection approaches for current Microsoft Sentinel Syslog ingestion scenarios.

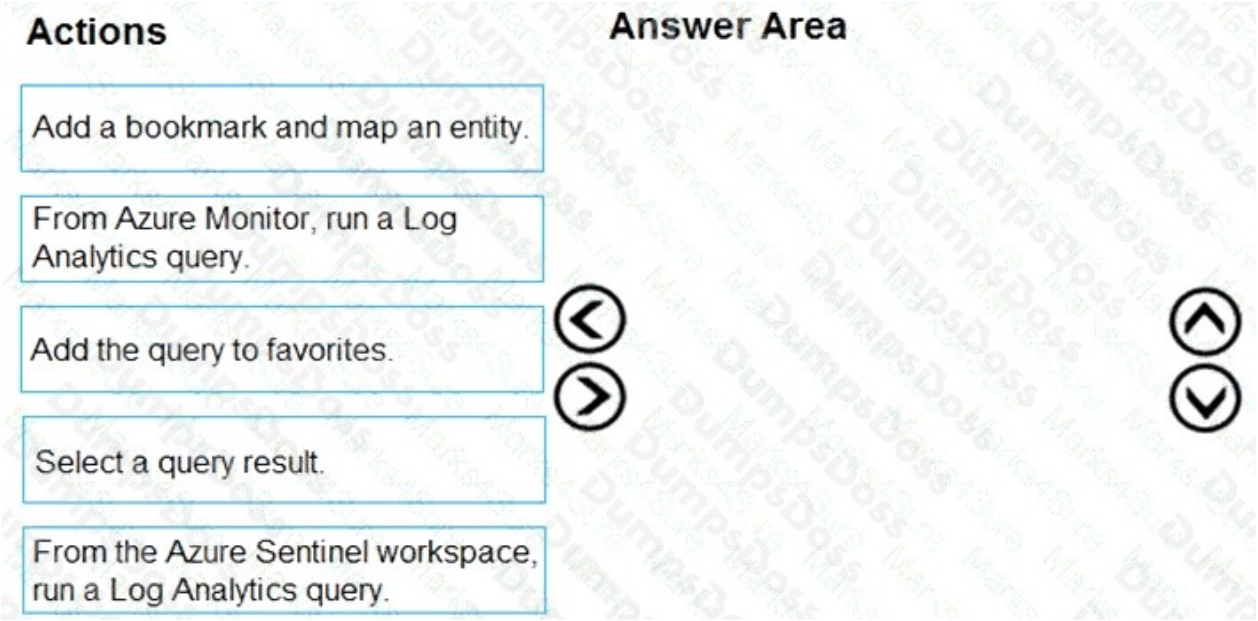
Creating and associating a **data collection rule (DCR)** defines which Syslog facilities and severities the agent must collect and identifies the destination Log Analytics workspace. The DCR must be associated with the target Linux servers so that the Azure Monitor Agent receives the required collection configuration. Together, the agent and DCR provide the collection path for Syslog data in the Syslog table.

For more information, see Collect Syslog data with the Azure Monitor Agent and Data collection rules in Azure Monitor.

QUESTION NO: 33 - (DRAG DROP)

You need to add notes to the events to meet the Azure Sentinel requirements.

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

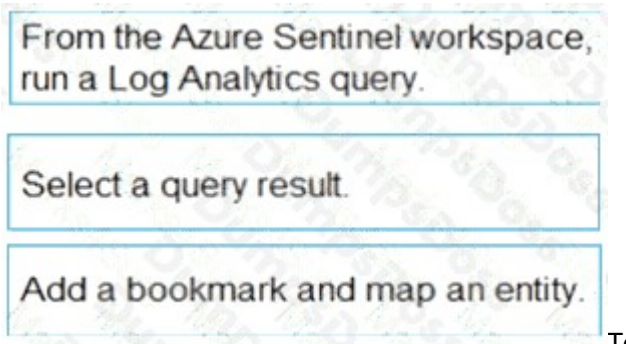


ANSWER:

Answer:

Answer:

Explanation:



To attach notes that you can later see during investigations and hunting, you use Bookmarks in Microsoft Sentinel. Bookmarks are created from the Hunting (or Logs) experience inside the Sentinel workspace and let you pin a specific query result (including IPs, accounts, hosts) with notes, tags, and mappe d entities so it appears in the investigation graph and is easily referenceable. The correct workflow is: first, run your KQL query from the Microsoft Sentinel workspace (not from generic Azure Monitor), because Sentinel's hunting experience is where bookmarks integrate with incidents and the investigation graph. Next, select a specific query result that represents the suspicious activity (e.g., a data access event from the target IP). Finally, create a Bookmark and map the relevant entity (IP address, Account, etc.) while adding your notes . Mapping the entity ensures the bookmarked event is connected in the investigation graph; the notes provide the narrative/context you need when pivoting later. Adding the query to favorites is optional for convenience but does not attach notes to a specific event, and running the query from Azure Monitor would not place the bookmark within Sentinel's investigation context.

Explanation:

To add notes to a particular event for later investigation and hunting, first run a Log Analytics query from the Azure Sentinel workspace. This establishes the Microsoft Sentinel context for the investigation and returns the event data that an analyst

wants to preserve. Microsoft Sentinel query results are the starting point for creating bookmarks because a bookmark is tied to a specific result rather than merely to the saved query itself.

Next, select the relevant query result. The selected row identifies the exact event or observation to document, such as a sign-in, network connection, process execution, or other suspicious activity. Selecting that result lets Sentinel retain the event context, including the fields that can be used in the investigation.

Finally, add a bookmark and map an entity. When creating the bookmark, the analyst can enter notes that capture the reasoning, findings, and follow-up context for the event. Entity mapping associates relevant values, such as an account, host, IP address, URL, or file hash, with the bookmark. This makes the information useful in Microsoft Sentinel investigations because the bookmarked evidence can be revisited and correlated with related entities and incident activity. Microsoft documents bookmarks as a way to retain query-result evidence and contextual information for later use in investigations and hunting. See Microsoft Sentinel bookmarks and Investigate incidents in Microsoft Sentinel.

QUESTION NO: 34

You have a Microsoft Entra ID P2 tenant.

You need to respond automatically to the following Identity Protection detections:

Require users who are determined to be at risk to change their passwords.

Require multifactor authentication (MFA) when a sign-in is determined to be risky.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure a user risk policy that requires a secure password change.

B. Configure a sign-in risk policy that requires MFA.

C. Configure an access review for all users.

D. Configure a Conditional Access policy that blocks all sign-ins.

E. Configure a password protection custom banned password list.

ANSWER: A B

Explanation:

Configure a **user risk policy** that requires a secure password change. User risk represents the likelihood that an account has been compromised. A user risk policy can automatically remediate affected users by requiring them to complete a secure password change.

Configure a **sign-in risk policy** that requires MFA. Sign-in risk is evaluated for an individual authentication attempt. Requiring MFA for risky sign-ins provides an additional verification step before access is granted.

Conditional Access policies can also use risk conditions, but the Identity Protection user risk and sign-in risk policies directly meet the separate remediation requirements in this scenario. For more information, see Configure Microsoft Entra ID Protection risk policies.

QUESTION NO: 35

You need to remediate ac tive attacks to meet the technical requirements.

What should you include in the solution?

A. Azure Automation runbooks

B. Azure Logic Apps

C. Azure Functions

ANSWER: B

Explanation:

Azure Logic Apps is the appropriate component because Microsoft Sentinel playbooks are workflows built on Azure Logic Apps. Playbooks provide Sentinel's security orchestration, automation, and response capability, allowing a response workflow to run when security alerts or incidents require action. For example, a playbook can invoke connectors and APIs to disable or block a compromised account, isolate a device through a security product integration, create a ticket, send notifications, or collect additional context for remediation.

In Microsoft Sentinel, an automation rule can be configured to run a playbook when an incident is created or updated, or when specific alert and incident conditions are met. This creates an alert-driven remediation process rather than relying on an analyst to manually start each response. Logic Apps also provides the managed workflow features, connectors, authentication, conditional logic, and error-handling capabilities needed to coordinate actions across Microsoft and third-party security services.

Microsoft documents that Sentinel playbooks are based on Azure Logic Apps workflows and are intended to automate and orchestrate threat response. See Automate threat response with playbooks in Microsoft Sentinel and Automate incident handling with automation rules in Microsoft Sentinel.

QUESTION NO: 36

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add a playbook.

B. Associate a playbook to an incident.

C. Enable Entity behavior analytics.

D. Create a workbook.

E. Enable the Fusion rule.

ANSWER: A B

Explanation:

"Add a playbook." is required because Microsoft Sentinel playbooks are Azure Logic Apps that orchestrate response actions. A playbook can use the Microsoft Teams connector and its channel-posting action to deliver a notification to the selected Teams channel. The playbook therefore contains the actual integration and message-posting logic needed after a suspicious sign-in is detected.

"Associate a playbook to an incident." is also required so that the response executes automatically in response to the detection. In the current Microsoft Sentinel experience, this association is normally implemented by an automation rule that runs the playbook when an incident is created or updated. The analytics rule detecting the suspicious sign-in creates the alert or incident, and the automation rule invokes the Teams-enabled playbook. Together, these actions provide both the response workflow and the automatic trigger needed to notify the channel whenever the detection occurs.

For implementation guidance, see Automate threat responses with playbooks in Microsoft Sentinel and Automate incident handling with automation rules.

QUESTION NO: 37

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.

C. From the Azure portal, create an Azure Event Grid subscription.

D. From the workspace created by Defender for Cloud, set the data collection level to All Events

E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

ANSWER: A E

Explanation:

From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines is correct because it centrally deploys the required monitoring agent and configuration to the existing servers covered by the subscription. This avoids manually installing and configuring data collection on each of the 100 Windows Server virtual machines, substantially reducing operational effort. Automatic provisioning also applies to newly created eligible virtual machines, helping maintain consistent coverage over time.

From the workspace created by Defender for Cloud, set the data collection level to Common is correct because the Common level gathers the Windows security-event set used for Defender for Cloud security monitoring while reducing the amount of event data ingested compared to collecting all Windows security events. Since Log Analytics ingestion volume affects cost, selecting the common event set meets the stated requirement to collect event data while minimizing cost. Together, automatic provisioning establishes scalable collection across the VM estate and the Common collection level limits collection to the security-relevant event volume needed for this scenario. Microsoft describes Defender for Cloud data-collection configuration at Enable data collection in Defender for Cloud and explains security event collection choices in Defender for Servers FAQ.

QUESTION NO: 38

You have 50 Microsoft Sentinel workspaces.

You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.

Which page should you use in the Azure portal?

A. Microsoft Sentinel - Incidents

B. Microsoft Sentinel - Workbooks

C. Microsoft Sentinel

D. Log Analytics workspaces

ANSWER: A

Explanation:

Microsoft Sentinel - Incidents is the centralized incident-management page for this requirement. Microsoft Sentinel supports a multitenant, multi-workspace incident experience in the Azure portal, allowing security operations teams to review incidents across workspaces from one incident queue rather than opening each workspace separately. This is particularly

appropriate for an environment with 50 workspaces because it provides the built-in operational view without requiring a custom query, workbook design, dashboard maintenance, or manual workspace-by-workspace review.

From the Microsoft Sentinel incident experience, an analyst can use the relevant directory or workspace scope to access incidents they are authorized to see, then triage, assign, investigate, and manage those incidents from the consolidated view. Access is governed by Azure RBAC permissions on the underlying workspaces, so the appropriate Sentinel and Log Analytics permissions must be assigned to the analysts who need centralized visibility. Microsoft documents the multiple-workspace view as a way to monitor and manage incidents across workspaces, while the incident page is the primary interface for incident operations. See Work with multiple Microsoft Sentinel workspaces and Investigate incidents with Microsoft Sentinel.

QUESTION NO: 39 - (HOTSPOT)

You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.

ANSWER:

Explanation:

Assign **Security Admin** to Group1 and **Contributor** to Group2. The Security Admin role is the appropriate Azure built-in role for a group responsible for administering security through Microsoft Defender for Cloud. It allows the security team to manage Defender for Cloud security policies and related security settings, and to work with the security information surfaced by the service. This supports a security-administration responsibility without giving that group unrestricted control over every resource in the subscription.

The Contributor role is appropriate for the group that must implement remediation. Defender for Cloud recommendations commonly require changes to the protected Azure resources, such as changing a resource configuration, enabling a protection setting, or deploying a remediation. Contributor grants the ability to create and manage those resources. Importantly, it does not include permission to manage Azure RBAC role assignments, which preserves separation of duties while still allowing the group to carry out the required fixes.

This combination separates security governance and Defender for Cloud administration from operational resource remediation. Microsoft documents the permissions model for Defender for Cloud in its Permissions in Microsoft Defender for

Cloud guidance. The detailed permissions for Security Admin and Contributor are available in the Azure built-in roles reference.

QUESTION NO: 40

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices. As part of an incident investigation, you identify the following suspected malware files:

sys pdf docx xlsx

You need to create indicator hashes to block users from downloading the files to the devices. Which files can you block by using the indicator hashes?

A. File1.sys only

B. File1.sys and File3.docx only

C. File1.sys, File3.docx, and File4.xlsx only

D. File2.pdf, File3.docx, and File4.xlsx only

E. File1.sys, File2.pdf, File3.docx, and File4.xlsx

ANSWER: A

Explanation:

File1.sys only is correct. Microsoft Defender for Endpoint custom file indicators support blocking Portable Executable (PE) files by their SHA-256 hash. A Windows `.sys` file is a system-driver binary and uses the PE format, so it is within the supported file type scope for a hash-based block indicator. When the indicator is created with the Block and remediate action, Microsoft Defender Antivirus can prevent the identified driver binary from being downloaded or used on onboarded Windows devices, subject to indicator policy and cloud-delivered protection requirements.

Custom indicators are valuable during incident response because they provide a targeted control for a known malicious binary, rather than requiring a broadly scoped policy change. The SHA-256 value should be obtained from the investigated sample and added in the Microsoft Defender portal under Indicators, with the applicable device groups selected. Microsoft documents that file hash indicators are supported for PE files, which includes driver files such as `.sys`. See Create indicators for files and Manage indicators.

QUESTION NO: 41 - (HOTSPOT)

You have an Azure subscription named Sub1 and an Azure DevOps organization named AzDO1. AzDO1 uses Defender for Cloud and contains a project that has a YAML pipeline named Pipeline1.

Pipeline1 outputs the details of discovered open source software vulnerabilities to Defender for Cloud.

You need to configure Pipeline1 to output the results of secret scanning to Defender for Cloud,

What should you add to Pipeline1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ANSWER:

Explanation:

Add an `inputs:` block to the Microsoft Security DevOps task configuration and set `categories:` to `'secrets'`. This directs the task to perform secret-scanning analysis as part of the Azure DevOps YAML pipeline. The Microsoft Security DevOps extension is designed to run Microsoft security analysis tools in Azure DevOps and publish the resulting security findings for consumption in Defender for Cloud. Specifying the `secrets` category enables the secret-scanning workload, allowing discovered credentials, tokens, keys, and similar sensitive values to be reported by the pipeline.

The required YAML fragment is `inputs:` with the nested setting `categories: 'secrets'`. In the displayed answer area, place the upper selection on `inputs:` and the lower selection on `categories:`; the shown value remains `'secrets'`. This configuration scopes the task to the required analysis category while preserving the pipeline's existing reporting path to Defender for Cloud. Microsoft documents Microsoft Security DevOps and its pipeline integration in the Microsoft Security DevOps extension overview. Microsoft also documents how Defender for Cloud uses DevOps security findings as part of its Defender for DevOps capabilities.

QUESTION NO: 42

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever an incident representing a signin risk event is activated in Azure Sentinel.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable Entity behavior analytics.

B. Associate a playbook to the analytics rule that triggered the incident.

C. Enable the Fusion rule.

D. Add a playbook.

E. Create a workbook.

ANSWER: B D

Explanation:

Add a playbook. is required because Microsoft Sentinel uses playbooks, implemented as Azure Logic Apps, to automate response and orchestration actions. A playbook can start from a Microsoft Sentinel incident trigger and include a Microsoft Teams connector action that posts a message to a selected team and channel. The message can contain incident details, such as its title, severity, status, involved entities, and a link for analysts to investigate the incident.

Associate a playbook to the analytics rule that triggered the incident. completes the automation path. The analytics rule detects the sign-in risk activity and creates the incident; associating the playbook ensures the Teams notification workflow runs when the relevant incident is generated. In current Microsoft Sentinel terminology, this association can be managed through automation rules that run a playbook when an incident is created, but the essential requirement remains linking the incident-generating detection to the Teams-posting playbook.

This design provides an immediate operational notification while retaining the incident in Microsoft Sentinel for triage, investigation, and response. For implementation details, see Automate threat responses with playbooks in Microsoft Sentinel and Automate incident handling with automation rules.

QUESTION NO: 43

You have an Azure subscription.

You need to stream the Microsoft Graph activity logs to a third-party security information and event management (SIEM) tool. The solution must minimize administrative effort. To where should you stream the logs?

A. an Azure Event Hubs namespace

B. an Azure Event Grid namespace

C. an Azure Storage account

D. a Log Analytics workspace

ANSWER: A

Explanation:

an Azure Event Hubs namespace is the appropriate destination because Microsoft Graph activity logs can be exported through an Azure Monitor diagnostic setting to an event hub. Azure Event Hubs is designed for high-throughput, near-real-time event ingestion and streaming, which aligns with the operational needs of a third-party SIEM. Rather than requiring a custom process to periodically retrieve, transform, and forward stored log files, the SIEM or its supported connector can consume the continuous event stream from the event hub. This reduces the amount of Azure-side administration required while providing a scalable integration point for security monitoring.

Microsoft Graph activity logs record requests made to Microsoft Graph and can be routed by diagnostic settings to supported Azure destinations. Event Hubs provides the streaming endpoint needed for external tools to ingest these records as they are emitted. The receiving SIEM team can configure its Event Hubs-compatible connector or consumer to read from the namespace, consumer group, and event hub, while Azure handles the durable event-stream delivery layer. This makes an Azure Event Hubs namespace the best fit for exporting Microsoft Graph activity data to a non-Microsoft SIEM with minimal operational overhead. See Microsoft Graph activity logs overview and Azure Monitor diagnostic settings.

QUESTION NO: 44

You haw the resources shown in the following Table.

Name	Type	Description	Location
Server1	Server	File server that runs Windows Server	On-premises
Server2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)
Server3	Virtual machine	Domain controller that runs Windows Server	Azure
Server4	Server	Domain controller that runs Windows Server	On-premises

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to enable Microsoft Defender lot Servers on each resource.

Which resources will require the installation of the Azure Arc agent?

A. Server 3 only

B. Server 1 and Server 4 only

C. Server 1, Server 2, and Server 4 only

D. Server 1, Server 2, Server 3, and Server 4

ANSWER: C

Explanation:

Server 1, Server 2, and Server 4 only is correct. Microsoft Defender for Servers relies on Azure Arc-enabled servers to onboard and manage supported machines that are outside the native Azure virtual machine management plane. Installing the Azure Connected Machine agent registers each applicable non-Azure server as an Azure Arc-enabled server. Defender for Cloud can then deploy or coordinate the required security extensions, collect security posture and workload-protection signals, and apply Defender for Servers capabilities consistently through the Azure subscription.

The resources identified in this answer are the servers in the table that require this Arc-based onboarding path. After the Connected Machine agent is installed and the machines are connected to Azure Arc, Defender for Cloud can enable the relevant Defender for Servers components according to the selected plan and configuration. Microsoft documents Azure Arc onboarding as the supported method for bringing non-Azure machines into Defender for Servers management, including the installation of the Azure Connected Machine agent before enabling protections. See Onboard non-Azure machines to Defender for Cloud and Azure Arc-enabled servers overview.

QUESTION NO: 45

You haw the resources shown in the following Table.

Name	Type	Description	Location
Server1	Server	File server that runs Windows Server	On-premises
Server2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)
Server3	Virtual machine	Domain controller that runs Windows Server	Azure
Server4	Server	Domain controller that runs Windows Server	On-premises

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to enable Microsoft Defender lot Servers on each resource. Which resources will require the installation of the Azure Arc agent?

A. Server 3 only

B. Server1 and Server4 only

C. Server1, Server2, and Server4 only

D. Server1, Server2, Server3, and Server4

ANSWER: C

Explanation:

Server1, Server2, and Server4 only is correct. The table identifies Server1 and Server4 as on-premises Windows Server machines and Server2 as a Linux virtual machine hosted in AWS. These are non-Azure servers, so they must be connected to Azure as Azure Arc-enabled servers before Microsoft Defender for Servers can provide its server protection and management capabilities. Installing the Azure Connected Machine agent is the onboarding mechanism that creates the Azure Arc server resource and enables Azure management services, including Defender for Cloud, to work with those machines.

After Arc onboarding, Defender for Cloud can apply the Defender for Servers plan to the connected machines and deploy or manage the required security extensions, depending on the selected plan and configuration. This approach provides a consistent way to protect servers across on-premises infrastructure and other clouds from the Azure portal. Server3 is an Azure virtual machine, which is already a native Azure resource and does not require Azure Arc onboarding for Defender for Servers.

Microsoft documents that Azure Arc-enabled servers are non-Azure physical or virtual machines connected to Azure by using the Connected Machine agent. Microsoft also documents Azure Arc onboarding as the route for protecting non-Azure machines with Defender for Servers. See Azure Arc-enabled servers overview and Microsoft Defender for Servers overview.

QUESTION NO: 46

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to configure Defender for Cloud to mitigate the following risks:

Vulnerabilities within the application source code

Exploitation toolkits in declarative templates

Operations from malicious IP addresses

Exposed secrets

Which two Defender for Cloud services should you use? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. Microsoft Defender for APIs

B. Microsoft Defender for Resource Manager

C. Microsoft Defender for App Service

D. Microsoft Defender for DevOps

E. Microsoft Defender for Servers

ANSWER: B D

Explanation:

Microsoft Defender for DevOps provides security coverage throughout the development lifecycle and is the appropriate Defender for Cloud service for identifying vulnerabilities in application source code and exposed secrets. Its DevOps security capabilities integrate findings from source-code and secret-scanning tools into Defender for Cloud, helping security teams prioritize and remediate issues before vulnerable code or credentials reach production. This shifts security assessment earlier into repositories and CI/CD workflows.

Microsoft Defender for Resource Manager protects the Azure management plane by monitoring Azure Resource Manager operations. It uses behavioral analytics to identify suspicious management activity, including operations originating from malicious IP addresses. It also detects potentially malicious deployments, including the use of exploitation toolkits or suspicious artifacts delivered through declarative Azure Resource Manager templates. Together, these services address both predeployment risks in the code and repository environment and threats arising from deployment and management-plane activity in Azure.

For implementation details, see Microsoft Defender for DevOps documentation and Microsoft Defender for Resource Manager documentation.

QUESTION NO: 47

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.

B. Create a hunting query that references the built-in parse.

C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.

D. Build a custom unify parse and include the build- parse version

E. Create an analytics rule that includes the built-in parse

ANSWER: A D

Explanation:

Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any. This deployment approach creates workspace-managed parser resources from the built-in parser content. The workspace deployment is under the organization’s control, so subsequent Microsoft updates to the managed built-in parser do not

automatically replace the deployed parser version that queries use. The parameters ensure that the deployment covers the relevant caller context and source-specific parser selection rather than limiting the deployment to a narrower case.

Build a custom unify parse and include the build- parse version is also a complete solution because a custom unifying parser is maintained in the workspace and can explicitly call the desired version of a source-specific parser. Pinning the parser reference in that custom layer provides version stability for normalized queries, analytics, and hunting content. The organization can then choose when to revise the custom parser and adopt later Microsoft parser releases, instead of inheriting changes automatically.

Microsoft's ASIM guidance distinguishes Microsoft-managed built-in parsers from parsers that customers deploy and maintain in their own workspaces. For more detail, see ASIM parsers overview and Manage ASIM parsers.

QUESTION NO: 48

You have a Microsoft Sentinel workspace that contains an analytics rule for detecting port scans.

You identify 20 approved vulnerability-scanning IP addresses that generate false-positive alerts.

You need to exclude the approved IP addresses from the analytics rule. The solution must minimize ongoing administrative effort.

What should you use?

A. a watchlist

B. a bookmark

C. an automation rule

D. a notebook

ANSWER: A

Explanation:

A **watchlist** is the appropriate solution. A Microsoft Sentinel watchlist stores reference data, such as approved scanner IP addresses, in a centrally managed list. The analytics-rule query can reference the watchlist by using the `_GetWatchlist()` function and exclude matching source IP addresses from the detection results.

This approach is easier to maintain than repeatedly editing a query to add or remove individual IP-address exclusions. When the approved scanner inventory changes, an analyst can update the watchlist while preserving the rule logic. The rule continues to generate port-scan alerts for IP addresses that are not included in the approved list. See Use watchlists in Microsoft Sentinel.

QUESTION NO: 49

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a user named User1.

You need to ensure that User1 can manage Microsoft Defender XDR custom detection rules and Endpoint security policies. The solution must follow the principle of least privilege. Which role should you assign to User1?

A. Desktop Analytics Administrator

B. Security Operator

C. Security Administrator

D. Cloud Device Administrator

ANSWER: C

Explanation:

Security Administrator is the appropriate least-privileged built-in Microsoft Entra role for this combined requirement. This role grants administrative permissions for Microsoft 365 security services, including Microsoft Defender XDR. Those permissions enable the user to manage security configuration rather than merely investigate alerts or perform limited operational response activities. Managing custom detection rules is a security-configuration task: the user must be able to create, edit, enable, disable, and otherwise administer detections that query advanced hunting data and generate alerts.

The same role also provides the administrative access needed to manage endpoint security settings and policies exposed through the Microsoft security and endpoint-management experience. This is important because endpoint security policies control protective configurations for managed devices and require configuration-level privileges, not just read access or incident-handling permissions.

Assigning Security Administrator meets both stated responsibilities through one built-in role while avoiding broader tenant-wide roles, such as Global Administrator. Microsoft documents Security Administrator as a role that can manage security services and security settings. Microsoft Defender XDR documentation also identifies the required permissions for managing custom detections and supports role-based access for security administration.

References: Microsoft Entra Security Administrator permissions; Microsoft Defender XDR custom detections overview.

QUESTION NO: 50

You have an Azure subscription that use Microsoft Defender for Ctoud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security operator

B. Security Admin

C. Owner

D. Contributor

ANSWER: B

Explanation:

Security Admin is the appropriate least-privilege Azure RBAC role for a user who must modify Microsoft Defender for Cloud security policies. At the subscription scope, this built-in role includes permissions to view and update security policies and to manage Defender for Cloud security configurations. This allows User1 to perform the required security-policy administration without receiving general management permissions over all resources in the subscription.

Microsoft Defender for Cloud uses Azure RBAC roles to control access to its management-plane capabilities. Assigning Security Admin at the subscription level scopes the permission to the Defender for Cloud configuration for that subscription, which is the appropriate scope when the user must manage its security policies. The role is specifically intended for security administration and is therefore aligned with the principle of least privilege.

Microsoft documents the permissions included in the Security Admin built-in role at Azure built-in roles: Security Admin. Defender for Cloud's role requirements and permission model are described in Microsoft Defender for Cloud permissions.

QUESTION NO: 51

You have an Azure subscription that use Microsoft Defender for Cloud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security operator

B. Security Admin

C. Owner

D. Contributor

ANSWER: B

Explanation:

Security Admin is the appropriate least-privilege Azure built-in role for a user who must modify Microsoft Defender for Cloud security policies. This role is designed for security-management activities within Defender for Cloud and includes the permissions required to manage security policy-related settings. It grants security-specific administrative access rather than broad control over all Azure resources in the subscription.

Defender for Cloud uses Azure role-based access control to separate security administration from general resource administration. Assigning **Security Admin** at the subscription scope gives User1 the required authority wherever Defender for Cloud policy configuration applies in that subscription. If the policy-management requirement applies only to a narrower applicable scope, the role should be assigned at that scope to further minimize permissions.

Microsoft documents that the Security Admin built-in role can manage Defender for Cloud security policies and settings. Its definition includes Microsoft.Security permissions intended for administering Microsoft security services. This makes **Security Admin** the role aligned to both the operational requirement and the principle of least privilege. See Security Admin built-in role and Microsoft Defender for Cloud permissions.

QUESTION NO: 52

You need to restrict cloud apps running on CUENT1 to meet the Microsoft Defender for Endpoint requirements. Which two configurations should you modify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. the Cloud Discovery settings in Microsoft Defender for Cloud Apps

B. the Onboarding settings from Device management in Settings in Microsoft 365 Defender portal

C. Microsoft Defender for Cloud Apps anomaly detection policies

D. Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal

ANSWER: A D

Explanation:

The required configurations are **the Cloud Discovery settings in Microsoft Defender for Cloud Apps** and **Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal**. Defender for Cloud Apps uses Cloud Discovery to provide visibility into cloud-app usage and to classify discovered apps. An administrator can tag an app as unsanctioned, which identifies it as an app that should not be used in the organization. This classification supplies the policy decision used for endpoint enforcement.

To enforce that decision on a Windows device such as CUENT1, the Defender for Cloud Apps integration must be enabled in Microsoft Defender for Endpoint advanced features. Defender for Endpoint then receives the unsanctioned-app indicators from Defender for Cloud Apps. With Network Protection enabled in block mode on the endpoint, Defender for Endpoint can block access to the domains associated with apps tagged as unsanctioned. Thus, Cloud Discovery establishes which cloud apps are disallowed, while the endpoint advanced-feature integration enables Defender for Endpoint to apply the restriction on onboarded devices. Microsoft documents this workflow for blocking unsanctioned cloud apps through Defender for Endpoint integration and Network Protection. See Integrate Microsoft Defender for Endpoint with Defender for Cloud Apps and Network protection.

QUESTION NO: 53

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription. You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer present part of the solution NOTE: Each correct selection is worth one point.

A. Create custom rule based on the Office 365 connector templates.

B. Create a Microsoft incident creation rule based on Microsoft Defender for Cloud.

C. Create a Microsoft Cloud App Security connector.

D. Create an Azure AD Identity Protection connector.

ANSWER: A D

Explanation:

Fusion is a Microsoft Sentinel correlation engine that identifies multistage attacks by applying machine learning to alerts from multiple data sources. To detect the stated sequence, Fusion needs identity-risk alerts that represent suspicious sign-in behavior and alert-producing activity from the Microsoft 365 workload. Creating an Azure AD Identity Protection connector brings Identity Protection risk detections into the workspace. These detections, such as risky users and risky sign-ins, provide the identity-related security signals Fusion can correlate with subsequent activity.

Creating custom rule based on the Office 365 connector templates enables analytics detections over the Office 365 data collected by the connector. The resulting alerts supply the Office 365 security events needed for Fusion to associate anomalous SaaS activity with an earlier identity signal. With both sources configured and their relevant analytic detections enabled, Fusion can create a higher-fidelity incident that represents the attack progression rather than treating the identity and Office 365 events independently.

Microsoft documents Fusion as correlating alerts across products and domains to identify multistage attacks. Connector and analytics-rule configuration guidance is available in the Microsoft Sentinel Fusion documentation and the Microsoft Sentinel data connectors reference.

QUESTION NO: 54

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. cp /bin/echo ./asc_alerttest_662jfi039n

B. ./alerttest testing eicar pipe

C. cp /bin/echo ./alerttest

D. ./asc_alerttest_662jfi039n testing eicar pipe

ANSWER: A D

Explanation:

The required commands are `cp /bin/echo ./asc_alerttest_662jfi039n` and `./asc_alerttest_662jfi039n testing eicar pipe`. Together, they perform Microsoft Defender for Cloud's documented Linux alert-validation procedure. The first command creates a copy of the harmless `/bin/echo` executable using the precise filename recognized by the Defender for Cloud test. The filename is significant: it identifies the executable invocation as an intentional validation event rather than a real malicious binary.

The second command executes that copied file with the expected test arguments, including `eicar`. This produces the telemetry pattern used to validate that the VM is properly onboarded, its security monitoring is functioning, and Microsoft Defender for Cloud can generate an alert for the resource. After execution, allow time for the signal to be processed and then review security alerts in the Defender for Cloud portal. Microsoft states that validation alerts are test events and should be used to confirm the alerting pipeline, not as evidence of an actual compromise. The product formerly called Azure Defender is now included in Microsoft Defender for Cloud. See Validate Defender for Cloud alerts and Microsoft Defender for Servers overview.

QUESTION NO: 55

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Yes. Adding the designated decoy accounts as Honeytoken accounts through Entity tags meets the goal. In Microsoft Defender for Identity, a honeytoken is an existing Active Directory user account intentionally designated as a decoy. It should not be used for ordinary business activity, so attempts to authenticate with it, enumerate it, or otherwise interact with it can provide a high-confidence signal of malicious reconnaissance or lateral-movement activity. This makes honeytoken accounts suitable accounts for attackers to discover and attempt to exploit.

Microsoft Defender for Identity supports configuring honeytokens in the portal by locating the relevant user entity and applying the Honeytoken tag under Entity tags. After the tag is applied, Defender for Identity monitors activity involving the account and can generate detections when suspicious use occurs. The account must already exist in Active Directory; tagging it identifies it to Defender for Identity as the intentional deception account rather than creating a new account. For implementation guidance, Microsoft recommends ensuring that the account appears realistic in the environment but remains unused by legitimate users.

See Manage sensitive and honeytoken accounts in Microsoft Defender for Identity and Manage entity tags in Microsoft Defender for Identity.

QUESTION NO: 56

You use Azure Sentinel.

You need to receive an alert in near real-time whenever Azure Storage account keys are enumerated.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a livestream

B. Add a data connector

C. Create an analytics rule

D. Create a hunting query.

E. Create a bookmark.

ANSWER: B C

Explanation:

“Add a data connector” is required because Microsoft Sentinel must first ingest the Azure control-plane events that record Storage account key enumeration. The Azure Activity connector brings Azure subscription Activity Log events into the workspace, including administrative operations performed through Azure Resource Manager. A query can then identify the relevant key-listing operation, such as the Storage resource provider’s `listKeys` action, along with the caller, target resource, time, and operation status.

“Create an analytics rule” is required to turn that detected event into an alert. Scheduled analytics rules execute a Kusto Query Language query at a configured frequency and generate alerts and incidents when matching records are found. For near-real-time notification, configure the rule with an appropriate short query frequency and lookup period, while accounting for Activity Log ingestion latency. The rule can also map entities and attach useful event details so that security analysts can investigate the key-enumeration activity promptly.

Microsoft documents the Azure Activity data connector and the Activity Log data it collects at Azure Activity connector for Microsoft Sentinel. Analytics-rule configuration and alert generation are described in Detect threats with analytics rules in Microsoft Sentinel.

QUESTION NO: 57

Your company deploys the following services:

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.

Which two roles should assign to the analyst? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)

B. the Active remediation actions role in Microsoft Defender for Endpoint

C. the Security Administrator role in Azure Active Directory (Azure AD)

D. the Security Reader role in Azure Active Directory (Azure AD)

ANSWER: B D

Explanation:

The **Security Reader role in Azure Active Directory (Azure AD)** provides the security analyst with read-only access to security information and reports in the Microsoft security portal. This role supports access to the security experience without assigning broad administrative permissions, which follows the least-privilege requirement.

The **Active remediation actions role in Microsoft Defender for Endpoint** supplies the specific Defender for Endpoint RBAC permission needed to manage pending remediation actions. In Defender for Endpoint, automated investigation and response can generate actions that require manual approval or rejection. Assigning this role enables the analyst to review and act on those pending remediation decisions while avoiding unnecessary permissions to manage Defender settings, users, or other tenant-wide security configuration.

Combining read access through Security Reader with the narrowly targeted Active remediation actions permission gives the analyst the required portal visibility and remediation-approval capability. Microsoft documents Defender for Endpoint custom RBAC roles and the permissions associated with remediation actions in its Defender RBAC guidance. See Microsoft Defender for Endpoint role-based access control and Microsoft Entra Security Reader permissions.

QUESTION NO: 58

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

You discover that when Microsoft Defender for Endpoint generates alerts for a commonly used executable file, it causes alert fatigue. You need to tune the alerts.

Which two actions can an alert tuning rule perform for the alerts?

Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. delete

B. hide

C. resolve

D. merge

E. assign

ANSWER: B C

Explanation:

hide and **resolve** are supported actions for Microsoft Defender XDR alert tuning rules. Alert tuning is designed to reduce operational noise from alerts that analysts have determined are expected, benign, or otherwise do not require recurring investigation. For example, a rule can match alerts from Microsoft Defender for Endpoint based on properties such as the alert title, detection source, or entities associated with a repeated executable-related detection.

Using **hide** removes matching alerts from normal alert queue views, helping analysts focus on alerts that require attention while preserving the alert data for audit and review. This is useful when the organization wants to suppress repeated visibility of a known, accepted pattern without removing the underlying detection capability.

Using **resolve** automatically closes matching alerts so that recurring, understood detections do not remain active and inflate the operational workload. The rule applies consistently to future matching alerts, which makes it appropriate for reducing alert fatigue caused by a frequently used executable after its behavior has been validated.

Microsoft documents alert tuning actions and the supported rule configuration workflow in Alert tuning in Microsoft Defender XDR. Related alert-management behavior is described in Manage alerts in Microsoft Defender XDR.