DUMPSBOSS.

Microsoft Security Operations Analyst

Microsoft SC-200

Version Demo

Total Demo Questions: 20

Total Premium Questions: 455

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1 - (DRAG DROP)

DRAG DROP

You have an Azure subscription that contains two users named User1 and User2 and a Microsoft Sentinel workspace named workspace1. You need to ensure that the users can perform the following tasks in workspace1:

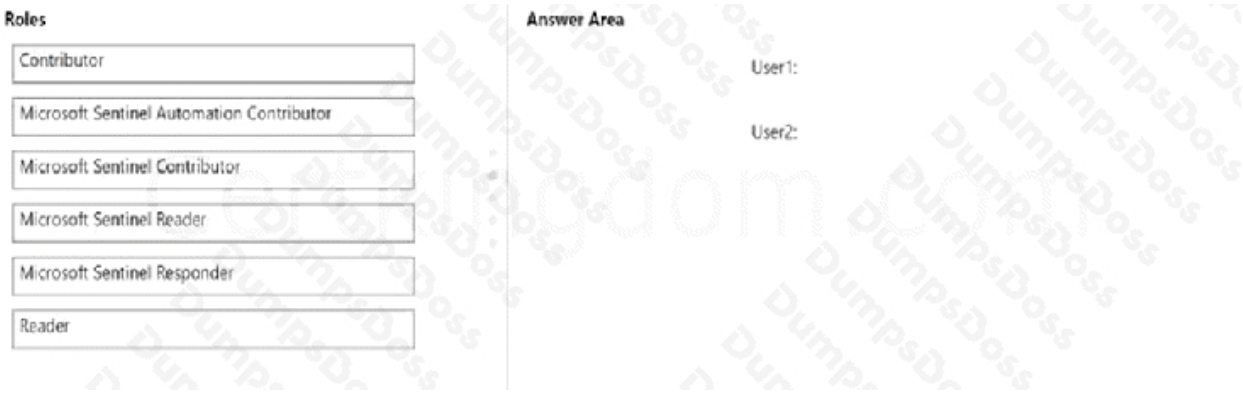
User1 must be able to dismiss incidents and assign incidents to users.

User2 must be able to modify analytics rules.

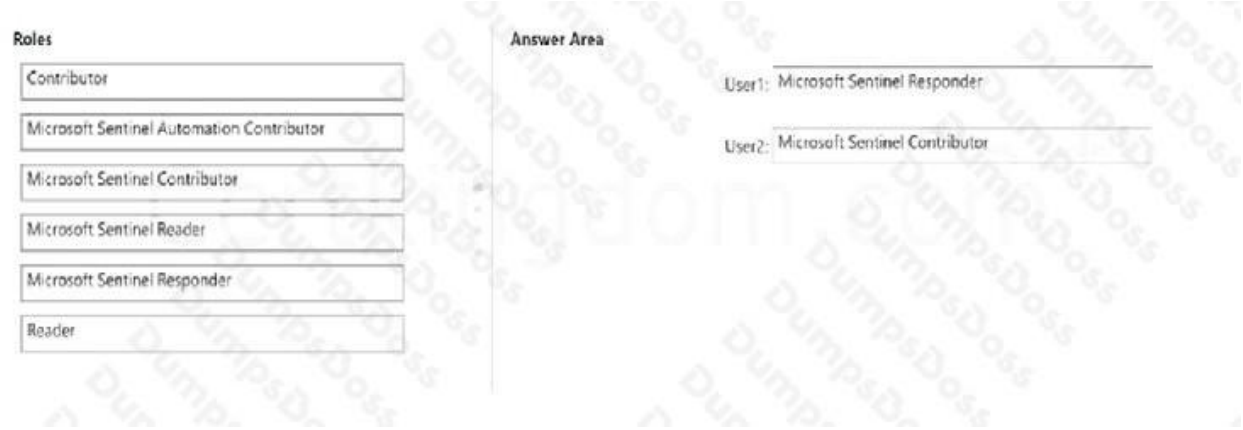
The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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:

QUESTION NO: 2

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: D E

Explanation:

To collect Windows security event data at scale, you want Defender for Cloud to automatically deploy and configure the needed agents on all (and future) VMs. Turning on **automatic provisioning** does exactly that, so you don't have to touch 100 servers one-by-one, which saves a lot of admin time.

Once the machines are connected to the Log Analytics workspace, you also need the workspace to actually ingest the Windows events you care about. Setting the workspace data collection to **All Events** ensures the full set of Windows Security Events is collected, which is what Defender for Cloud relies on for detections and investigations.

The other options don't really fit: Endpoint Manager auto-enrollment is for device management, and Event Grid is for event routing—not Windows security logs. "Common" collection reduces data, but it can miss events Defender for Cloud may need. References: https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection and https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events

QUESTION NO: 3

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:

To kick off something automatically when Defender for Cloud detects risky access (like a suspicious IP hitting your Storage account), you use workflow automation. That feature lets you react to Defender for Cloud alerts and route them into an automated response.

The usual way to do that response is with a Logic App that starts when a Defender for Cloud (Security Center) alert is created. Once the alert-triggered Logic App fires, it can run whatever steps you need—like calling Azure Automation to run a PowerShell runbook, invoking an Azure Function, or posting to an endpoint that runs your script.

A manual trigger won't help because you need this to happen automatically, and an HTTP trigger by itself doesn't connect to Defender for Cloud alerts unless something else calls it. App registration in Azure AD also isn't required just to wire up workflow automation for alert-driven playbooks.

References: https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation and https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview

QUESTION NO: 4

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

You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

B. The target workspace was deleted.

C. Permissions to the data sources of the rule query were modified.

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

ANSWER: A D

Explanation:

Intermittent failures in Microsoft Sentinel analytics rules usually point to issues that come and go, rather than something permanently broken. One common cause is simply that the KQL query sometimes takes too long—if it hits large data volumes, complex joins, or a busy cluster, it can exceed limits and time out.

Another realistic intermittent cause is data ingestion or availability problems. If there are temporary connectivity or ingestion hiccups between the data sources and the Log Analytics workspace, the query may run but return incomplete results or fail while the backend is under stress.

By contrast, a deleted workspace wouldn't be "intermittent"—the rule would fail consistently. And while permissions changes can break a rule, that's typically a steady failure after the change, not something that flaps on and off.

References: https://learn.microsoft.com/en-us/azure/sentinel/analytics-rule-concepts and https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-ingestion-time

QUESTION NO: 5

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.

Which two configurations should you modify? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

A. the Onboarding settings from Device management in Microsoft Defender Security Center

B. Cloud App Security anomaly detection policies

C. Advanced features from Settings in Microsoft Defender Security Center

D. the Cloud Discovery settings in Cloud App Security

ANSWER: C D

Explanation:

To restrict (block) cloud apps on a Windows device using Microsoft Defender for Endpoint, you're really relying on the Defender for Cloud Apps + MDE integration. First, in Microsoft Defender XDR (Defender portal), you need to make sure the integration feature is turned on under **Advanced features**. Without that switch enabled, Defender for Endpoint won't send the needed signals or enforce governance actions for discovered apps.

Second, you configure the actual app control behavior in Defender for Cloud Apps under **Cloud Discovery**. That's where you discover cloud apps used on endpoints, tag apps as sanctioned/unsanctioned, and then use governance actions (like blocking unsanctioned apps) that are enforced through MDE on the device.

Anomaly detection policies don't block apps—they mainly detect suspicious behavior. Onboarding is important to get the device into MDE, but it's not the specific setting you change to restrict cloud apps once the device is already managed.

References: https://learn.microsoft.com/en-us/defender-cloud-apps/mde-govern, https://learn.microsoft.com/en-us/defender-endpoint/enable-advanced-features

QUESTION NO: 6

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?

A. Run the Log Analytics Troubleshooting Tool.

B. Copy a executable and rename the file as ASC_AlerTest_662jf10N,exe

C. Modify the settings of the Microsoft Monitoring Agent.

D. Run the MMASetup executable and specify the -foo argument

ANSWER: B

Explanation:

To generate a “safe” test alert in Microsoft Defender for Cloud, the usual first step is to create the built-in test file that Defender for Cloud looks for. On Windows machines, that’s done by copying any executable and renaming it to the specific test name (ASC_AlertTest_662jfi039N.exe). When Defender for Cloud detects that file, it triggers a sample alert so you can confirm your agent and security monitoring pipeline are working end to end.

The other choices (running troubleshooting tools, changing MMA settings, or using a made-up installer argument) don’t actually simulate an attack pattern that Defender for Cloud uses to raise an alert. They might help if data isn’t flowing, but they won’t reliably create a security alert by themselves.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation

QUESTION NO: 7 - (HOTSPOT)

HOTSPOT

You have an on-premises datacenter that contains a custom web app named Appl. App1 uses Active Directory Domain Services (AD DS) authentication and is accessible by using Microsoft Entra application proxy.

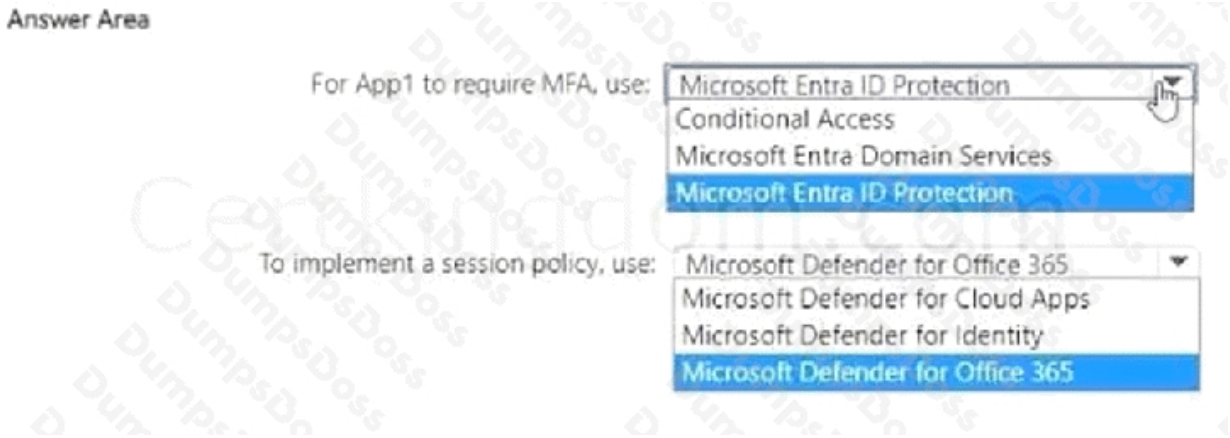
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You receive an alert that a user downloaded highly confidential documents.

You need to remediate the risk associated with the alert by requiring multi-factor authentication (MFA) when users use App1 to initiate the download of documents that have a Highly Confidential sensitivity label applied.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



ANSWER:

Explanation:

To force MFA for a specific app like App1 (published through Entra application proxy), you do that with **Conditional Access**, not Entra ID Protection. Then, to control the user session and apply controls like restricting/conditioning downloads (including based on sensitivity labels), you use **Microsoft Defender for Cloud Apps** session controls (Conditional Access App Control).

References: Conditional Access overview, Defender for Cloud Apps session controls (Conditional Access App Control)

QUESTION NO: 8

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

You have an Azure subscription that contains a Microsoft Sentinel workspace named Workspace 1. All Microsoft Defender XDR events are ingested into Workspace1.

You have a Microsoft Entra tenant.

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

You need to ensure that query1 runs every hour. The solution must minimize administrative effort. What should you configure?

A. an automation rule

B. automated investigation and response (AIR)

C. a watchlist

D. a custom detection rule

ANSWER: D

Explanation:

To run a KQL query on a schedule (like every hour) in Microsoft Sentinel with the least ongoing effort, you'd use a **custom (scheduled) analytics detection rule**. That rule runs your query automatically at the interval you choose and can generate incidents or alerts when it finds matching results.

The other choices don't really fit the "run this query every hour" need. Automation rules trigger *after* an alert/incident is created, AIR is Defender's automated response flow (not a Sentinel query scheduler), and watchlists are just reference data you can join to queries—they don't execute queries on a timer.

So the clean, built-in way is to create a scheduled analytics rule in Sentinel and paste in query1, then set the rule frequency to 1 hour.

References: https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom https://learn.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION NO: 9

You have a Microsoft 365 E5 subscription that contains a database server named DB1. DB1 is onboarded to Microsoft Defender XDR.

You need to ensure that DB1 appears on the attack surface map. What should you configure?

A. a critical asset rule

B. an asset rule

C. a honeytoken entity tag

D. a sensitive entity tag

ANSWER: A

Explanation:

To make sure a specific high-value server like DB1 shows up on the attack surface map, you typically need to mark it as something Defender should treat as "important" and track as part of your organization's key assets. That's what a **critical asset rule** is for—it helps Defender identify and highlight important devices (like database servers, domain controllers, crown-jewel systems) so they're surfaced in views such as the attack surface map.

The other choices don't really fit. An "asset rule" isn't the feature used for surfacing devices on the attack surface map in Defender XDR. Honeytoken and sensitive entity tags are more about deception and labeling entities for investigation context, not forcing a device to appear on the attack surface map.

Reference: https://learn.microsoft.com/en-us/defender-xdr/critical-assets

QUESTION NO: 10

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 in Microsoft Sentinel works best when it can correlate alerts and signals across identity and SaaS activity. For the "suspicious sign-ins" part, you don't just want raw sign-in logs—you want the higher-fidelity risk detections (like "leaked credentials" or "atypical travel"), which come from Azure AD Identity Protection. So, adding the Azure AD Identity Protection connector gives Fusion the right identity-risk inputs to correlate.

For the Office 365 side, Fusion relies on having the Office 365 activity data flowing into Sentinel. Creating analytics rules from the Office 365 connector templates helps you surface the relevant Office 365 anomalies as alerts/incidents that Fusion can stitch together into a multi-stage story.

References: https://learn.microsoft.com/en-us/azure/sentinel/fusion https://learn.microsoft.com/en-us/azure/sentinel/data-connectors-reference#azure-active-directory-identity-protection https://learn.microsoft.com/en-us/azure/sentinel/data-connectors-reference#office-365

QUESTION NO: 11

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: A

Explanation:

Yes, this meets the goal. Even if Microsoft Defender Antivirus is running in passive mode because a third-party AV is the primary antivirus, Microsoft Defender for Endpoint can still provide detection and response capabilities through EDR. When you turn on Automated Investigation and Response (AIR), Defender for Endpoint can automatically investigate alerts and take remediation actions (like quarantining files, stopping malicious processes, or cleaning up persistence) based on what it finds.

The key idea is that you're not relying on Defender Antivirus real-time protection here. You're using Defender for Endpoint's post-breach protection: it can spot suspicious or malicious artifacts that the third-party AV missed, then AIR can help contain and remediate them across devices. This is exactly the kind of safety net you want in a "third-party AV + Defender passive mode" setup.

References: https://learn.microsoft.com/en-us/defender-endpoint/automated-investigations https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-compatibility

QUESTION NO: 12 - (DRAG DROP)

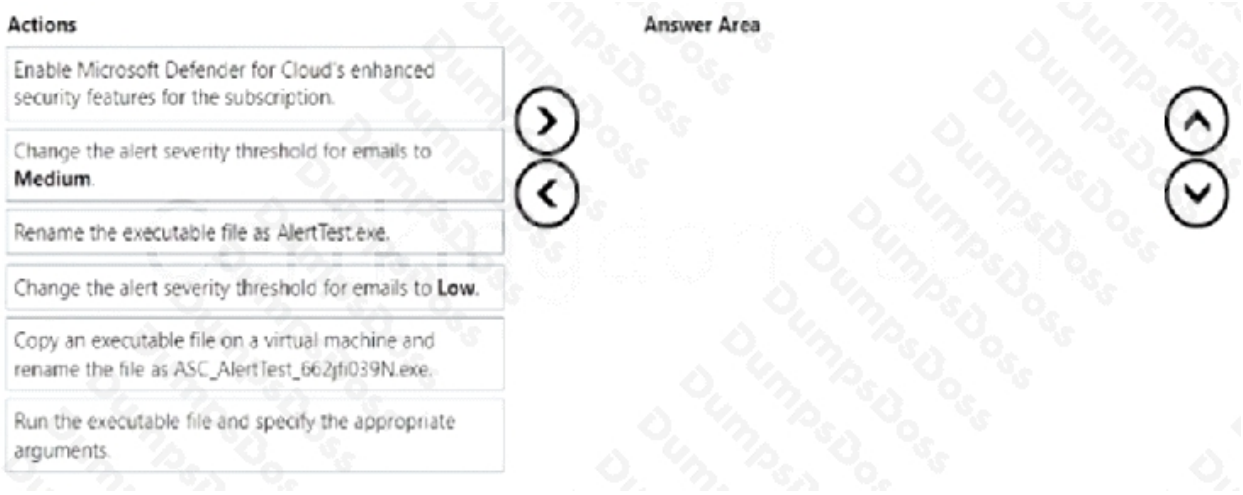
DRAG DROP

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.

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

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



ANSWER:

Explanation:

The Answer Area is blank in the provided image, so the response is incomplete/incorrect.

To trigger the built-in Defender for Cloud alert validation on a Windows VM, you first need Defender for Cloud's enhanced security enabled for the subscription, then you place the special test executable on the VM using the exact required filename, and finally you run it with the documented arguments. The "change email severity threshold" options and renaming the file to `AlertTest.exe` aren't part of the alert validation workflow.

Reference: Alert validation in Microsoft Defender for Cloud

QUESTION NO: 13 - (HOTSPOT)

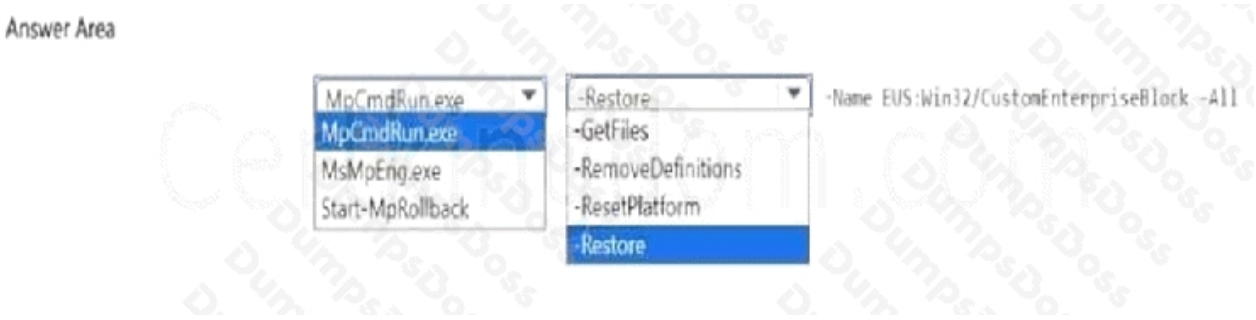
HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.

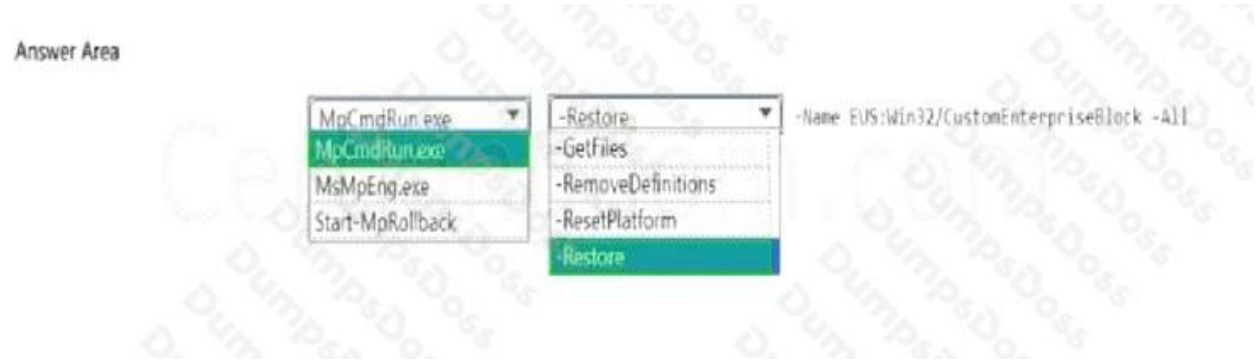
Twenty files on Device1 are quarantined by custom indicators as part of an investigation. You need to release the 20 files from quarantine.

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

NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

The selected options are correct. **MpCmdRun.exe** is the Microsoft Defender Antivirus command-line utility, and the **-Restore** switch is used to restore items from quarantine. Using **-All** restores all quarantined items that match the specified threat name, which fits the requirement to release all 20 files.

References: Run Microsoft Defender Antivirus scans and use command-line tools, Microsoft Defender Antivirus command-line arguments

QUESTION NO: 14

You use Microsoft 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 bookmark.

B. Create an analytics rule.

C. Create a livestream.

D. Create a hunting query.

E. Add a data connector.

ANSWER: B E

Explanation:

To get near real-time alerts in Microsoft Sentinel, you need two things: the right logs coming in, and a rule that turns those log events into incidents/alerts. That's why you start by adding the appropriate data connector, so Sentinel can ingest the Azure activity that records Storage account key listing events (for example, "List Storage Account Keys").

Once the data is flowing, you create an analytics rule. Analytics rules run on a schedule (often every few minutes) and can generate an alert and incident when the query matches, which is exactly what you want for "near real-time" notification.

A hunting query is useful for manual investigation and proactive searching, but it doesn't automatically alert you. Bookmarks and livestream are also investigation tools, not alerting mechanisms.

References: https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources and https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom

QUESTION NO: 15

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

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

NOTE: Each correct selection is worth one point.

A. Resolve the alert automatically.

B. Hide the alert.

C. Create a suppression rule scoped to any device.

D. Create a suppression rule scoped to a device group.

E. Generate the alert.

ANSWER: A B D

Explanation:

To get rid of noisy, known-good macro alerts without weakening security, you typically do two things: hide what's already cluttering the queue, and prevent the same "known false positive" from showing up again.

First, you can **hide the alert**. That removes it from the main Alerts queue view so analysts aren't wasting time on it, but it doesn't change your detection capability.

Next, create a **suppression rule scoped to a device group**

Finally, you'll want to **resolve the alert automatically** (or mark it as resolved after validation) so it's treated as handled and doesn't keep appearing as an open item. Together, these steps keep the queue clean while still allowing the alert to fire elsewhere if the same behavior shows up in other teams.

References: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts and https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/suppression-rules

QUESTION NO: 16

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.

You need to ensure that the Fusion rule can generate alerts.

What should you do?

A. Disable, and then enable the rule.

B. Add data connectors

C. Create a new machine learning analytics rule.

D. Add a hunting bookmark.

ANSWER: B

Explanation:

Fusion is a built-in analytics rule that relies on signals coming from other data sources and detections. If you've just deployed Microsoft Sentinel and Fusion isn't firing, the most common reason is simply that there isn't enough data flowing in yet for Fusion to correlate anything.

To fix that, you need to connect and start ingesting relevant logs by configuring data connectors (for example, Microsoft Entra ID, Microsoft Defender products, Microsoft 365, Azure Activity, and so on). Once those connectors are sending data into Sentinel, Fusion has the raw events it needs to correlate activity and generate incidents.

Disabling/re-enabling the rule won't help if there's no data to work with, and creating a new ML rule or adding a hunting bookmark doesn't feed Fusion either—those are separate features. The real requirement is getting the right telemetry into the workspace.

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

QUESTION NO: 17

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan Z and contains 1,000 Windows devices.

You have a PowerShell script named Script Vps1 that is signed digitally.

You need to ensure that you can run Script1.psl in a live response session on one of the devices. What should you do first from the live response session?

A. Run the library command.

B. Run the putfile command

C. Modify the PowerShell execution policy of the device.

D. Upload Script1.ps 1 to the library.

ANSWER: D

Explanation:

In Microsoft Defender for Endpoint Live Response, you can't just run any local PowerShell script directly. The normal way to run a script is to first place it in the Live Response *library*, which is basically the approved script repository that Live Response can access.

Once the script is uploaded to the library, you can pull it down to the device and run it during the session. That's why "Upload Script1.ps1 to the library" is the first step—you're making it available to Live Response in a supported way.

Commands like `putfile` are used to copy files to the device during a session, but you still need the script available in the library first if you want to run it as a Live Response script. Changing the device execution policy isn't the right move here either; Live Response is meant to be controlled and auditable, and the library approach is the expected method.

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

QUESTION NO: 18

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:

In Sentinel, the built-in ASIM parsers can be updated when Microsoft ships newer versions. If you want to “freeze” what you’re using, you need to stop relying on the auto-managed built-in parser directly and instead use your own copy/versioned layer.

One way is to redeploy the built-in parser as a workspace resource (a copy you control) and set the parameters so your environment prefers your deployed version rather than the built-in one. That effectively prevents automatic changes from impacting your queries because you’re no longer using the Microsoft-managed definition.

Another solid approach is to build your own custom unifying parser and explicitly reference a specific parser version. That keeps your normalization stable, because your custom parser won’t magically change when Microsoft updates the built-in one.

Just referencing the parser in hunting queries or analytics rules doesn’t stop updates—those queries will still resolve to whatever the current built-in parser definition is.

References: https://learn.microsoft.com/en-us/azure/sentinel/normalization-about-parsers and https://learn.microsoft.com/en-us/azure/sentinel/normalization

QUESTION NO: 19

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: You add each account as a Sensitive account.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No, marking accounts as *Sensitive accounts* doesn't create "bait" for attackers. Sensitive accounts are treated as high-value identities, so Defender for Identity gives them extra attention and helps reduce noise (for example, by focusing alerts and monitoring around those important users).

If your goal is to set up accounts that attackers might try to use (and then get detected when they do), you're looking for *honeytoken accounts*. Honeytokens are intentionally planted decoy accounts that should never be used in real life—so any activity on them is suspicious and can trigger alerts.

In short: "Sensitive" is for protecting real important accounts, while "honeytoken" is for catching bad behavior with decoys. More details here: https://learn.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

QUESTION NO: 20

You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.

You need to mitigate the following device threats:

What should you use?

A. Microsoft Defender Antivirus

B. attack surface reduction rules in Microsoft Defender for Endpoint

C. Windows Defender Firewall

D. adaptive application control in Azure Defender

ANSWER: B

Explanation:

The best fit here is **attack surface reduction (ASR) rules in Microsoft Defender for Endpoint**. ASR rules are designed to prevent common attack techniques that target Windows endpoints and Office apps—things like blocking Office from creating child processes, stopping Office from making suspicious executable content, and blocking credential stealing behaviors. That's exactly the kind of "device threat mitigation" you typically need across a large Windows 10 + Microsoft 365 fleet.

Microsoft Defender Antivirus and Windows Defender Firewall are important, but they're more general-purpose protections. ASR rules are more specific and proactive for the common real-world threats that come through Office and user activity. Azure Defender's adaptive application control is aimed more at server/workload scenarios (like Azure VMs) rather than managing Office-focused endpoint attack vectors on 1,000 Windows 10 devices.

More details: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction