MS-500$^{\text{Q\&As}}$

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled. The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors. You need to ensure that you can detect when sensitive groups are modified and when malicious services

are created.

What should you do?

A. Configure Azure ATP notifications

B. Configure Event Forwarding on the domain controllers

C. Configure auditing in the Office 365 Security and Compliance center

D. Modify the Domain synchronizer candidate settings on the Azure ATP sensors

Correct Answer: B

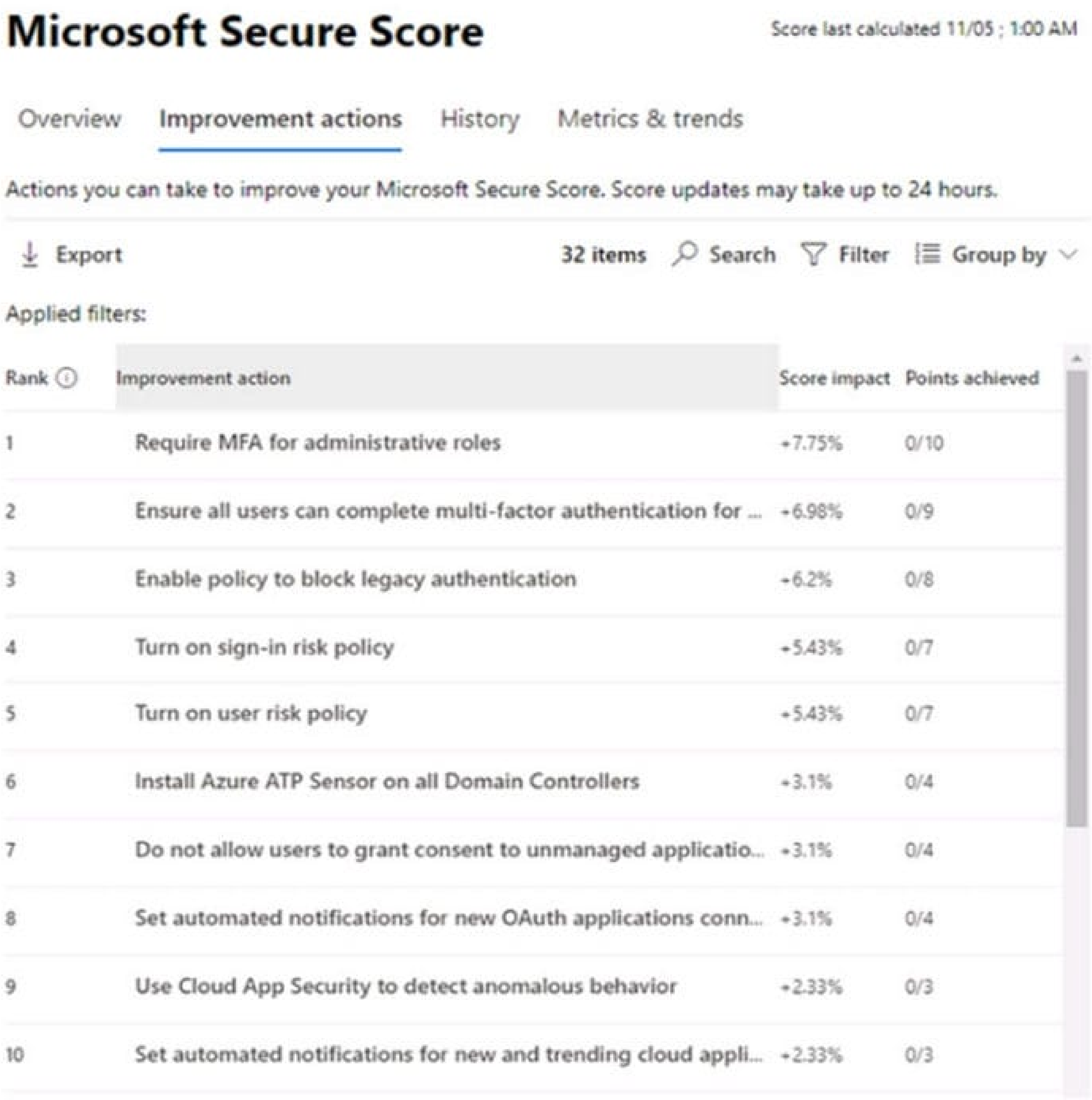
Reference: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

QUESTION 2

HOTSPOT

You have a Microsoft 365 subscription that contains 100 users.

Microsoft Secure Score for the subscription is shown in the following exhibit.



Microsoft Secure Score

Score last calculated 11/05 ; 1:00 AM

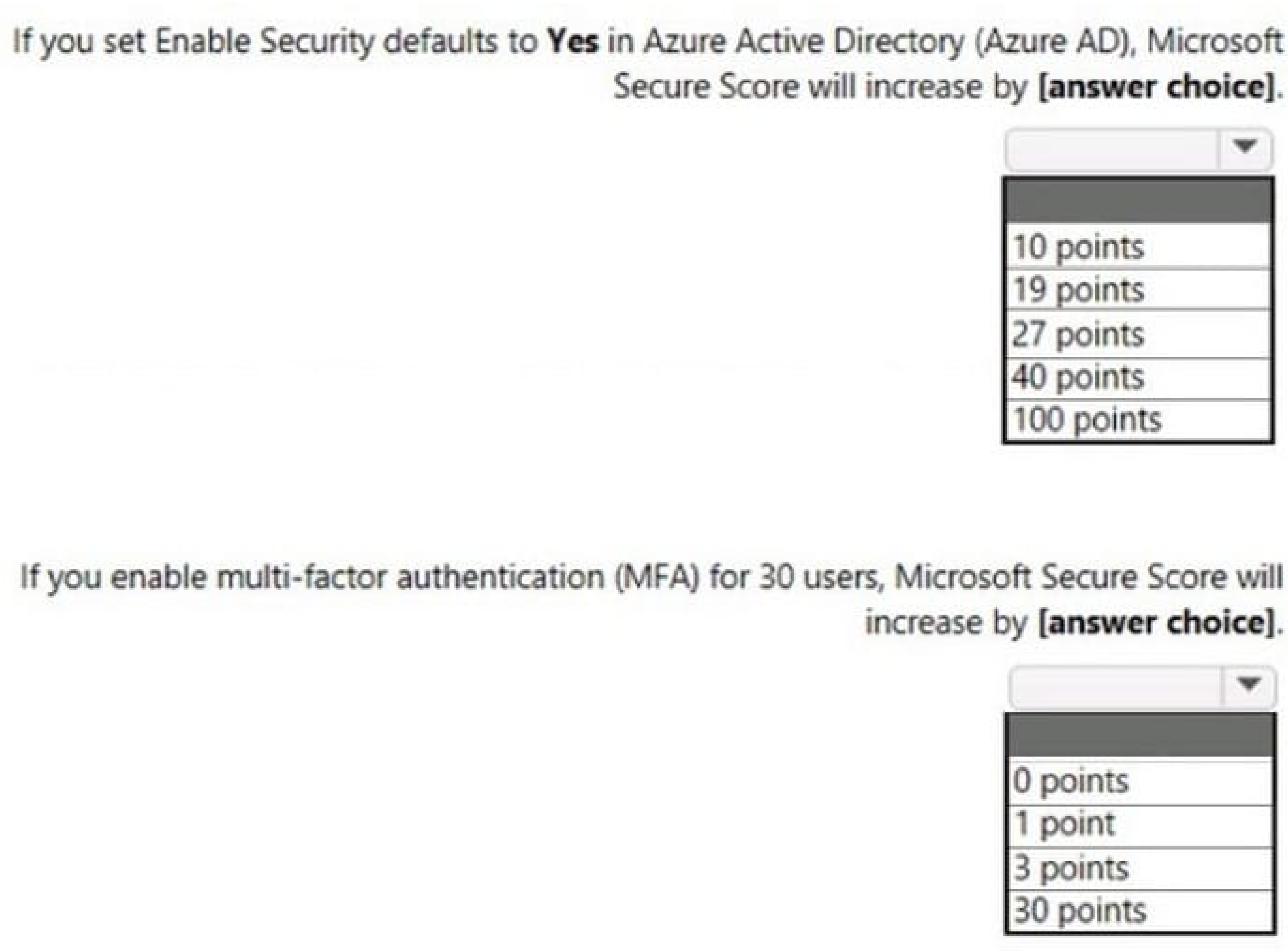
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters:

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+7.75%	0/10
2	Ensure all users can complete multi-factor authentication for ...	+6.98%	0/9
3	Enable policy to block legacy authentication	+6.2%	0/8
4	Turn on sign-in risk policy	+5.43%	0/7
5	Turn on user risk policy	+5.43%	0/7
6	Install Azure ATP Sensor on all Domain Controllers	+3.1%	0/4
7	Do not allow users to grant consent to unmanaged applicatio...	+3.1%	0/4
8	Set automated notifications for new OAuth applications conn...	+3.1%	0/4
9	Use Cloud App Security to detect anomalous behavior	+2.33%	0/3
10	Set automated notifications for new and trending cloud appli...	+2.33%	0/3

Use the drop-down menus to select the answer choice that completes each statement based on the the information presented in the graphic. NOTE: Each correct selection is worth one point.

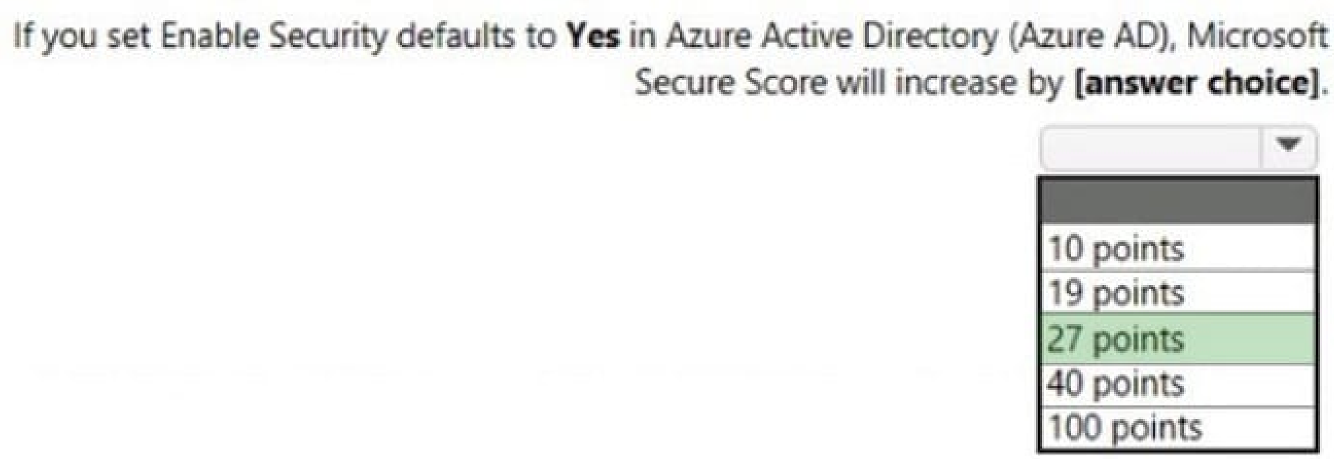
Hot Area:



If you set Enable Security defaults to **Yes** in Azure Active Directory (Azure AD), Microsoft Secure Score will increase by **[answer choice]**.

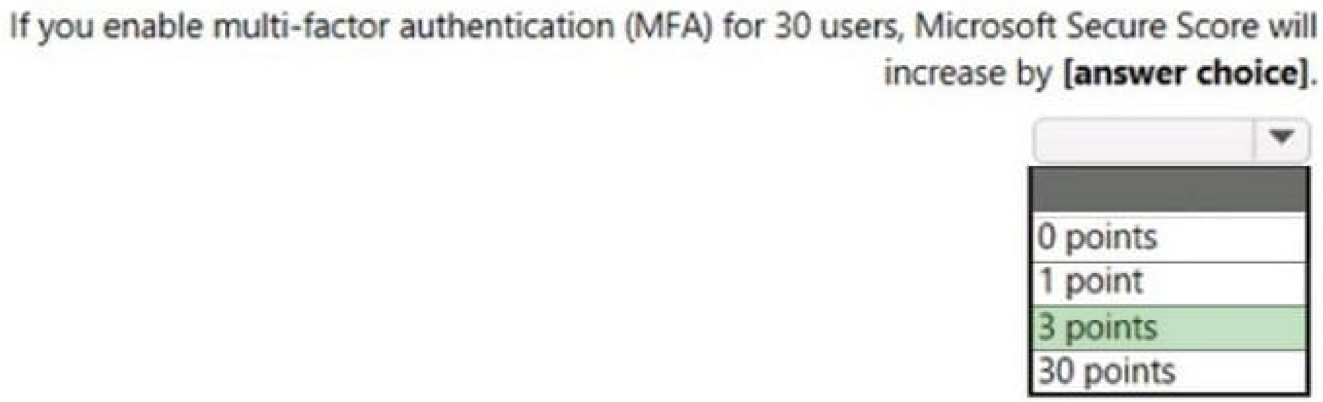
If you enable multi-factor authentication (MFA) for 30 users, Microsoft Secure Score will increase by **[answer choice]**.

Correct Answer:



If you set Enable Security defaults to **Yes** in Azure Active Directory (Azure AD), Microsoft Secure Score will increase by **[answer choice]**.

10 points
19 points
[✓ 27 points]
40 points
100 points



If you enable multi-factor authentication (MFA) for 30 users, Microsoft Secure Score will increase by **[answer choice]**.

0 points
1 point
[✓ 3 points]
30 points

Box 1: 27 points

Security defaults

Microsoft Secure Score has updated improvement actions to support security defaults in Azure Active Directory, which make it easier to help protect your organization with pre-configured security settings for common attacks.

If you turn on security defaults, you\\'ll be awarded full points for the following improvement actions:

Ensure all users can complete multi-factor authentication for secure access (9 points)

Require MFA for administrative roles (10 points)

Enable policy to block legacy authentication (7 points)

Box 2: 3 points

Some improvement actions only give points when fully completed. Some give partial points if they\\'re completed for some devices or users.

In this case: 30/100 * 10 = 3 points

Note: How improvement actions are scored

Each improvement action is worth 10 points or less, and most are scored in a binary fashion. If you implement the improvement action, like create a new policy or turn on a specific setting, you get 100% of the points. For other improvement

actions, points are given as a percentage of the total configuration.

For example, an improvement action states you get 10 points by protecting all your users with multi-factor authentication. You only have 50 of 100 total users protected, so you\\'d get a partial score of 5 points (50 protected / 100 total * 10 max

pts = 5 pts).

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score

QUESTION 3

You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA).

To complete this task, sign in to the Microsoft Office 365 admin center.

Correct Answer: See explanation below.

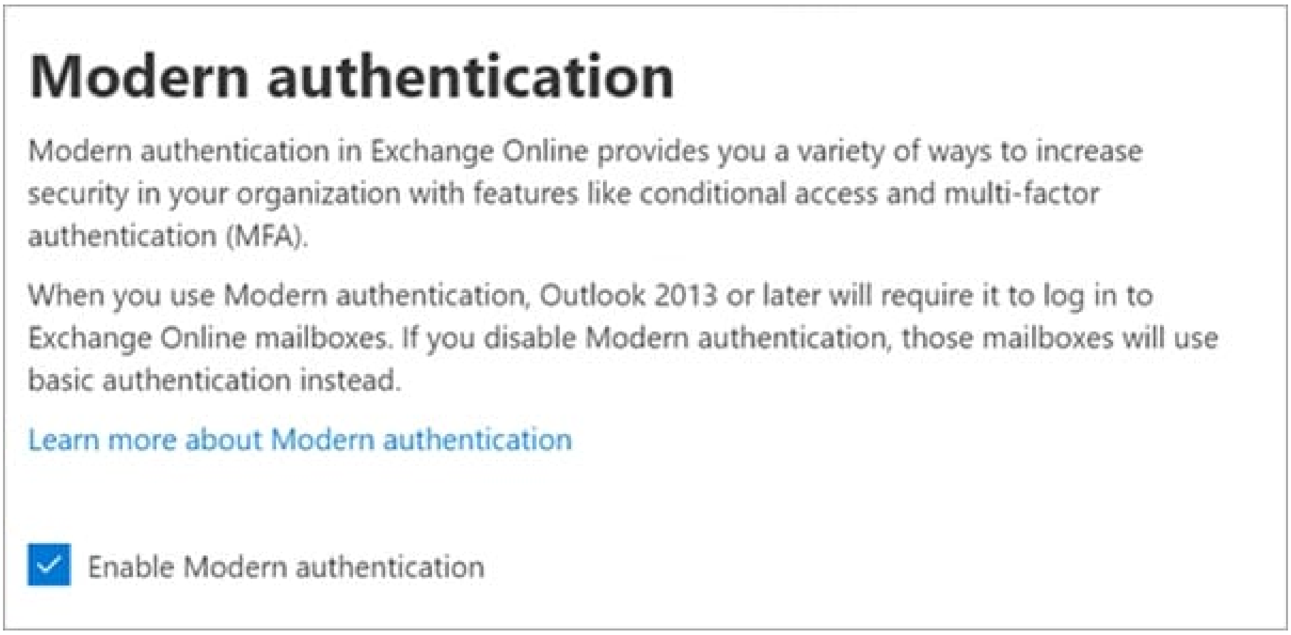
Enable Modern authentication for your organization

1.

To enable modern authentication, from the admin center, select Settings > Settings and then in the Services tab, choose Modern authentication from the list.

2.

Check the Enable modern authentication box in the Modern authentication panel.



Modern authentication

Modern authentication in Exchange Online provides you a variety of ways to increase security in your organization with features like conditional access and multi-factor authentication (MFA).

When you use Modern authentication, Outlook 2013 or later will require it to log in to Exchange Online mailboxes. If you disable Modern authentication, those mailboxes will use basic authentication instead.

Learn more about Modern authentication

☑ Enable Modern authentication

Enable multi-factor authentication for your organization

1.

In the admin center, select Users and Active Users.

2.

In the Active Users section, Click on multi-factor authentication.

3.

On the Multi-factor authentication page, select user if you are enabling this for one user or select Bulk Update to enable multiple users.

4.

Click on Enable under Quick Steps.

5.

In the Pop-up window, Click on Enable Multi-Factor Authentication.

After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices.

Reference: https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

QUESTION 4

DRAG DROP

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains a Windows 10 device named Device1.

You have a PowerShell script named script1 that collects forensic data and saves the results as a file on the device from which the script is run.

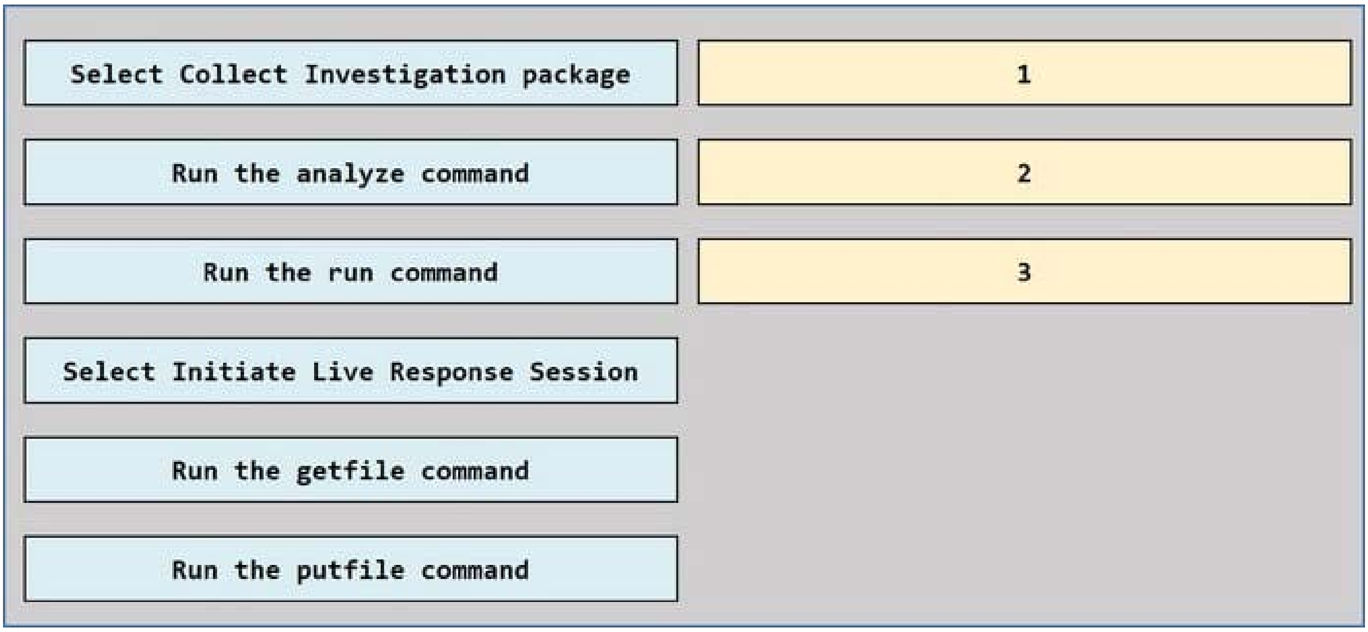
You receive a Microsoft Defender for Endpoint alert for suspicious activities on Device1.

You need to run script1 on Device1 and retrieve the output file of the script.

Which four actions should you perform in sequence in Microsoft 365 Defender portal?

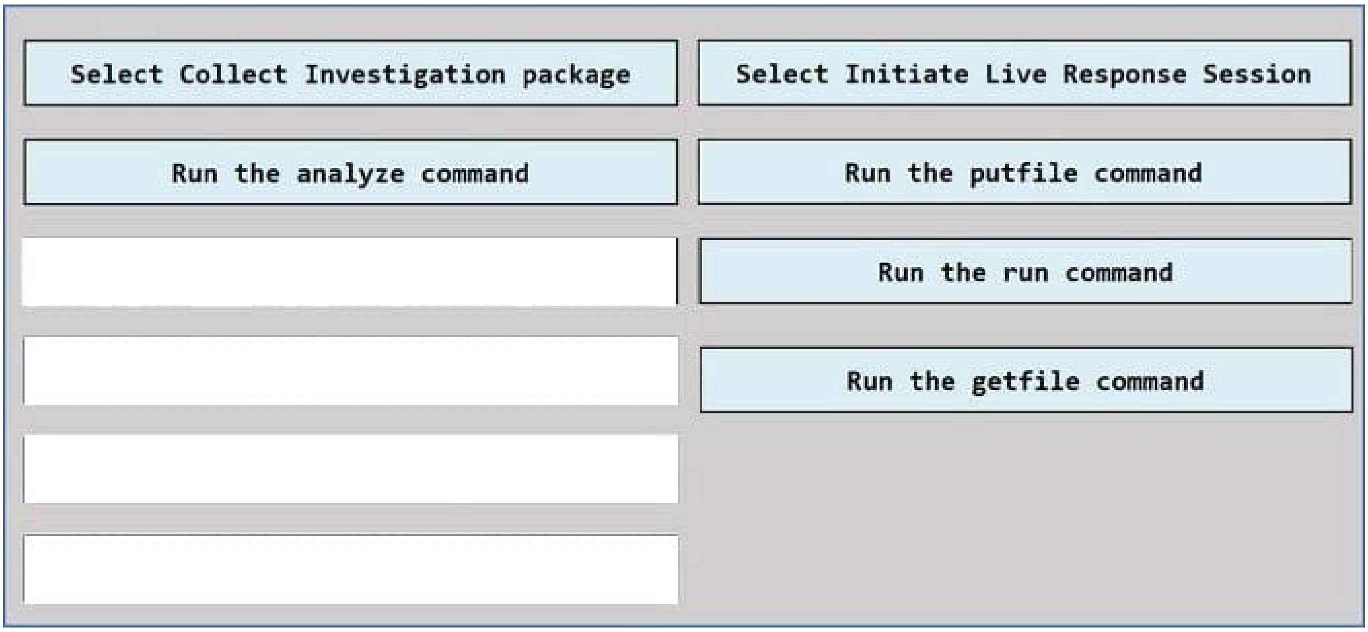
To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Select Collect Investigation package	1
Run the analyze command	2
Run the run command	3
Select Initiate Live Response Session	
Run the getfile command	
Run the putfile command	

Correct Answer:



Select Collect Investigation package	Select Initiate Live Response Session
Run the analyze command	Run the putfile command
	Run the run command
	Run the getfile command

Step 1: Select Initiate Live Response Session. Initiate a live response session on a device

1.

Sign in to Microsoft 365 Defender portal.

2.

Navigate to Endpoints > Device inventory and select a device to investigate. The devices page opens.

3.

Launch the live response session by selecting Initiate live response session. A command console is displayed. Wait while the session connects to the device.

4.

Use the built-in commands to do investigative work.

5.

After completing your investigation, select Disconnect session, then select Confirm.

Note: Initiate live response Session

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions to promptly contain identified

threats in real time.

Live response is designed to enhance investigations by enabling you to collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.

Step 2: Run the putfile command

putfile - Puts a file from the library to the device. Files are saved in a working folder and are deleted when the device restarts by default.

Step 3: Run the run command

run - Runs a PowerShell script from the library on the device.

Step 4: Run the getfile command

getfile - Downloads a file.

For scenarios when you\\'d like get a file from a device you\\'re investigating, you can use the getfile command. This allows you to save the file from the device for further investigation.

Incorrect:

*

Select Collect Investigation package.

Collect investigation package from devices

As part of the investigation or response process, you can collect an investigation package from a device. By collecting the investigation package, you can identify the current state of the device and further understand the tools and techniques

used by the attacker.

*

Run the analyze command

Analyze - Analyses the entity with various incrimination engines to reach a verdict.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts

QUESTION 5

You have a Microsoft 365 E5 subscription.

You plan to implement retention policies for Microsoft Teams.

Which item types can be retained?

A. voice memos from the Teams mobile client

B. code snippets

C. embedded images

Correct Answer: C

Code snippets, recorded voice memos from the Teams mobile client, thumbnails, announcement images, and reactions from others in the form of emoticons aren\\'t retained when you use retention policies for Teams.

Reference:

https://docs.microsoft.com/en-us/microsofteams/teams-recording-policy