Microsoft Security Operations Analyst

1. You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts.
What should you review?

A. the status update time

B. the resolution method of the source computer

C. the alert status

D. the certainty of the source computer

Answer(s): D

---

2. The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive

B. sales

C. marketing

Answer(s): B

---

3. The issue for which team can be resolved by using Microsoft Defender for Office 365?

A. executive

B. marketing

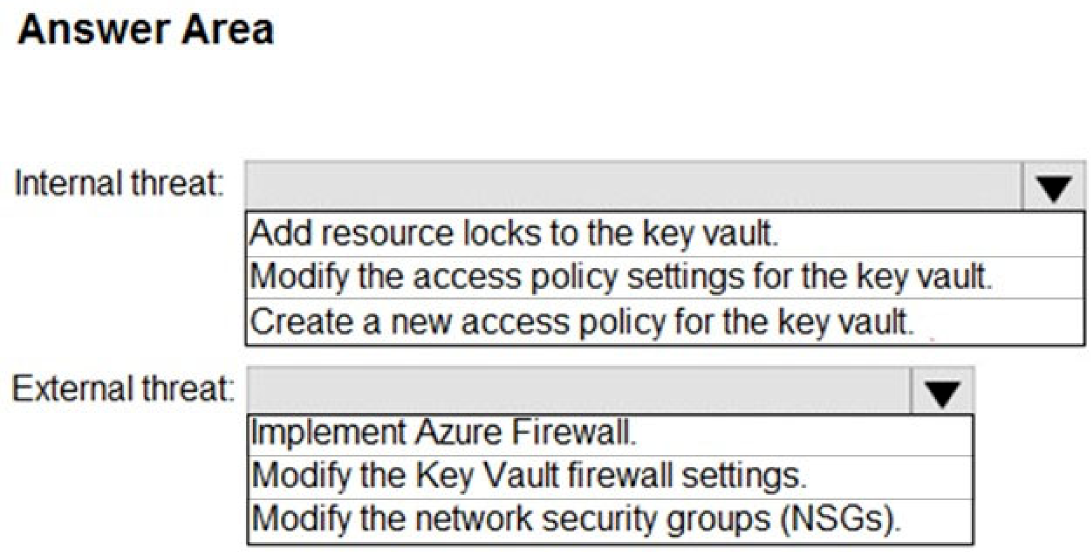
C. security

D. sales

Answer(s): B

---

4. HOTSPOT (Drag and Drop is not supported)
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Internal threat:
- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Create a new access policy for the key vault.

External threat:
- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

A. See Explanation section for answer.

Answer(s): A

---

5. You need to implement the Azure Information Protection requirements. What should you configure first?

A. Device health and compliance reports settings in Microsoft Defender Security Center

B. scanner clusters in Azure Information Protection from the Azure portal

C. content scan jobs in Azure Information Protection from the Azure portal

D. Advanced features from Settings in Microsoft Defender Security Center

Answer(s): D

---

6. You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

A. Activity from suspicious IP addresses

B. Activity from anonymous IP addresses

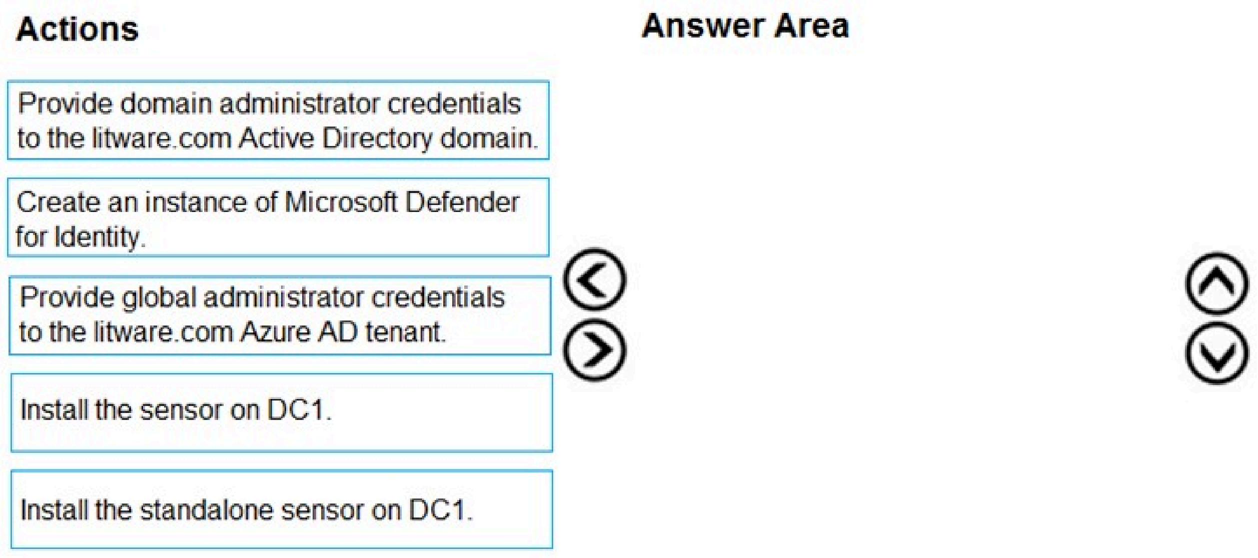
C. Impossible travel

D. Risky sign-in

Answer(s): C

---

7. DRAG DROP (Drag and Drop is not supported)
You need to configure DC1 to meet the business requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Provide domain administrator credentials to the litware.com Active Directory domain.

Create an instance of Microsoft Defender for Identity.

Provide global administrator credentials to the litware.com Azure AD tenant.

Install the sensor on DC1.

Install the standalone sensor on DC1.

Answer Area

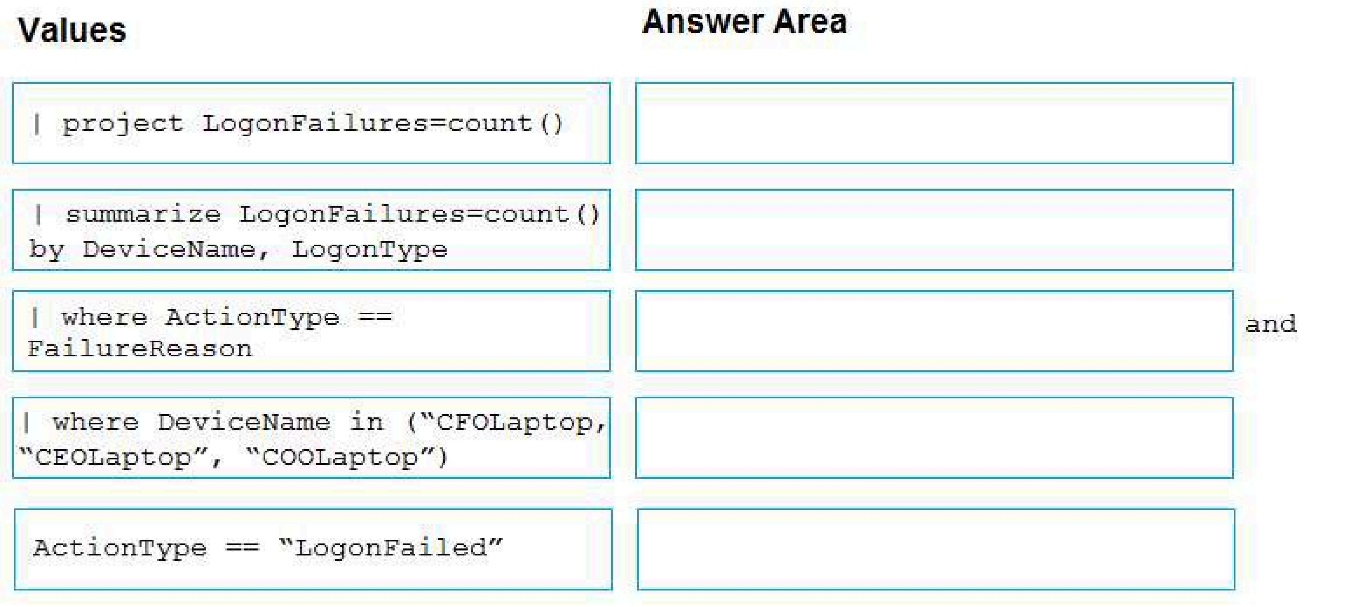
A. See Explanation section for answer.

Answer(s): A

---

8. DRAG DROP (Drag and Drop is not supported)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Select and Place:



Values

```
| project LogonFailures=count()
```

```
| summarize LogonFailures=count()
by DeviceName, LogonType
```

```
| where ActionType ==
FailureReason
```

```
| where DeviceName in (“CFOLaptop,
“CEOLaptop”, “COOLaptop”)
```

```
ActionType == “LogonFailed”
```

Answer Area

and

A. See Explanation section for answer.

Answer(s): A

---

9. You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?

A. Impossible travel

B. Activity from anonymous IP addresses

C. Activity from infrequent country

D. Malware detection

Answer(s): C

---

10. 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(s): C

---

11. 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.

□ B.

□ C.

□ D.

Answer(s): B C

---

12. 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.

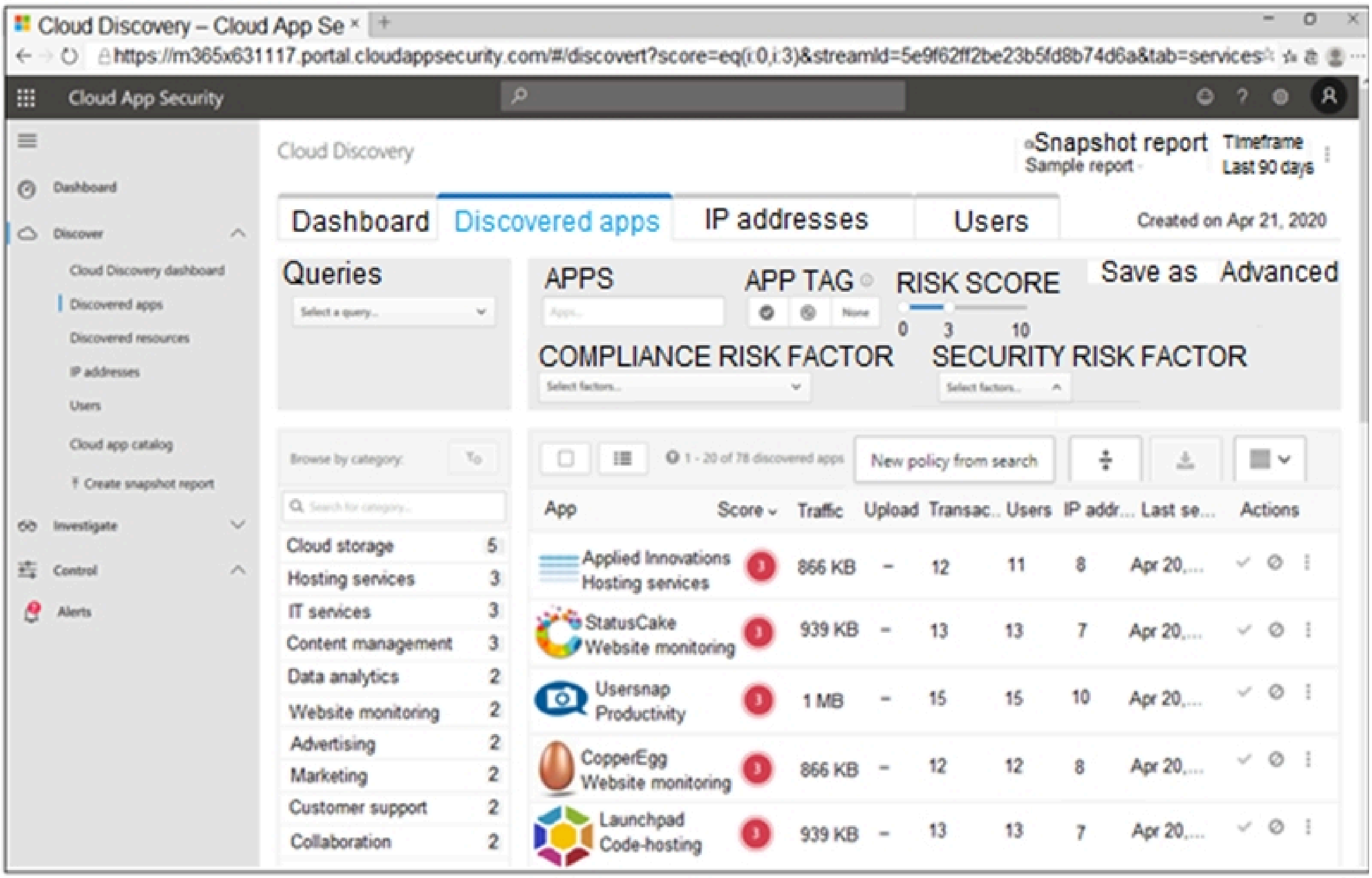
□ E. Generate the alert.

Answer(s): B D E

---

13. DRAG DROP (Drag and Drop is not supported)

You open the Cloud App Security portal as shown in the following exhibit.



Cloud Discovery – Cloud App Se ×

https://m365x631117.portal.cloudappsecurity.com/#/discover?score=eq(i:0,i:3)&streamId=5e9f62ff2be23b5fd8b74d6a&tab=services

Cloud App Security

Cloud Discovery

Snapshot report: Sample report

Timeframe: Last 90 days

Dashboard | Discovered apps | IP addresses | Users

Created on Apr 21, 2020

Queries: Select a query...

APPS: Apps...

APP TAG

RISK SCORE: 0 3 10

Save as | Advanced

COMPLIANCE RISK FACTOR: Select factors...

SECURITY RISK FACTOR: Select factors...

Browse by category

Category	Count
Cloud storage	5
Hosting services	3
IT services	3
Content management	3
Data analytics	2
Website monitoring	2
Advertising	2
Marketing	2
Customer support	2
Collaboration	2

1 - 20 of 78 discovered apps

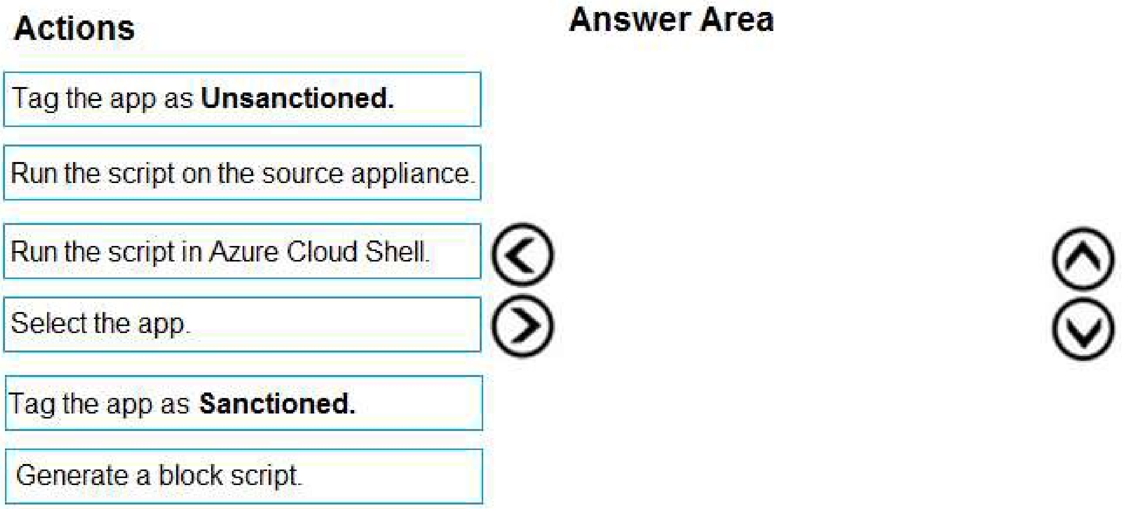
New policy from search

App	Score	Traffic	Upload	Transac...	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	3	866 KB	-	12	11	8	Apr 20,...	
StatusCake Website monitoring	3	939 KB	-	13	13	7	Apr 20,...	
Usersnap Productivity	3	1 MB	-	15	15	10	Apr 20,...	
CopperEgg Website monitoring	3	866 KB	-	12	12	8	Apr 20,...	
Launchpad Code-hosting	3	939 KB	-	13	13	7	Apr 20,...	

You need to remediate the risk for the Launchpad app.

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

Select and Place:



Actions

Tag the app as **Unsanctioned.**

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned.**

Generate a block script.

Answer Area

A. See Explanation section for answer.

Answer(s): A

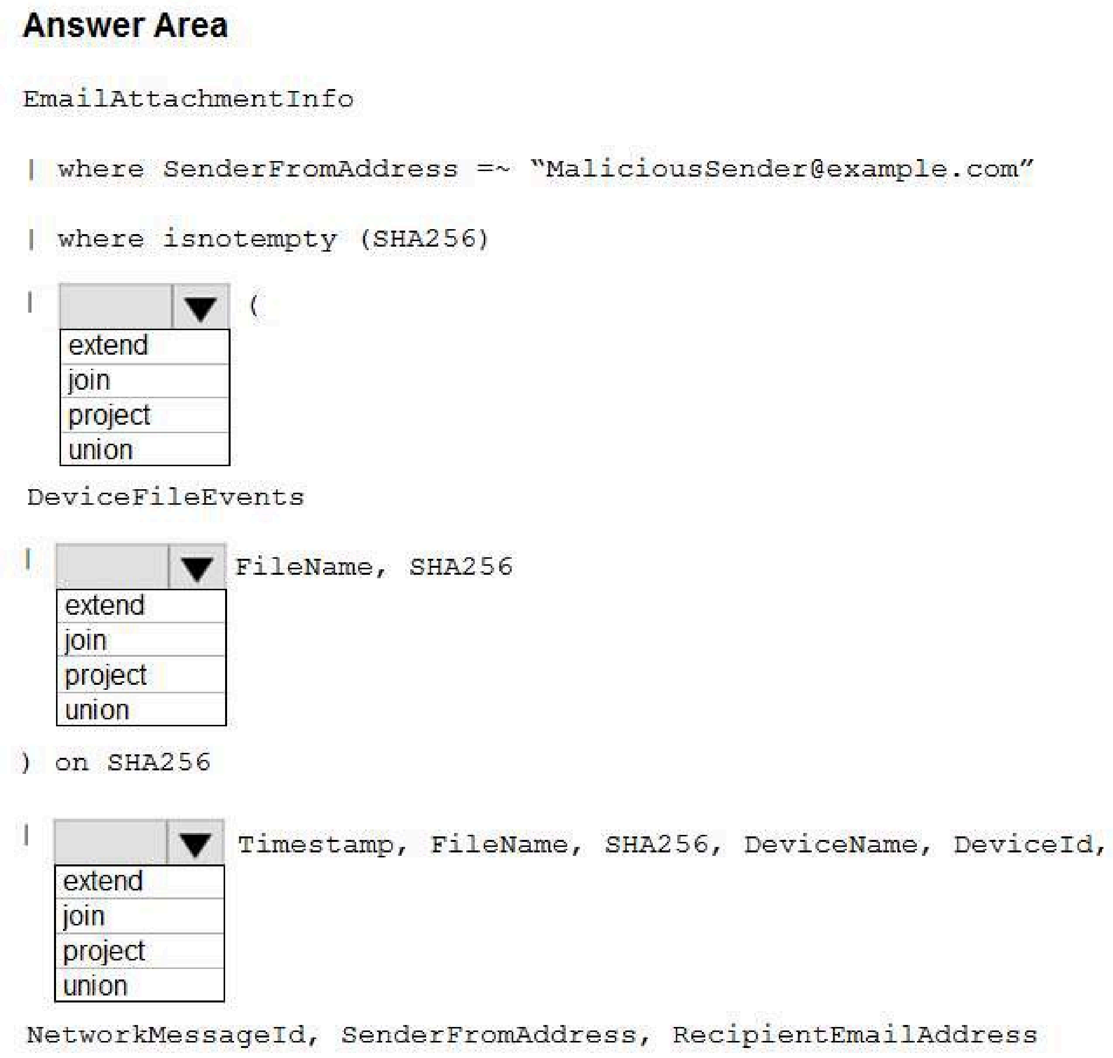
---

14. HOTSPOT (Drag and Drop is not supported)

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain 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 area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|            (
```

```
DeviceFileEvents

|            FileName, SHA256
```

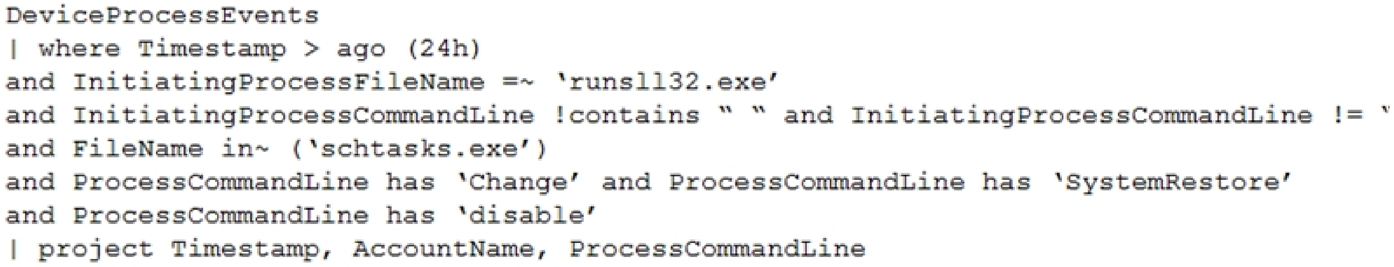
```
) on SHA256

|            Timestamp, FileName, SHA256, DeviceName, DeviceId,
```

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

A. See Explanation section for answer.

Answer(s): A

15. You have the following advanced hunting query in Microsoft 365 Defender.



```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != '
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.
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 detection rule.

□ B. Create a suppression rule.

□ C. Add | order by Timestamp to the query.

□ D. Replace DeviceProcessEvents with DeviceNetworkEvents.

□ E. Add DeviceId and ReportId to the output of the query.

Answer(s): A E

---

16. You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.
You have three custom device groups.
You need to be able to temporarily group the machines to perform actions on the devices.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

□ A. Assign a tag to the device group.

□ B. Add the device users to the admin role.

□ C. Add a tag to the machines.

□ D. Create a new device group that has a rank of 1.

□ E. Create a new admin role.

□ F. Create a new device group that has a rank of 4.

Answer(s): A C D

---

17. Note: This question is part of a series ofquestions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Somequestionsets 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(s): A

---

18. 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 Azure Identity Protection, you configure the sign-in risk policy.
Does this meet the goal?

A. Yes

B. No

Answer(s): B

---

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 the accounts to an Active Directory group and add the group as a Sensitive group.
Does this meet the goal?

A. Yes

B. No

Answer(s): B

---

20. You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

A. Dynamic Delivery

B. Replace

C. Block and Enable redirect

D. Monitor and Enable redirect

Answer(s): A