ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Topic 1, Contoso Ltd

Case study

Overview

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment

End-User Environment

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements

Planned Changes

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.

Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

```
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where        == True
```

Question: 1

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

A. executive

B. sales

C. marketing

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft- defender-atp-ios

Question: 2

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

A. executive

B. marketing

C. security

D. sales

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and- teams?view=o365-worldwide

Question: 3

HOTSPOT for the Azure virtual

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.

Answer Area

Internal threat. N

Add resource locks to the key vault Modify the access policy settings for the key vault.

Modify the role-based access control (RBAC) settings for the key vault

External threat: ▼

Implement Azure Firewall

Modify the Key Vault firewall settings

Modify the network security groups (NSGs).

Answer:

Explanation:

Answer Area

Internal threat: i

Add resource locks to the key vault. Modify the access policy settings for the key vault
Modify the role-based access control (RBAC) settings for the key vault

External threat: V

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

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

Question: 4

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.
What should you include in the recommendation?

A. just-in-time (JIT) access

B. Azure Defender

C. Azure Firewall

D. Azure Application Gateway

Answer: B

Explanation:

Reference:

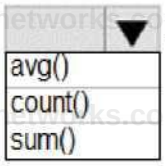
https://docs.microsoft.com/en-us/azure/security-center/azure-defender

Question: 5

HOTSPOT

You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

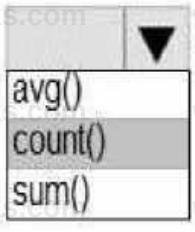

```
| where TimeStamp > ago(2d)
| summarize activityCount =
```




```
by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Answer:


```
| where TimeStamp > ago(2d)
| summarize activityCount =
```




```
by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Question: 6

You need to remediate active attacks to meet the technical requirements.What should you include in the solution?

A. Azure Automation runbooks

B. Azure Logic Apps

C. Azure Functions

D. Azure Sentinel livestreams

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Question: 7

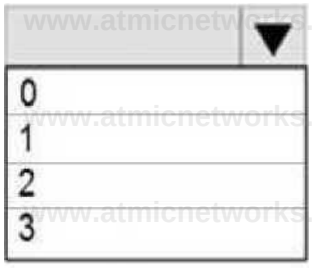
HOTSPOT

You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.

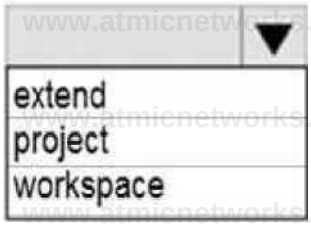
What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:



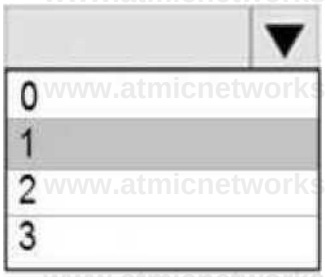
Query element required to correlate data between tenants:



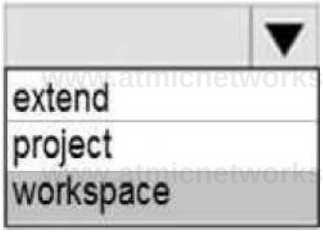
Answer:

Explanation:

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:



Query element required to correlate data between tenants:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Question: 8

You need to complete the query for failed sign-ins to meet the technical requirements.

Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center

B. Activity log in Azure

C. Azure Advisor

D. the query windows of the Log Analytics workspace

Answer: D

Explanation:

Topic 2, Litware inc.

Case study

Overview

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18 04 LTS

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.

Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

- The principle of least privilege must be used whenever possible.
- Costs must be minimized, as long as all other requirements are met.
- Logs collected by Log Analytics must provide a full audit trail of user activities.
- All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection – Data discovery dashboard.

Microsoft Defender for Endpoint requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security requirements

Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements

All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

Integrate Azure Sentinel and Cloud App Security.

Ensure that a user named admin1 can configure Azure Sentinel playbooks.

Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.

Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.

Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question: 9

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: D

Explanation:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information- protection-in-windows-overview

Question: 10

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: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Question: 11

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.

Which role should you assign?

A. Automation Operator
B. Automation Runbook Operator
C. Azure Sentinel Contributor
D. Logic App Contributor

Answer: C

Explanation:

Reference:

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

Question: 12

You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

A. From Set rule logic, turn off suppression.

B. From Analytics rule details, configure the tactics.

C. From Set rule logic, map the entities.

D. From Analytics rule details, configure the severity.

Answer: C

Explanation:

Reference:

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

Question: 13

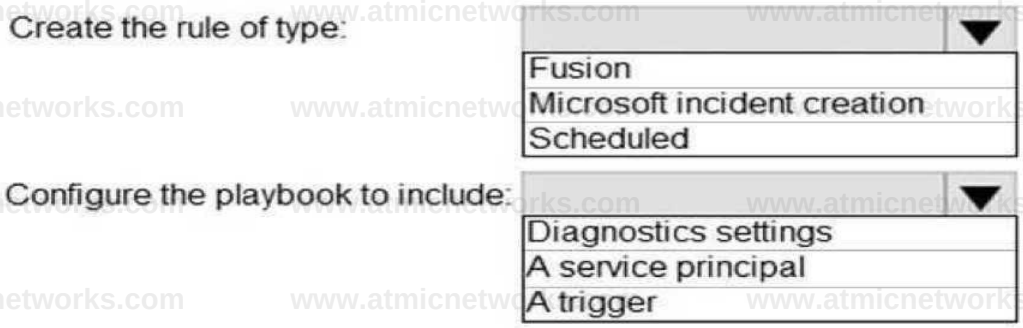
HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include

Diagnostics settings
A service principal
A trigger

Question: 14

DRAG DROP

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

Install the sensor on DC1

Install the standalone sensor on DC1

Answer Area

Answer:

Explanation:

Provide global administrator credentials to the litware com Azure AD tenant

Create an instance of Microsoft Defender for Identity.

Provide domain administrator credentials

l to the litware com Active Directory domain

Install the sensor on DC1

Step 1: log in to https://portal.atp.azure.com as a global admin

Step 2: Create the instance

Step 3. Connect the instance to Active Directory

Step 4. Download and install the sensor.

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/install-step1

https://docs.microsoft.com/en-us/defender-for-identity/install-step4

Question: 15

HOTSPOT

You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.

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

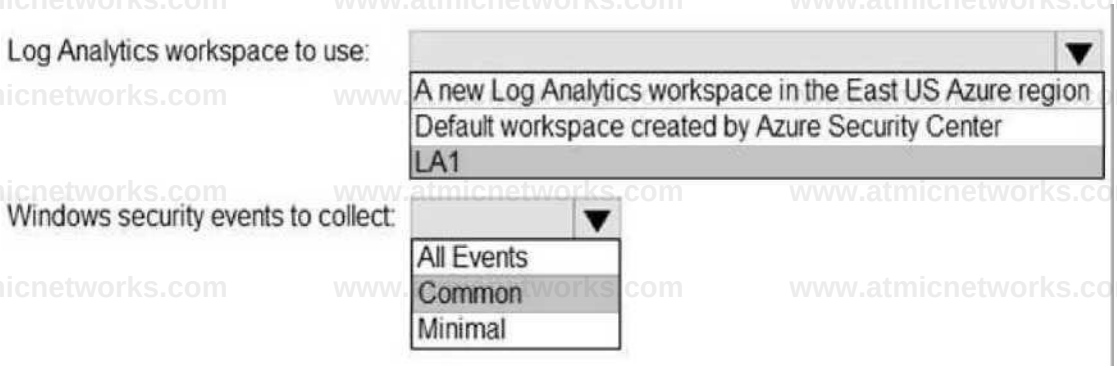
NOTE: Each correct selection is worth one point.

Log Analytics workspace to use: ▼ A new Log Analytics workspace in the East US Azure region Default workspace created by Azure Secunty Center LAI

Windows security events to collect: ▼
All Events
Common
Minimal

Answer:

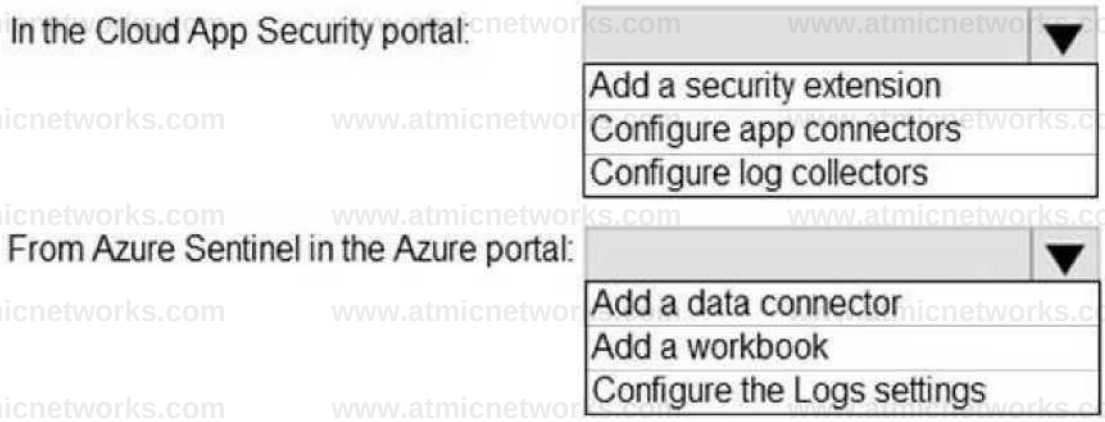
Explanation:



Question: 17

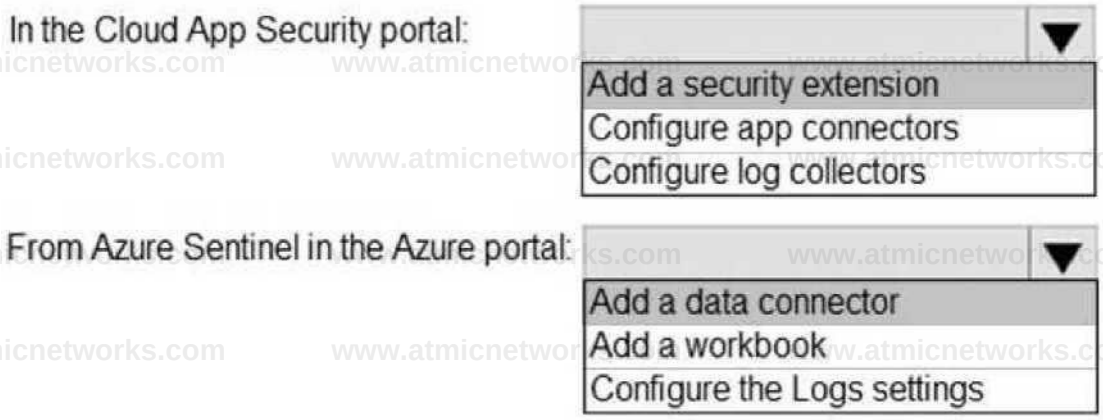
HOTSPOT

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

Question: 18

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: CD

Explanation:

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

Question: 19

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:

Question: 20

HOTSPOT

You need to configure the Microsoft Sentinel integration to meet the Microsoft Sentinel requirements. What should you do? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

In the Microsoft Defender for Cloud Apps portal [Adda Khanty extension'

•nston

Configure app connectors
Configure log collectors

From Microsoft Sentinel in the Azure portal [Ada a data connector

Add a workbook
Configure the Logs settings

Answer:

Explanation:

Answer Area

In the Microsoft Defender for Cloud Apps portal Add a security extension

From Microsoft Sentinel in the Azure portae Ado a data connector

Question: 21

HOTSPOT

You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements

and the business requirements. What should you include in the solution? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

Log Analytics workspace to use: ▼ A new Log Analytics workspace in the East US Azure region Default workspace created by Azure Security Center **LAI**

Windows security events to collect: ▼
All Events
Common
Minimal

Answer:

Explanation:

Answer Area

log Anal/tics workspace to use LAI

Windows security events to collect Common

Question: 22

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:

Question: 23

You need to modify the anomaly detection policy settings to meet the Microsoft Defender for Cloud Apps requirements and resolve the reported problem.

Which policy should you modify?

A. Activity from suspicious IP addresses

B. Risky sign-in

C. Activity from anonymous IP addresses

D. Impossible travel

Answer: D

Explanation:

Topic 3, Adatum Corporation

Overview

Adatum Corporation is a United States-based financial services company that has regional offices in New York, Chicago, and San Francisco.

The on-premises network contains an Active Directory Domain Services (AD DS) forest named corp.adatum.com that syncs with an Azure AD tenant named adatum.com. All user and group management tasks are performed in corp.adatum.com. The corp.adatum.com domain contains a group named Group! that syncs with adatum.com.

All the users at Adatum are assigned a Microsoft 365 E5 license and an Azure Active Directory Perineum 92 license.

The cloud environment contains a Microsoft 365 subscription, an Azure subscription linked to the adatum.com tenant, and the resources shown in the following table.

Name	Type	Description
Sentinel 1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery!
Server?	Azure virtual machine	Runs Windows Server 2022

The on-premises network contains the resources shown in the following table.

Name	Type	Description
Serveri	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webappl	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infobloxl	Infoblox DNS service	A third-party DNS service appliance linked to Sentinell by using a data connector

Adatum plans to perform the following changes;

- Implement a query named rulequery1 that will include the following KQL query.

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Nam« = tostring(split(Caller, '@'» 0)[0]), Account_0_UPN$uffix =
    tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerlpAddress, TimeGenerated
```

- Implement a Microsoft Sentinel scheduled rule that generates incidents based on rulequery1.

Adatum identifies the following Microsoft Defender for Cloud requirements:

- The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives.
- Microsoft Defender for Servers Plan 2 must be enabled on all the Azure virtual machines.
- Server2 must be excluded from agentless scanning.

Adatum identifies the following Microsoft Sentinel requirements:

- Implement an Advanced Security Information Model (ASIM) query that will return a count of DNS requests that results in an NXDOMAIN response from Infoblox1.
- Ensure that multiple alerts generated by rulequery1 in response to a single user launching Azure Cloud Shell multiple times are consolidated as a single incident.
- Implement the Windows Security Events via AMA connector for Microsoft Sentinel and configure it to monitor the Security event log of Server1.
- Ensure that incidents generated by rulequery1 are closed automatically if Azure Cloud Shell is launched by the company's SecOps team.

- Implement a custom Microsoft Sentinel workbook named Workbook1 that will include a query to dynamically retrieve data from Webapp1.
- Implement a Microsoft Sentinel near-real-time (NRT) analytics rule that detects sign-ins to a designated break glass account
- Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.
- Ensure that higher than normal volumes of password resets for corp.adatum.com user accounts are detected.
- Minimize the overhead associated with queries that use ASIM parsers.
- Ensure that the Group1 members can create and edit playbooks.
- Use built-in ASIM parsers whenever possible.

Adatum identifies the following business requirements:

- Follow the principle of least privilege whenever possible.
- Minimize administrative effort whenever possible.

Directory Perineum 92 license.

Question: 24

You need to configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements. What should you create first?

A. a Microsoft Sentinel automation rule

B. a Microsoft Sentinel scheduled query rule

C. a Data Collection Rule (DCR)

D. an Azure Event Grid topic

Answer: C

Explanation:

Question: 25

You need to implement the Defender for Cloud requirements.

What should you configure for Server2?

A. the Microsoft Antimalware extension

B. an Azure resource lock

C. an Azure resource tag

D. the Azure Automanage machine configuration extension for Windows

Answer: D

Explanation:

Question: 26

HOTSPOT

You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

ASIM parser: Im Dns
Im. Dns
Jm_Dns_InfobloxNIOS
imDns

Filter A filtering parameter
A filtering parameter
A pack parameter
The WHERE clause

Answer:

Explanation:

Answer Area

ASIM parser: Im_Dns

Filter: A filterinq parameter

Question: 27

HOTSPOT

You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

Data source to query:

JSON
A custom endpoint
A custom resource provider

On WebappT

Enable Cross-Orioin Resource Shinno fCORS)

Enable Same Origin Policy (SOP).
Enforce TLS12.

Answer

Explanation:

Answer Area

Data source to query: JSON

On Webappl: Enable Cross-Origin Resource Sharing (CORS).

Question: 28

You need to ensure that the configuration of HuntingQuery1 meets the Microsoft Sentinel requirements.

What should you do?

A. Add HuntingQuery1 to a livestream.

B. Create a watch list.

C. Create an Azure Automation rule.

D. Add HuntingQuery1 to favorites.

Answer: D

Explanation:

Question: 29

HOTSPOT

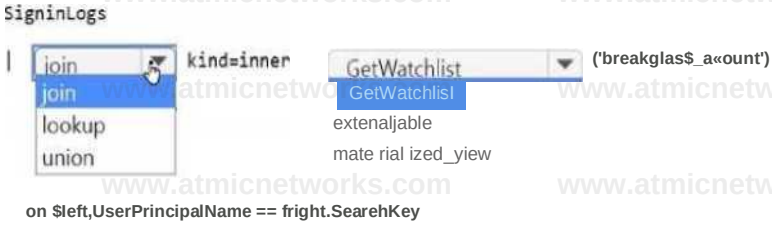
You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account.

The solution must meet the Microsoft Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

SigninLogs

I join ^ **kindainner** _GetWatchlist **on Heft.UserPrincipalName** ▼ **('breakglas$_account')**

s= fright.SearchKey

Question: 30

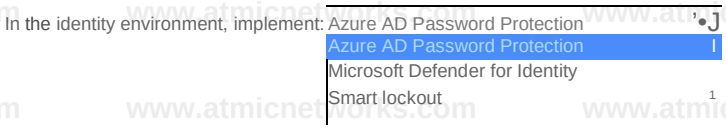
HOTSPOT

You need to monitor the password resets. The solution must meet the Microsoft Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area



In Microsoft Sentinel, configure: | The Windows Security Events via AMA connector] A Microsoft security rule

1 he Windows Security Events via AMA connector

| User and Entity Behavior Analytics (UEBA)

Answer:

Explanation:

Answer Area

In the identity environment, implement: Azure AD Password Protection

In Microsoft Sentinel, configure: The Windows Security Events via AMA connector

Question: 31

You need to ensure that the processing of incidents generated by rulequery1 meets the Microsoft Sentinel requirements.

What should you create first?

A. a playbook with an incident trigger

B. a playbook with an entity trigger

C. an Azure Automation rule

D. a playbook with an alert trigger

Answer: A

Explanation:

Question: 32

You need to implement the Defender for Cloud requirements.

Which subscription-level role should you assign to Group1?

A. Security Admin

B. Owner

C. Security Assessment Contributor

D. Contributor

Answer: B

Explanation:

Question: 33

You need to implement the scheduled rule for incident generation based on rulequery1.

What should you configure first?

A. entity mapping

B. custom details

C. event grouping

D. alert details

Answer: D

Explanation:

Question: 34

You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.

Which role should you assign to Group1?

A. Microsoft Sentinel Automation Contributor

B. Logic App Contributor

C. Automation Operator

D. Microsoft Sentinel Playbook Operator

Answer: C

Explanation:

Topic 4, Misc. Questions

Fabrikam. Inc. is a financial services company.

The company has branch offices in New York. London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled. The fabrikam.com forest contains two global groups named Group1 and Group2.

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license. Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Fabrikam has an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint
SAWkspcI	Azure Synapse Analytics workspace	SAWkspd hosts an Apache Spark pool named Pool1
LAWkspd	Log Analytics workspace	LAWkspd will be used in a planned Microsoft Sentinel implementation,

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

When the users use the VPN connections. Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives. Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Minimize the administrative effort required to investigate the false positive alerts.

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last30days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool! by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

Question: 35

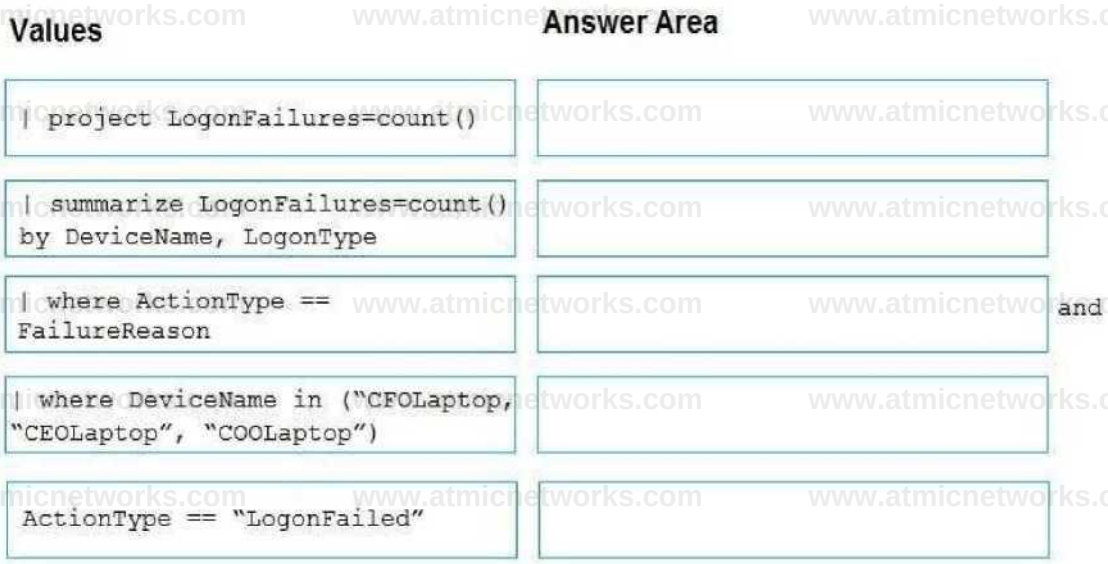
DRAG DROP

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.

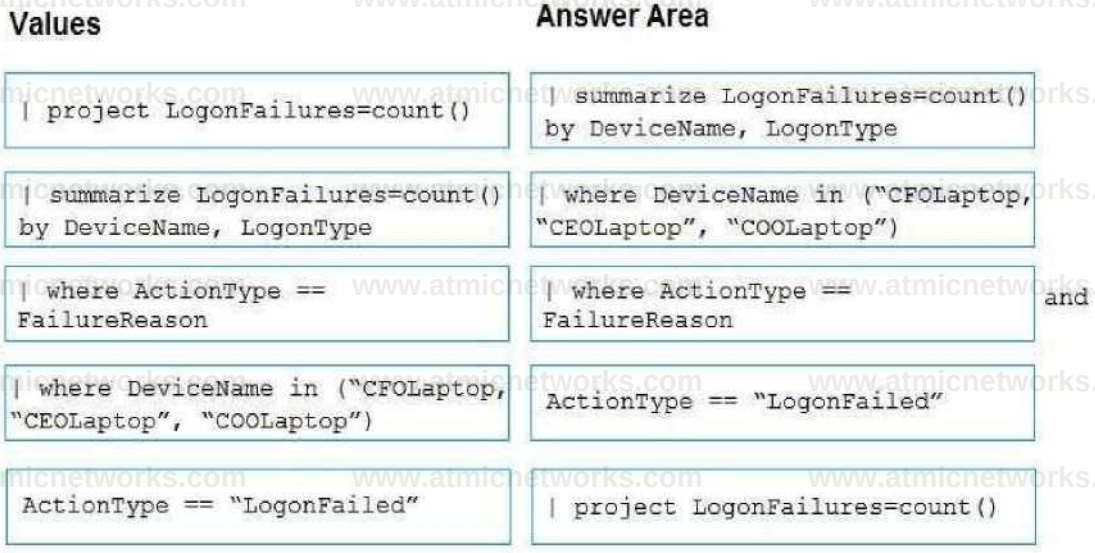
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 36

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: C

Explanation:

Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. Activity from the same user in different locations within a time period that is shorter than the expected travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN.

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Question: 37

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: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Question: 38

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 - AD5F3CS0688A -AttackSurfaceR8ductionHules_Actions Enabled

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

C. Add-MpPreference -AttackSurfaceReductionRulesIds D4F940AB -401B -4EFC -AADC -

ADSF3C50688A -AttackSurfaceReductionRules_Actions AuditMode

D. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC - AADC - AD5F3C50686A -AttackSurfaceReductionRules_Actions Enabled

A. Option A

B. Option B

C. Option C

D. Option D

Answer: BC

Explanation:

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/attack-surface- reduction

Question: 39

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: BCE

Explanation:

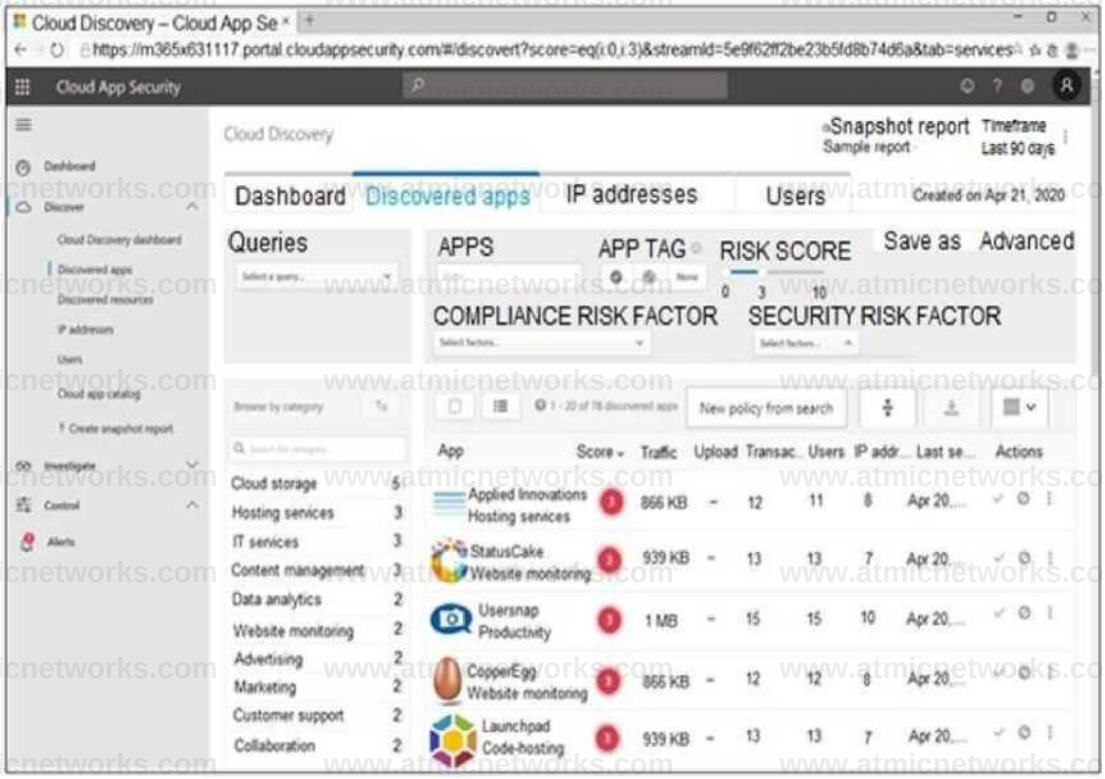
Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/manage-alerts

Question: 40

DRAG DROP

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



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.

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

Answer:

Explanation:

Actions	Answer Area
Tag the app as Unsanctioned.	Select the app.
Run the script on the source appliance.	Tag the app as Unsanctioned.
Run the script in Azure Cloud Shell.	Generate a block script.
Select the app.	on the source
Tag the app as Sanctioned.	
Generate a block script.	

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

Question: 41

HOTSPOT

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.

Answer Area

```
Ema ilAt t achmentInfo

| where SenderFromAddress =~ "MaliciousSender8example.com"

| where isnotempty (SHA256)
```

1 ¡▼ <

extend join project union

```
DeviceFileEvents

        ▼ FileName, SHA256
```

extend

join

project union

```
) on SHA256

        ▼ Timestamp, FileName, SHA256, DeviceName, Deviceld, extend join
```

project union

```
NetworkMessageld, SenderFromAddress, RecipientEmailAddress
```

Answer:

Explanation:

Answer Area

```
Ema i1 At t achmentInfo

| where SenderFromAddress =~ "MaliciousSender8example.com"

| where isnotempty (SHA256)
```

1 ¡▼ <

extend join project union

```
DeviceFileEvents

        ▼ FileName, SHA256
```

extend join project union

```
) on SHA256

        ▼ Timestamp, FileName, SHA256, DeviceName, Deviceld, extend join
```

project union

```
NetworkMessageld, SenderFromAddress, RecipientEmailAddress
```

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide

Question: 42

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

```
DeviceProcessEvents
I where Timestamp > ago (24h)
and InitiatingProcessFileName =- 'runsI132.exe'
and InitiatingProcessCommandLine !contains " " and initiatingProcessCommandLine !
and FileName in- ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore' and
ProcessCommandLine has 'disable'
I 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. Block DeviceProcessEvents with DeviceNetworkEvents.

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

Answer: AE

Explanation:

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/custom-

detection- rules

Question: 43

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. Add 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: ACD

Explanation:

https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

Question: 44

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:

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 45

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: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 46

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: B

Explanation:

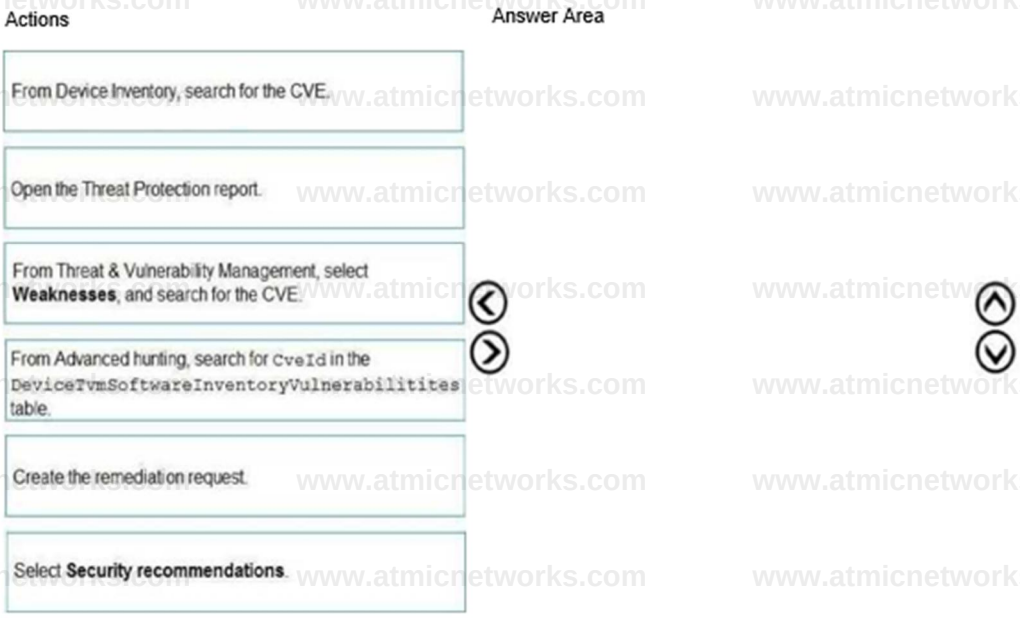
Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 48

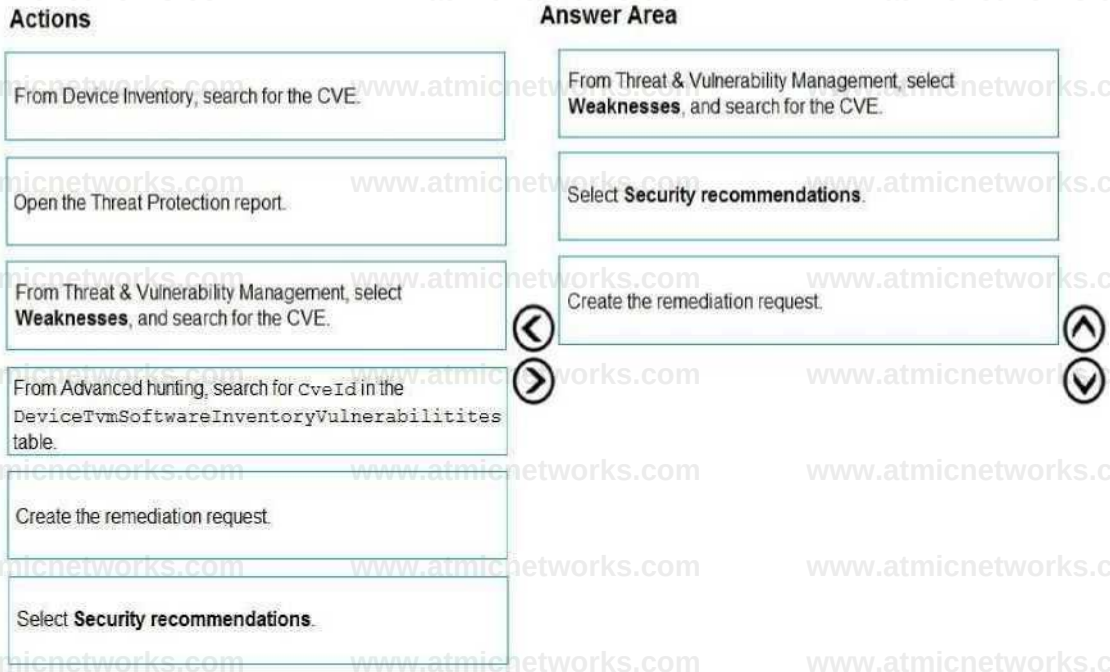
DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.Which three 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.



Answer:

Explanation:



Reference:

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

Question: 49

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 use Azure Security Center.You receive a security alert in Security Center.You need to view recommendations to resolve the alert in Security Center.Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding- alerts

Question: 50

You receive an alert from Azure Defender for Key Vault.You discover that the alert is generated from multiple suspicious IP addresses.You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue.The solution must be implemented as soon as possible and must minimize the impact on legitimate users.What should you do first?

A. Modify the access control settings for the key vault.

B. Enable the Key Vault firewall.

C. Create an application security group.

D. Modify the access policy for the key vault.

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

Question: 51

HOTSPOT

You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.
View the window
You need to test LA1 in Security Center.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or tnggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from

Recommendations
Workflow automation

Answer:

Explanation:

Answer Area

Set the LA1 trigger to

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from

Recommendations
Workflow automation

Reference:

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app- and-define-when-it-should-automatically-run

Question: 52

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:

Question: 53

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: AD

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate- alerts-on-your- azure-vms-linux-

Question: 54

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

A. In workspace1, install a solution.

B. In sub1, register a provider.

C. From Security Center, create a Workflow automation.

D. In workspace1, create a workbook.

Answer: A

Explanation:

Reference:

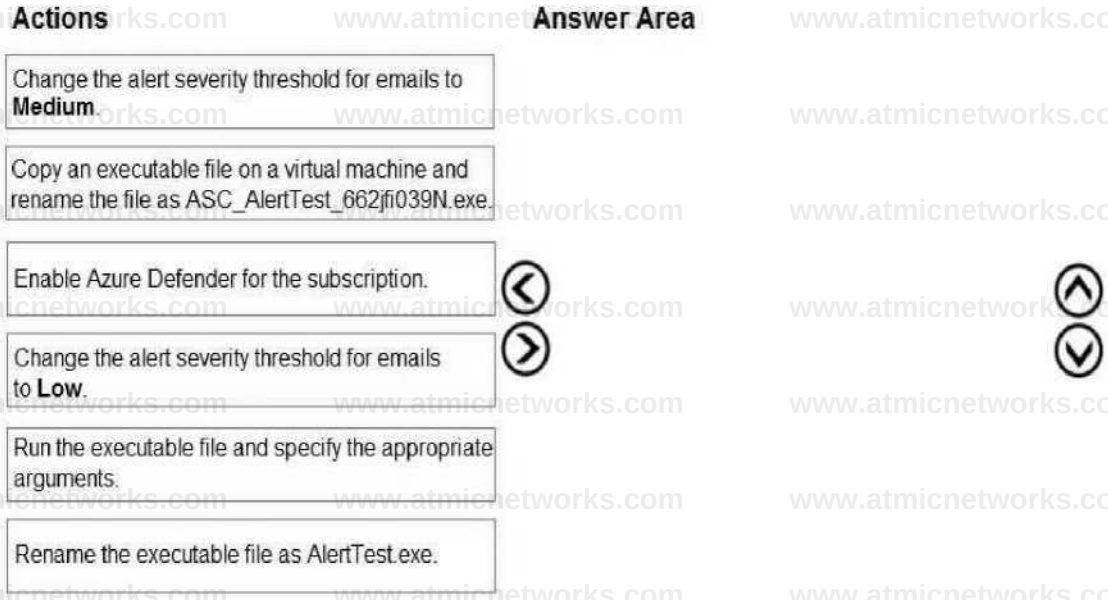
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Question: 55

DRAG DROP

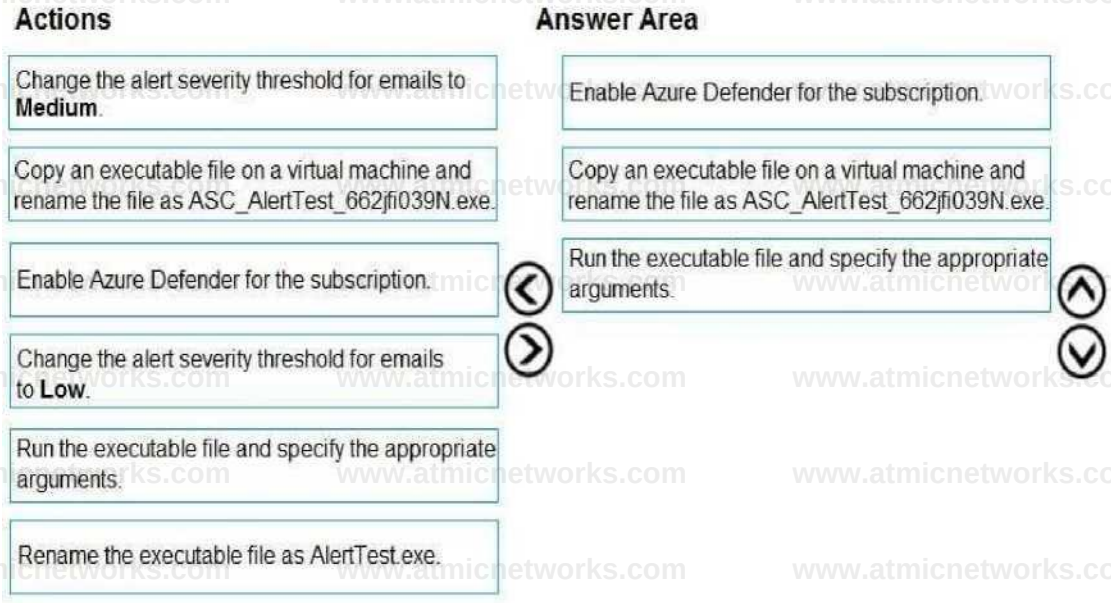
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

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.



Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

Question: 56

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

A. Security solutions

B. Security policy

C. Pricing & settings

D. Security alerts

E. Azure Defender

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact- details

Question: 57

DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Enable Security Health Analytics

From Azure Security Center, add cloud connectors

Configure the GCP Security Command Center

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API

Answer Area

Answer:

Explanation:

Configure the GCP Security Command Center

Enable Security Health Analytics,

Enable the GCP Security Command Center API

Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

Question: 58

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding- alerts

Question: 59

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding- alerts

Question: 60

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart. What should you include in the query?

A. extend

B. bin

C. makeset

D. workspace

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

Question: 61

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: AB

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Question: 62

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).

What should you use?

A. notebooks in Azure Sentinel

B. Microsoft Cloud App Security

C. Azure Monitor

D. hunting queries in Azure Sentinel

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/notebooks

Question: 63

You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.

You need to create a query that will be used to display a bar graph. What should you include in the query?

A. extend

B. bin

C. count

D. workspace

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

Question: 64

You use Azure Sentinel.

You need to receive an immediate alert 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: BC

Explanation:

B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.

C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

Question: 65

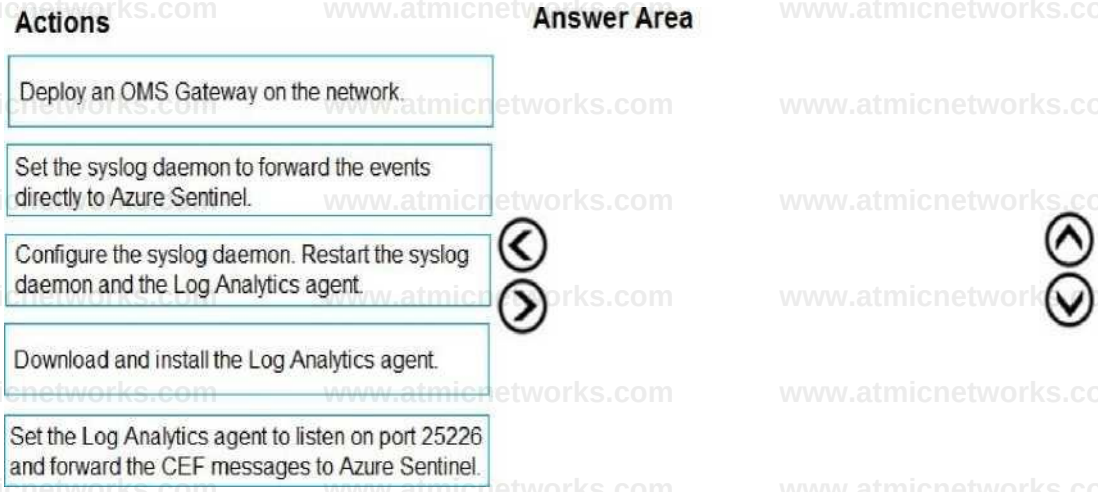
DRAG DROP

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure

Sentinel.

You need to deploy the log forwarder.

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



Answer:

Explanation:

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

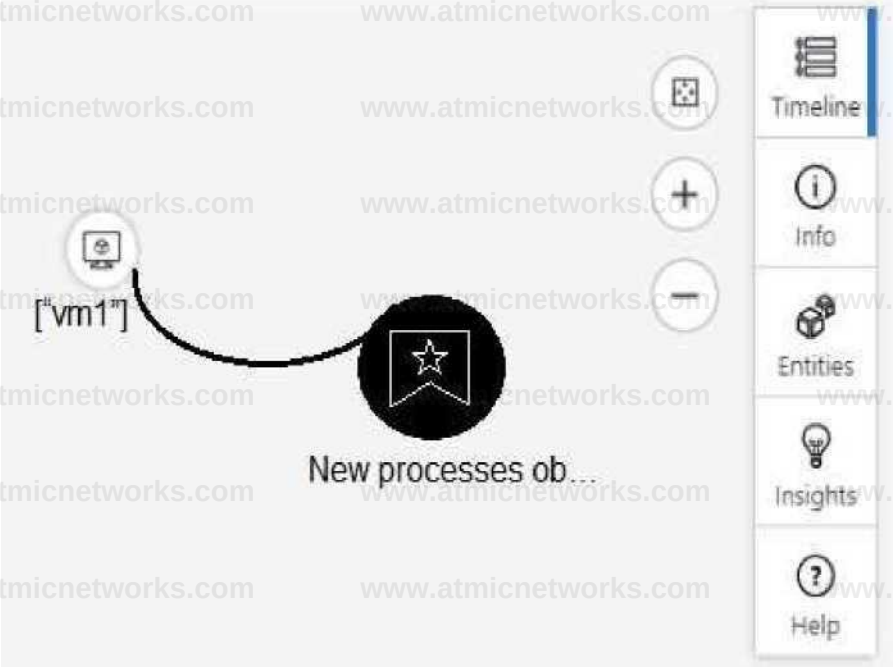
Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

Question: 66

HOTSPOT

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

If you hover over the virtual machine named vm1, you can view [answer choice].

the inbound network security group (NSG) rules
the last five Windows security log events
the open ports on the host
the running processes

Answer:

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation- graph-to-deep-dive

If you select [answer choice], you can navigate to the bookmarks related to the incident.

Entities
Info
Insights
Timeline

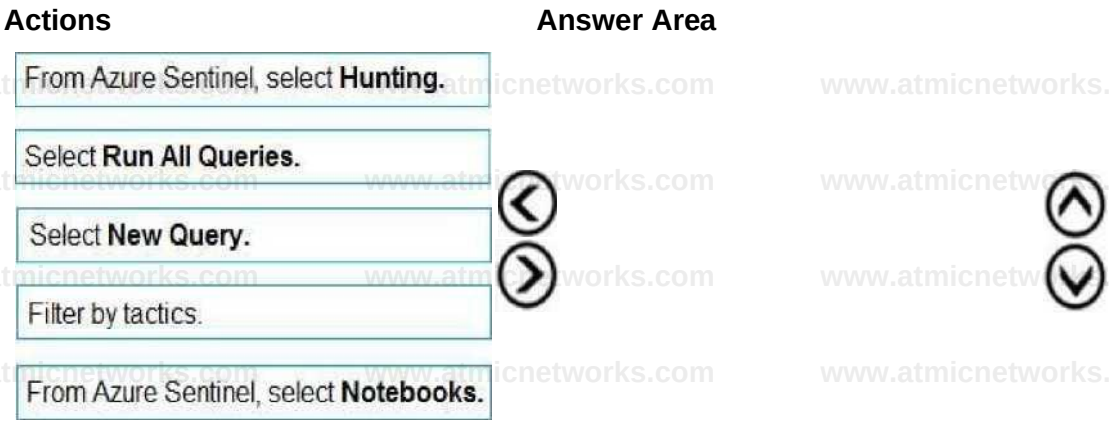
Question: 67

DRAG DROP

You have an Azure Sentinel deployment.

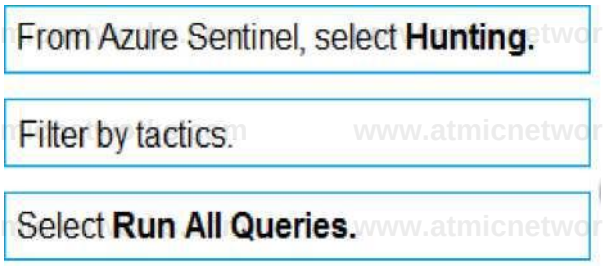
You need to query for all suspicious credential access activities.

Which three 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.



Answer:

Explanation:



Question: 68

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:

https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Question: 69

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

A. built-in queries

B. livestream

C. notebooks

D. bookmarks

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/notebooks

Question: 70

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.What should you do?

A. Add a parameter and modify the trigger.

B. Add a custom data connector and modify the trigger.

C. Add a condition and modify the action.

D. Add a parameter and modify the action.

Answer: D

Explanation:

Reference:

https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email- automatically/

Question: 71

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 = Id;
SecurityEvent
I where TimeGenerated >= ago(timeframe)
I where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
I summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
Eventcount = count() by
Computer, Account, EventID, Activity
I 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:

Question: 72

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.You deploy Azure Sentinel to a new Azure subscription.You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.Which two actions should you perform? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.

A. Add the Security Events connector to the Azure Sentinel workspace.

B. Create a query that uses the workspace expression and the union operator.

C. Use the alias statement.

D. Create a query that uses the resource expression and the alias operator.

E. Add the Azure Sentinel solution to each workspace.

Answer: BE

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Question: 73

You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

A. Playbooks

B. Analytics

C. Threat intelligence

D. Incidents

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a- playbook-on-demand

Question: 74

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:

Reference:

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

Question: 75

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

A. Azure Sentinel Responder

B. Logic App Contributor

C. Azure Sentinel Contributor

D. Azure Sentinel Reader

Answer: A

Explanation:

Reference:

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

Question: 76

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: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

Question: 77

HOTSPOT

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 signins performed by the recipients within an hour of receiving the known malicious email.

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

NOTE: Each correct selection is worth one point.

```
let MaliciousEmails = [ ▼ ]
                      EmailAttachementInfo
                      EmailEvents
                      IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);
MaliciousEmails
| join ( [ ▼ ]
         EmailAttachementInfo
         EmailEvents
         IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [ ▼ ]
  select 20
  take 20
  top 20
```

Answer:

Explanation:

let MaliciousEmails = ^

EmailAttachementInfo
EmailEvents
IdentityLogonEvents

I where MalwareFilterVerdict == "Malware"

| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName = tostring(split (RecipientEmailAddress, ”@") [0]);

MaliciousEmails

I join (_

EmailAttachementInfo
EmailEvents
IdentityLogonEvents

I project LogonTime = Timestamp, AccountName, DeviceName) on AccountName

| where (LogonTime - TimeEmail) between (Omin.. 60min)

| [▼]

select 20
take 20
top 20

Reference:

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

Question: 78

You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

A. a URL/domain indicator that has Action set to Alert only

B. a URL/domain indicator that has Action set to Alert and block

C. a file hash indicator that has Action set to Alert and block

D. a certificate indicator that has Action set to Alert and block

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

Question: 79

Your company deploys the following services:
Microsoft Defender for Identity
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
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: BD

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365- worldwide

Question: 80

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.

You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.

How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
EmailAttachmentlnfo | where SenderFromAddress =~
''MaliciousSender@example.com" where isnotempty I—
```

(DeviceId) (RecipientEmailAddress) (SenderFromAddress) (SHA256)

```
I join ( DeviceFileEvents
I project FileName, SHA256 ) on ▼
```

(DeviceId) (RecipientEmailAddress) (SenderFromAddress) (SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Answer:

Explanation:

```
EmailAttachmentlnfo
 I where SenderFromAddress =~ "MaliciousSender@example.com" where
isnotempty
                                                    _
```

(DeviceId) (RecipientEmailAddress) (SenderFromAddress) (SHA256)

```
I join (
DeviceFileEvents
| project FileName, SHA256
* 015
                                    ▼
```

(DeviceId) ~
(RecipientEmailAddress)

(SenderFromAddress) (SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Reference:

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

Question: 81

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?

A. Azure Cosmos DB

B. Azure Event Grid

C. Azure Event Hubs

D. Azure Data Lake

Answer: C

Explanation:

Reference: https://docsmicrosoftcom/en-us/azure/security-center/continuous-export?tabs=azure- portal

Question: 82

You are responsible for responding to Azure Defender for Key Vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.

What should you configure to mitigate the threat?

A. Key Vault firewalls and virtual networks

B. Azure Active Directory (Azure AD) permissions

C. role-based access control (RBAC) for the key vault

D. the access policy settings of the key vault

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

Question: 83

HOTSPOT

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
"resources"; [
    "type": ”                              yr /automations",
                Microsoft Automation
                Microsoft Logic
                Microsoft Security
     "apiversion": "2019-01-01-preview", "name": "[parameters('name')]", "location": "[parameters('location'
    ) ]", "properties": {
        "description": "[format(variables{'description'), '(0}', parameters ('subscriptionld')) ]",
        "isEnabled": true, "actions": [
            {
                "actionType": "LogicApp",
                "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters ('appName')) ]", "uri":
"[listCallbackURL(resourceId(parameters('subscriptionld'),
parameters('resourceGroupName'), '                              ▼ /workflows/triggers',
                                    Microsoft Automation Microsoft Logic Microsoft Security
 parameters('appName'), 'manual'), '2019-05-01').value]" }
        1,
```

Answer:

Explanation:

```
"resources": [

    "type": "                                    y /automations",
                Microsoft Automation
                Microsoft Logic
                Microsoft Security
    "apiversion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters!'location')]",
    "properties": {
        "description": "[format(variables('description'), '{0}', parameters ('subscriptionld'))]",
        "isEnabled": true,
        "actions": [

            "actionType": "LogicApp",
            "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters ('appName'))]",
            "uri": "[listCallbackURL(resourceId(parameters <'subscriptionld'),
parameters('resourceGroupName'), '                                    v /workflows/triggers',
                                    Microsoft Automation
                                    Microsoft Logic
                                    Microsoft Security
  parameters('appName'), 'manual'), '2019-05-01').value]" }
```

Reference:

https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

Question: 84

You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

A. at the subscription level

B. at the workspace level

C. at the resource level

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

Question: 85

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 appthat has a manual trigger
C. Create an Azure logic app that has an Azure Security Center alert trigger.
D. Create an Azure logic appthat has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

Answer: AC

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

Question: 86

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:

Reference:

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

Question: 88

A company uses Azure Sentinel.
You need to create an automated threat response.
What should you use?

A. a data connector

B. a playbook

C. a workbook

D. a Microsoft incident creation rule

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Question: 89

HOTSPOT

You use Azure Sentinel to monitor irregular Azure activity.
You create custom analytics rules to detect threats as shown in the following exhibit.

Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard - Edit existing rule

DeployVM

General Set rule logic Incident settings Automated response Review and create

Define the logic for your new analytics rule.

Rule query

Anytime Details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where Ope rat io nN ante —— "Create or Update Virtual Machine" or OperationName —
— "Create Deployment"
| where Activitystatus — "Succeeded"
| make-series dcount(ResourceId) default—I
on EventSubmissionTimestamp in range(ago(7d), now(). Id) by Caller
```

View query results >

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis Entity type must be a string

Entity Type Column

Account	Choose column v	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add
FileHash	Choose column	Add

Query scheduling

Run query every •

5 Minutes

Lookup data from the last • ©

["5 Hours

Alert threshold

Generate alert when number of query results

| Is greater than v [2

Event grouping

Configure how rule query results are grouped into alerts

(•) Group all events into a single alert

O Trigger an alert for each event

Suppression

Stop running query after alert is generated Q

: On Off

Stop running query for

5 Hours

Previous Next: Incident settings >

You do NOT define any incident settings as part of the rule definition.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If a user deploys three Azure virtual machines simultaneously, how many times will you receive [answer choice] in the next five hours.

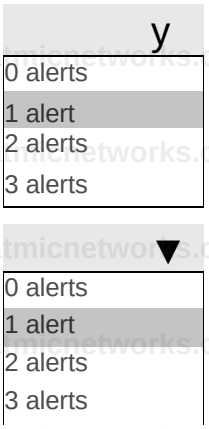
If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive [answer choice].

Answer:

Explanation:
Reference:

If a user deploys three Azure virtual machines simultaneously, how many times will you receive [answer choice] in the next five hours.

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive [answer choice].



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

Question: 90

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.

B. Modify the workspace settings of the existing Azure Sentinel deployment

C. Add Microsoft Sentinel to a workspace.

D. Create a data connector in Azure Sentinel.

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Question: 91

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: AD

Explanation:

Question: 92

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 Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a scheduled query rule for a data connector.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Question: 93

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 Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a hunting bookmark.
Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Question: 94

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 Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a Microsoft incident creation rule for a data connector.
Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Question: 95

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: DE

Explanation:

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp

https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

Question: 96

HOTSPOT

You purchase a Microsoft 365 subscription.

You plan to configure Microsoft Cloud App Security.

You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.

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

NOTE: Each correct selection is worth one point.

Policy template type:

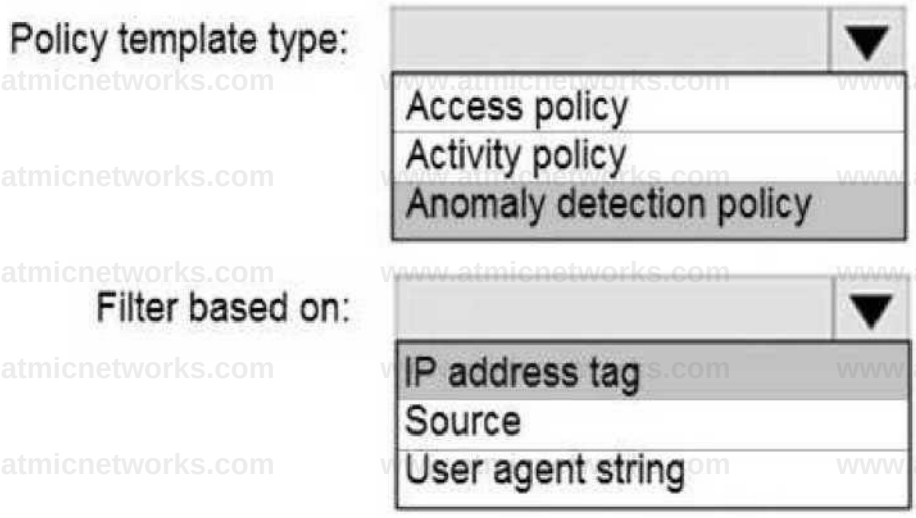
Access policy
Activity policy
Anomaly detection policy

Filter based on:

IP address tag
Source
User agent string

Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Question: 97

You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
What should you do?

A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.

B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.

C. From Regulatory compliance, download the report.

D. From Recommendations, download the CSV report.

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding- alerts

Question: 98

You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.

You are troubleshooting an issue on the virtual machines.

In Security Center, you need to view the alerts generated by the virtual machines during the last five days.

What should you do?

A. Change the rule expiration date of the suppression rule.

B. Change the state of the suppression rule to Disabled.

C. Modify the filter for the Security alerts page.

D. View the Windows event logs on the virtual machines.

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

Question: 99

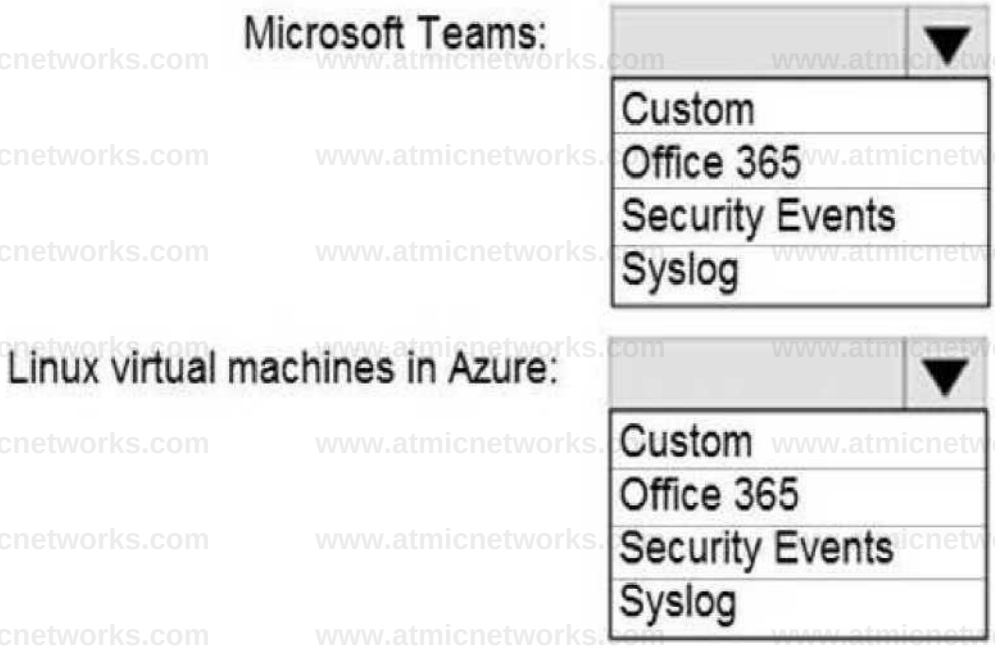
HOTSPOT

You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

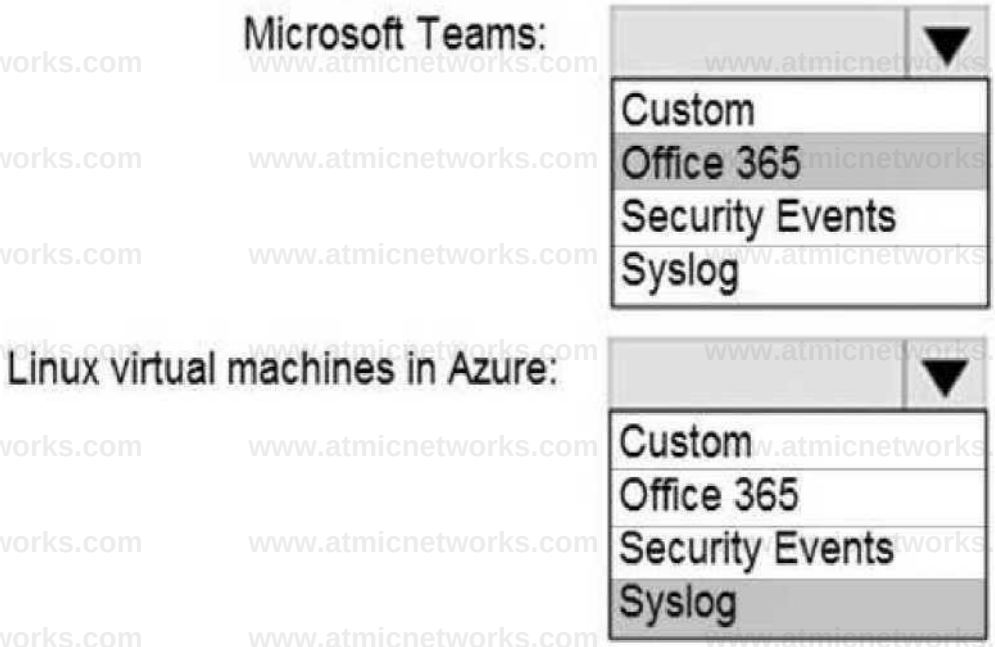
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365

https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

Question: 100

You are investigating an incident in Azure Sentinel that contains more than 127 alerts.
You discover eight alerts in the incident that require further investigation.
You need to escalate the alerts to another Azure Sentinel administrator.
What should you do to provide the alerts to the administrator?

A. Create a Microsoft incident creation rule

B. Share the incident URL

C. Create a scheduled query rule

D. Assign the incident

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

Question: 101

You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign in 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: AB

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

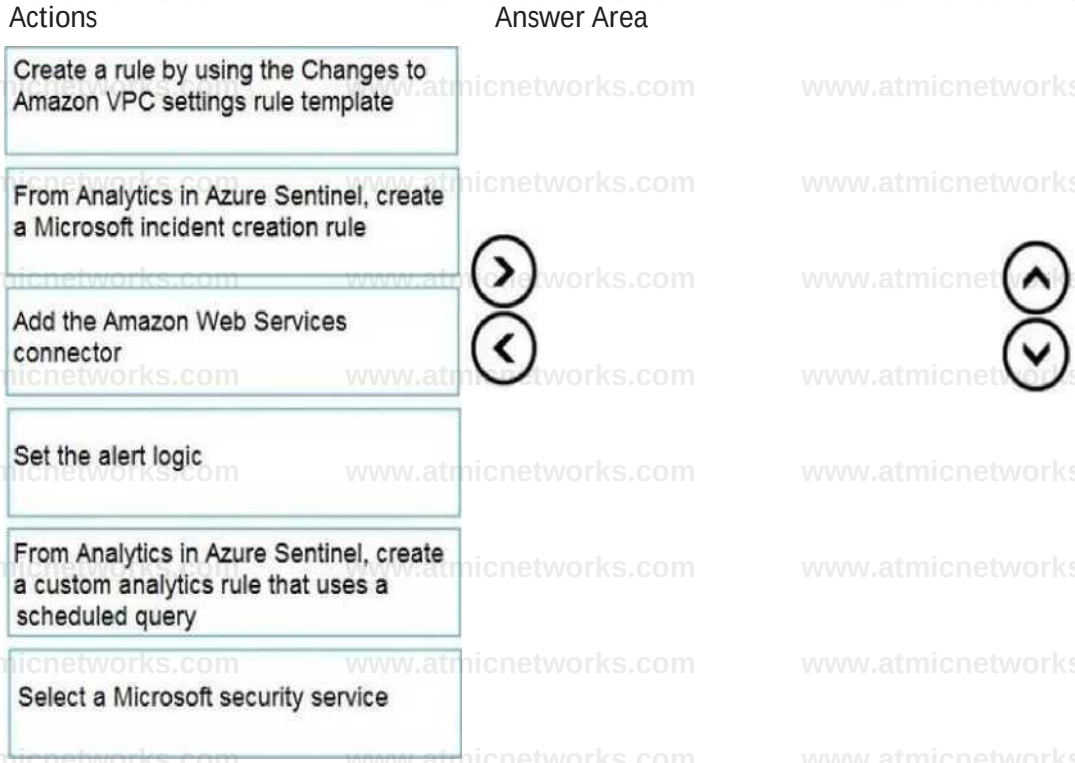
Question: 102

DRAG DROP

You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

Which three 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.

a Microsoft 365 E5



Answer:

Explanation:

Add the Amazon Web Services connector

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Set the alert logic

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

Question: 103

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: AD

Explanation:

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection

https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

Question: 104

Your company has a single office in Istanbul and a Microsoft 365 subscription.
The company plans to use conditional access policies to enforce multi-factor authentication (MFA).
You need to enforce MFA for all users who work remotely.
What should you include in the solution?

A. a fraud alert

B. a user risk policy

C. a named location

D. a sign-in user policy

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Question: 105

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.

You receive many alerts related to impossible travel and sign-ins from risky IP addresses.
You determine that 99% of the alerts are legitimate sign-ins from your corporate offices.

You need to prevent alerts for legitimate sign-ins from known locations.
Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Override automatic data enrichment.

B. Add the IP addresses to the corporate address range category.

C. Increase the sensitivity level of the impossible travel anomaly detection policy.

D. Add the IP addresses to the other address range category and add a tag.

E. Create an activity policy that has an exclusion for the IP addresses.

Answer: AD

Explanation:

Question: 106

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:

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Question: 107

HOTSPOT

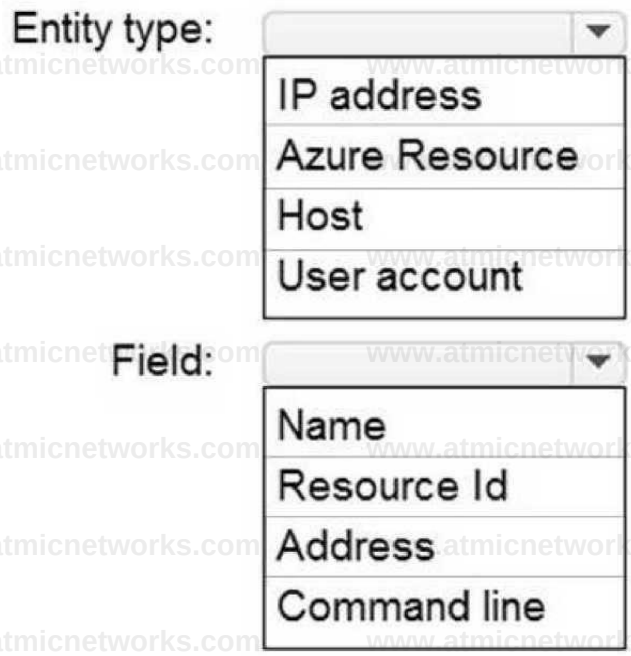
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the

development of an application.

You need to hide Azure Defender alerts for the storage account.

Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Explanation:

Answer:

Entity type:

IP address Azure Resource Host

User account

Field: _____

Name

Resource Id Address

Command line

Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure- security-center-alerts-are-now/ba-p/1404920

Question: 108

You create an Azure subscription.

You enable Azure Defender for the subscription.

You need to use Azure Defender to protect on-premises computers.

What should you do on the on-premises computers?

A. Install the Log Analytics agent.

B. Install the Dependency agent.

C. Configure the Hybrid Runbook Worker role.

D. Install the Connected Machine agent.

Answer: A

Explanation:

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

Data is collected using:

The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.

Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Question: 109

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.

The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.

You need to ensure that the security administrator receives email alerts for all the activities.

What should you configure in the Security Center settings?

A. the severity level of email notifications

B. a cloud connector

C. the Azure Defender plans

D. the integration settings for Threat detection

Answer: A

Explanation:

Reference:

https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-

incidents-from-microsoft-365/ba-p/2012518

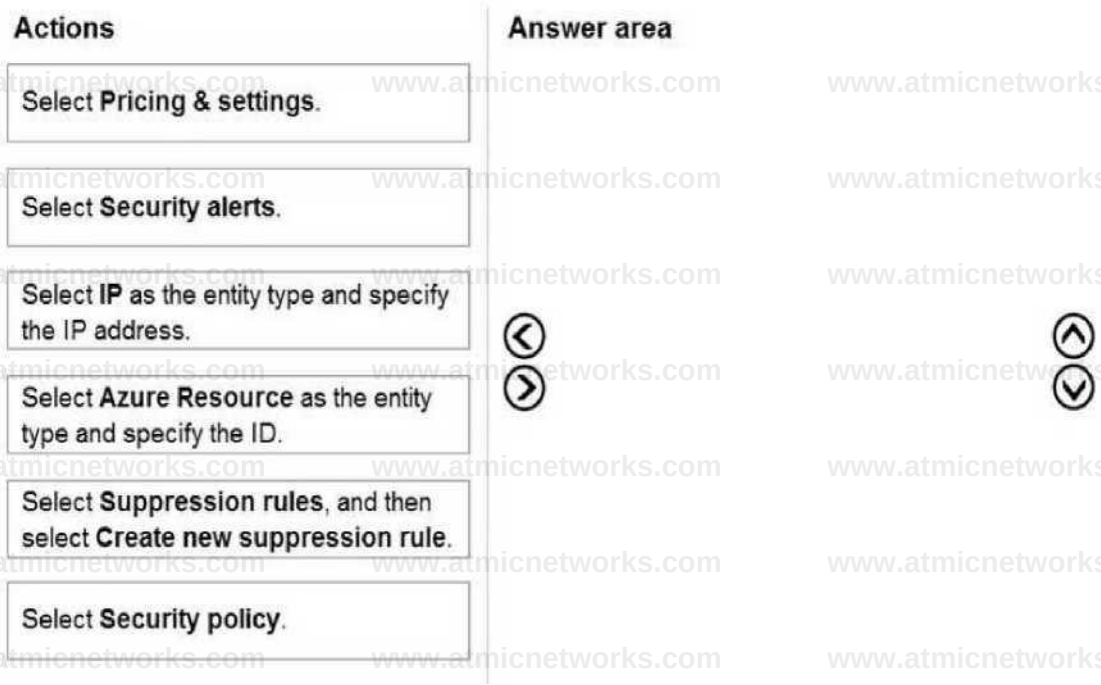
Question: 110

DRAG DROP

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Select Security policy

Select Suppression rules, and then select Create new suppression rule

Select Azure Resource as the entity type and specify the ID

Question: 111

DRAG DROP

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

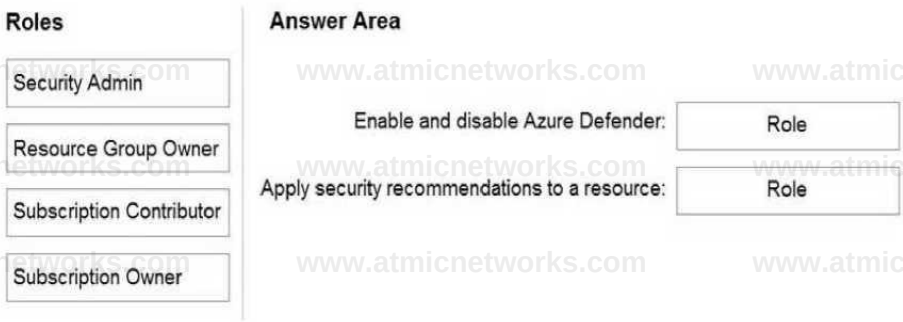
Enable and disable Azure Defender.

Apply security recommendations to resource.

The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. 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.



Explanation:

Enable and disable Azure Defender Security Admin

Apply security recommendations to a resource: Subscription Contributor

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

Question: 112

You use Azure Sentinel.

You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

A. Azure Sentinel Contributor

B. Security Administrator

C. Azure Sentinel Responder

D. Logic App Contributor

Answer: C

Explanation:

Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources.

Reference:

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

Question: 113

You create a hunting query in Azure Sentinel.

You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.

What should you use?

A. a playbook
B. a notebook
C. a livestream
D. a bookmark

Answer: C

Explanation:

Question: 114

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, B

Explanation:

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, you should perform the following two actions:

Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.

Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules

Question: 115

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.

What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

A. the Threat Protection Status report in Microsoft Defender for Office 365

B. the mailbox audit log in Exchange

C. the Safe Attachments file types report in Microsoft Defender for Office 365

D. the mail flow report in Exchange

Answer: A

Explanation:

To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

Question: 116

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:

Microsoft Excel macros that download scripts from untrusted websites

Users that open executable attachments in Microsoft Outlook

Outlook rules and forms exploits

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:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack- surface-reduction?view=o365-worldwide

Question: 117

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-events 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:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

Question: 118

HOTSPOT

You have an Azure subscription that uses Azure Defender.

You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

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

NOTE: Each correct selection is worth one point.

Set available effects to

Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use.

An Azure Automation runbook that has a webhook
An Azure Logi c Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Answer:

Explanation:

Set available effects to:

Append
DeployIfNotExists EnforceRegoPolicy

To perform remediation use

An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

Question: 119

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender.

Azure Defender has automatic provisioning enabled.

You need to create a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1.

What should you do first?

A. From Azure Security Center, add a workflow automation.

B. On VM1, run the Get-MPThreatCatalog cmdlet.

C. On VM1 trigger a PowerShell alert.

D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage- alerts?view=o365-worldwide

Question: 120

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 have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

Question: 121

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 have Linux virtual machines on Amazon Web Services (AWS).
You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You manually install the Log Analytics agent on the virtual machines.

Does this meet the goal? 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 Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a livestream from a query.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Question: 123

A. Yes

B. No

Answer: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

Question: 122

Note: This question is part of a series of questions that present the same scenario. Each question in the series

HOTSPOT

You need to create a query for a workbook. The query must meet the following requirements:
List all incidents by incident number.
Only include the most recent log for each incident.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
Securityincident
| project sort                    (LasModifiedTime,*) by IncidentNumber
| summarize
```

Answer:

Explanation:

```
Securityincident
| [project / sort / summarize] [arg_max / limit / top](LasModifiedTime,*) by IncidentNumber
```

Reference:

https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/

Question: 125

DRAG DROP

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

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.

Roles

- Contributor
- Owner
- Security administrator
- Security reader

Answer Area

User1: ;

User2: ;

Answer:

Explanation:
Box 1: Owner

Only the Owner can assign initiatives.

Box 2: Contributor

Only the Contributor or the Owner can apply security recommendations.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

Question: 126

HOTSPOT

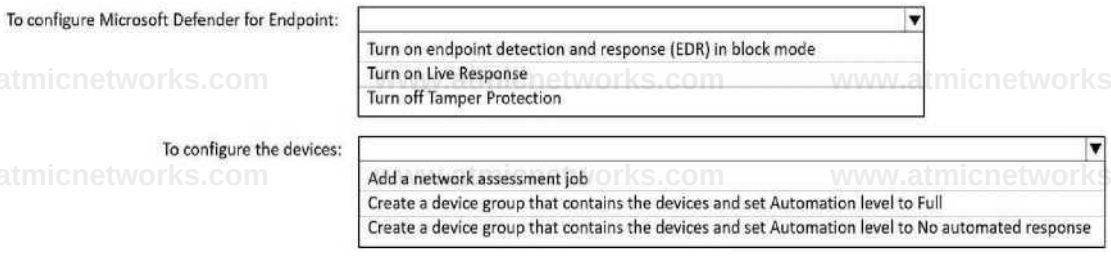
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

Box 1: Turn on Live Response

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.

Box: 2 : Add a network assessment job

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldwide

Question: 128

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

You delete users from the subscription.

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

What should you use?

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

Answer: C

Explanation:

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.

Default alert policies include:

Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Question: 129

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days.
What should you use?

A. the Incidents blade of the Microsoft 365 Defender portal
B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
C. Activity explorer in the Microsoft 365 compliance center
D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Answer: C

Explanation:

Labeling activities are available in Activity explorer.

For example:

Sensitivity label applied

This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.

It is captured at the time of save in Office native applications and web applications.

It is captured at the time of occurrence in Azure Information protection add-ins.

Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide

Question: 130

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

You need to identify all the entities affected by an incident.

Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations
B. Devices
C. Evidence and Response
D. Alerts

Answer: C

Explanation:

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents

Question: 131

You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

A. the Dependency agent
B. the Log Analytics agent
C. the Azure Connected Machine agent
D. the Guest Configuration extension

Answer: B

Explanation:

Defender for Cloud depends on the Log Analytics agent.

Use the Log Analytics agent if you need to:

* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage

Question: 134

You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.

You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.

What should you use to create the visuals?

A. plotly

B. TensorFlow

C. msticpy

D. matplotlib

Answer: C

Explanation:

msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.

MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:

Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.

Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX.

Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.

Visualization tools using event timelines, process trees, and geo mapping.

Advanced analyses, such as time series decomposition, anomaly detection, and clustering.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started

https://msticpy.readthedocs.io/en/latest/

Question: 135

HOTSPOT

You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.

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

NOTE: Each correct selection is worth one point.

```
AzureActivity
BehaviorAnalytics SecuntyEvent
| where OperationNameValue == "Microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue -* “Succeeded”
| join kind® inner (
        AsureAstivity
        | where OperationNameValue -- "Microsoft.storage/storageaccounts/listkeys/action”
        | where ActivityStatusValue == "Succeeded"
        | project ExpectedIpAddress-CallerIpAddress, Caller
| evaluate                                                    ’
```

```
                    autoclusterQ
                    binQ countQ
    ) on Caller
| where CallerIpAddress ! = ExpectedIpAddress
```

```
| summarise Resoureelds = make_set(ResoureeId), ResoureeldCount • deount(Res6ureeId)
        by OperationNaneValue> Caller, CallerlpAddress
```

Answer:

Explanation:

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.

The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.'

```
AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
    AzureActivity
```

```
    | where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
    | where ActivityStatusValue == "Succeeded"
    | project ExpectedIpAddress=CallerIpAddress, Caller
    | evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
```

Reference: https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_Of_Storage_Keys.yaml

Question: 136

DRAG DROP

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.

You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

The modification of local group memberships

The purging of event logs

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

Actions

From the details pane of the incident, select **Investigate.**

From the Investigation blade, select the entity that represents **VM1.**

From the Investigation blade, select the entity that represents **powershell .ex*.**

From the Investigation blade, select **Timeline**

From the investigation blade, select **Info**

From the Investigation blade, select **Insights**

Answer Area

Answer:

Explanation:

Step 1: From the Investigation blade, select Insights

The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.

Step 2: From the Investigation blade, select the entity that represents VM1.

The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights.

Incident Insights

The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights

The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

IP Address

Account

Host

URL

Step 3: From the details pane of the incident, select Investigate.

Choose a single incident and click View full details or Investigate.

Reference:

https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview

https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

Question: 137

You have a Microsoft Sentinel workspace that contains the following incident.

Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident.

What should you do?

A. From Overview, review the Potential malicious events map.

B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.

C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.

D. From Investigation, review insights on the incident entity.

Answer: A

Explanation:

Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

Question: 138

You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

A. Create an Azure Policy assignment.

B. Modify the Workload protections settings in Defender for Cloud.

C. Create an alert rule in Azure Monitor.

D. Modify the alert settings in Defender for Cloud.

Answer: D

Explanation:

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud.

Note: To create a rule directly in the Azure portal:

1. From Defender for Cloud's security alerts page:

Select the specific alert you don't want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

2. In the new suppression rule pane, enter the details of your new rule.

Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.

Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.

3. Enter details of the rule.
4. Save the rule.

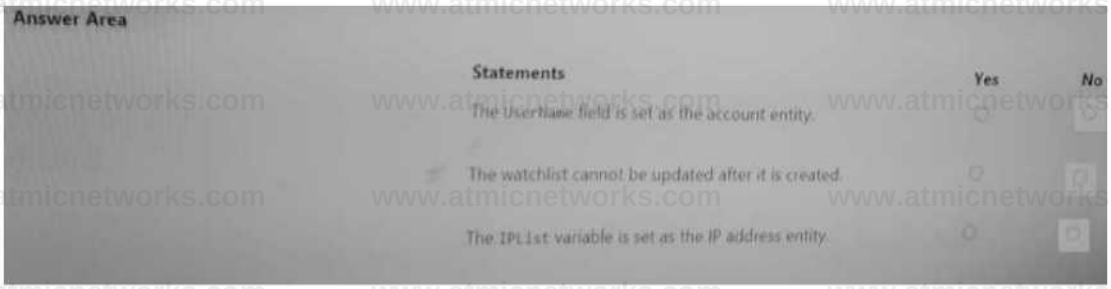
Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules

Question: 139

HOTSPOT

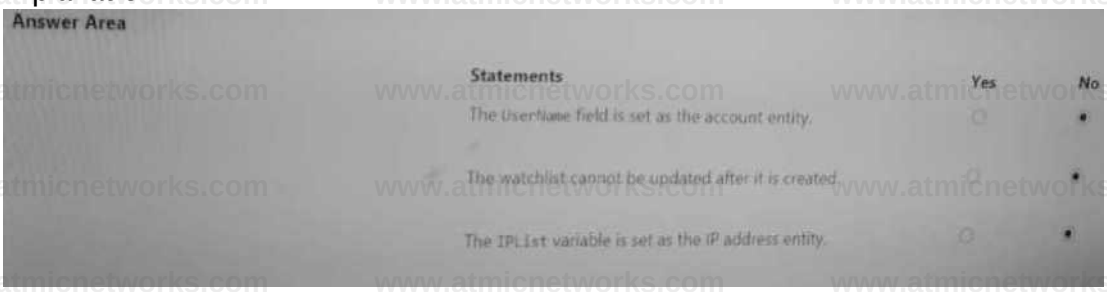
You have the following SQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
   | where Source == "Microsoft-Windows-Sysmon"
   | where EventID == 3
   | extend EvData = parse_xml(EventData)
   | extend EventDetail = EvData.DataItem.EventData.Data
   | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
   | where SourceIP in (IPList) or DestinationIP in (IPList)
   | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
   | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```



Answer

Explanation:



Question: 140

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.

You need to identify all the changes made to Domain Admins group during the past 30 days.

What should you use?

A. the Azure Active Directory Provisioning Analysis workbook
B. the Overview settings of Insider risk management
C. the Modifications of sensitive groups report in Microsoft Defender for Identity
D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Answer: C

Explanation:

Question: 141

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:

Question: 142

You have a Microsoft Sentinel workspace.

You receive multiple alerts for failed sign in attempts to an account.

You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.

- Ensure that failed sign-in alerts are generated for other accounts.
- Minimize administrative effort

What should do?

A. Create an automation rule.
B. Create a watchlist.
C. Modify the analytics rule.
D. Add an activity template to the entity behavior.

Answer: A

Explanation:

An automation rule will allow you to specify which alerts should be suppressed, ensuring that failed sign-in alerts are generated for other accounts while minimizing administrative effort. To create an automation rule, navigate to the Automation Rules page in the Microsoft Sentinel workspace and configure the rule parameters to suppress the false positive alerts.

Question: 143

You have a custom Microsoft Sentinel workbook named Workbooks.

You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.

What should you do?

A. In the query editor interface, configure Settings.

B. In the query editor interface, select Advanced Editor

C. In the grid query, include the project operator.

D. In the grid query, include the take operator.

Answer: B

Explanation:

Question: 144

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1. You need to configure just in time (JIT) VM access for the virtual machines in RG1. The solution must meet the following

- Limit the maximum request time to two hours.
- Limit protocol access to Remote Desktop Protocol (RDP) only.
- Minimize administrative effort.

What should you use?

A. Azure AD Privileged Identity Management (PIM)

B. Azure Policy

C. Azure Front Door

D. Azure Bastion

Answer: A

Explanation:

Question: 145

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:

Question: 146

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

You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.

What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

A. endpoint detection and response (EDR) in block mode

B. custom network indicators

C. web content filtering

D. Live response for servers

Answer: A

Explanation:

Question: 147

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.

You need to identify which blobs were deleted.

What should you review?

A. the Azure Storage Analytics logs

B. the activity logs of storage1

C. the alert details

D. the related entities of the alert

Answer: B

Explanation:

Question: 148

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:

Question: 149

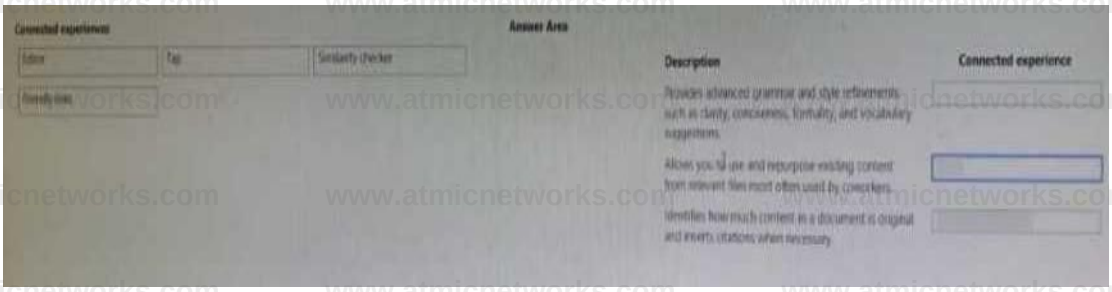
DRAG DROP

A company wants to analyze by using Microsoft 365 Apps.

You need to describe the connected experiences the company can use.

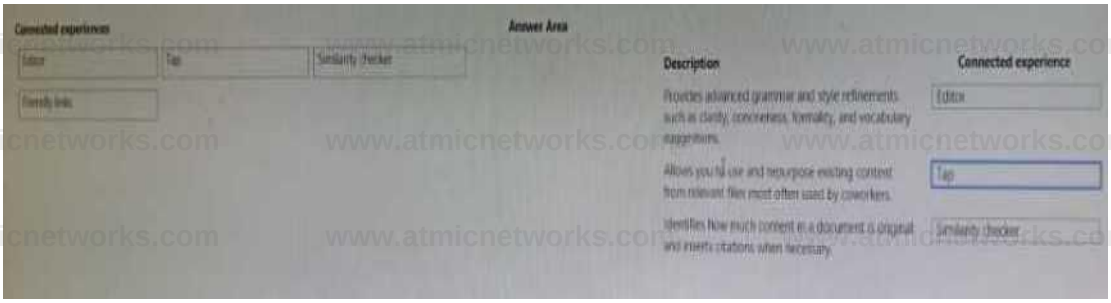
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 150

HOTSPOT

You have the following KQL query.

```
let IPlht • JSetNatchHst(*taMP#")j fvent
    I where Source ■• "Microsoft-Windows-Syswon" where EventIO ■■ 3
    | extend EvData • parsejtal(EventData)
      extend EventDetail • EvData.Dataltea.EventData.Data
    I extend Source!? • Event Detail. [?].{'M ext* J, Destination!? * EventDetall.(14].("next"]
    | where Source!? in (IPList) or Destination!? in (mist)
    | extend IPHatch • c«e( Source!? in (I?list), "Source!?", Destination!? In (mist), "Destination!?", "Hone") extend timestamp • TineGenerated, AccountCustonEntlty ■
      userHaoe, HostCuitoaiEntlty ■ Computer, *
```

Statements	Yes	No
The usemw field is set as the account entity.		
The watchlist cannot be updated after it is created		
The PList vanable is set as the IP address entity		

Answer: Answer:

Explanation:

Statements	Yes	No
The u$erMa« field is set as the account entity.	♦	O
The watchlist cannot be updated after it is created	•	
The jPUat vanable is set as the IP address entity	O	#

Question: 151

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

You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

A. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.

B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.

C. Select Add indicator and set the IP address to 171.23.34.32/27

D. Create an import file that contains the individual IP addresses in the range. Select Import and import the file.

Answer: D

Explanation:

This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.

Reference: [1] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft- defender-atp/threat-intelligence-manage-indicators

Question: 152

Your company has an on-premises network that uses Microsoft Defender for Identity.

The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.

You need remediate the security risk.

What should you do?

A. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.

B. Modify the properties of the computer objects listed as exposed entities.

C. Disable legacy protocols on the computers listed as exposed entities.

D. Enforce LDAP signing on the computers listed as exposed entities.

Answer: B

Explanation:

To remediate the security risk associated with unsecure Kerberos delegation, you should modify the properties of the computer objects listed as exposed entities. Specifically, you should set the

Kerberos delegation settings to either 'Trust this computer for delegation to any service' or 'Trust this computer for delegation to specified services only'. This will ensure that the computer is not allowed to use Kerberos delegation to access other computers on the network.

Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/microsoft- defender-for-identity/configure-kerberos-delegation

Question: 154

HOTSPOT

You have an Azure subscription that contains an Microsoft Sentinel workspace.

AudrtLogs
AmrcActiyity
AzureDiagnostics

("Microsoft .Netb*ork/net»<ork$securltyGroups/securltyRules/write")

"Succeeded"

You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:

• Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal

| nake-series dcount(ResourceId) defaulted on Event5ub«issionTi«estanp in range(ago(7d)# HON()# Id) by Caller

| extend tine st amp • todetetiae(Event$ubaissionTiiiiestanp[0]) ˅ AccountCustoaEntity ■ Caller

| extend
| parse-where
| where

Answer:

Explanation:

Answer:

Question: 155

You have an Azure subscription that uses Microsoft Sentinel.

You detect a new threat by using a hunting query.

You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.

What should you do?

A. Create a playbook.
B. Create a watchlist.
C. Create an analytics rule.
D. Add the query to a workbook.

Explanation:

Answer: A

By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once and it will run on a schedule, alerting you when

the threat is detected. Reference: https://docs.microsoft.com/en-us/azure/sentinel/analytics-create- rule

Question: 156

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in

storage1. You need to identify which blobs were deleted. What should you review?

A. the activity logs of storage1
B. the Azure Storage Analytics logs
C. the alert details
D. the related entities of the alert

Answer: A

Explanation:

To identify which blobs were deleted, you should review the activity logs of the storage account. The activity logs contain information about all the operations that have taken place in the storage account, including delete operations. These logs can be accessed in the Azure portal by navigating to the storage account, selecting "Activity log" under the "Monitoring" section, and filtering by the appropriate time range. You can also use Azure Monitor and Log Analytics to query and analyze the activity logs data.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-activity-logs

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-azure-storage

Question: 157

DRAG DROP

You have a Microsoft Sentinel workspace that contains an Azure AD data connector.

You need to associate a bookmark with an Azure AD-related incident.

What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade 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.

Blades

Hunting blade

Incident blade

Logs blade

Answer Area

Create a bookmark by using the: Blade

Associate a bookmark with the incident by using the: Blade

Answer:

Explanation:

You can use the Logs blade or incident blade to create a bookmark of an Azure AD-related incident. Once the bookmark is created, you can associate it with the incident by using the incident blade. This allows you to quickly and easily access important information related to the incident in the future.

Question: 158

DRAG DROP

You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort. Which three 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

Answer Area

Configure the Suppress similar alerts settings.

Configure the Mitigate the threat settings.

[Filter by alert title.

Select Take action

Configure the Prevent future attacks settings.

Configure the Trigger automated response settings.

Answer

Explanation:

A. Configure the Trigger automated response settings in the Azure Security Center or Azure Logic App,

B. Filter by alert title (e.g. "Suspicious process executed").

C. Select "Take action" (e.g. "Mitigate the threat").

Question: 159

You have a Microsoft Sentinel workspace.

You have a query named Query1 as shown in the following exhibit.

0 HrwOwyt* • +

~' 'ecdbKt p O«iei @ Q v

range Set tn query Q

where Hartenereted > egofrti)
where operation |t^ltM>» 'delete*
project TineGenerrted, userid, Operation, oHicewortloed, RecordType, Resource: tort by TiwCenereted devc null* lest

You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?

A. Remove line 2.

B. In line 4. remove the TimeGenerated predicate.

C. Remove line 5.

D. In line 3, replace the 'contains operator with the !has operator.

Answer: A

Explanation:

This can be confirmed by referring to the official Microsoft documentation on creating custom log queries in Azure Sentinel, which states that the “has” operator should not be used in the query, and that it is unnecessary. Reference: https://docs.microsoft.com/en-us/azure/sentinel/query-custom- logs

Question: 160

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

A. Modify the properties of the connector.

B. Create a Data Collection Rule (DCR).

C. Create a scheduled query rule.

D. Enable User and Entity Behavior Analytics (UEBA)

Answer: D

Explanation:

Question: 161

DRAG DROP

You have 50 on-premises servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.

You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:

- Provide threat and vulnerability management.

- Support data collection rules.

Which three 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.

From the Data controller settings in the Azure portal, create an Azure Arc data controller

On the on-premises servers, install the Azure Monitor agent.

From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.

On the on premises servers, install the Azure Connected Machine agent

On the on-premises servers, install the Log Analytics agent

Answer:

Explanation:

To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:

On the on-premises servers, install the Azure Connected Machine agent.

On the on-premises servers, install the Log Analytics agent.

From the Data controller settings in the Azure portal, create an Azure Arc data controller.

Once these steps are completed, the on-premises servers will be able to communicate with the

Azure Defender for Cloud deployment and will be able to support threat and vulnerability management as well as data collection rules. Reference: https://docs.microsoft.com/en- us/azure/security-center/deploy-azure-security-center#on-premises-deployment

Question: 162

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.
You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort
Which blade should you use in the Microsoft 365 Defender portal?

A. Advanced hunting

B. Threat analytics

C. Incidents & alerts

D. Learning hub

Answer: B

Explanation:

To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help you identify risks and prioritize threats in your environment. Reference: https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defender- threat-analytics

Question: 163

You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use m the Microsoft 365 Defender portal?

A. From Threat tracker, review the queries.

B. From the History tab in the Action center, revert the actions.

C. From the investigation page, review the AIR processes.

D. From Quarantine from the Review page, modify the rules.

Answer: B

Explanation:

Question: 164

You have a Microsoft Sentinel workspace named Workspaces

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

What should you create in Workspace1?

A. a workbook

B. a hunting query

C. a watchlist

D. an analytic rule

Answer: D

Explanation:

To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace. An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used. Reference: https://docs.microsoft.com/en- us/azure/sentinel/analytics-create-analytic-rule

Question: 165

Your company uses Microsoft Sentinel

A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.

You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

A. Microsoft Sentinel Responder

B. Logic App Contributor

C. Microsoft Sentinel Reader

D. Microsoft Sentinel Contributor

Answer: A

Explanation:

The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac

Question: 166

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a custom report that will visualise sign-in information over time.

What should you create first?

A. a workbook

B. a hunting query

C. a notebook

D. a playbook

Answer: A

Explanation:

A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription. Reference: https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview

Question: 168

You create an Azure subscription.
You enable Microsoft Defender for Cloud for the subscription.
You need to use Defender for Cloud to protect on-premises computers.
What should you do on the on-premises computers?

A. Configure the Hybrid Runbook Worker role.
B. Install the Connected Machine agent.
C. Install the Log Analytics agent
D. Install the Dependency agent.

Answer: C

Explanation:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

.

Question: 170

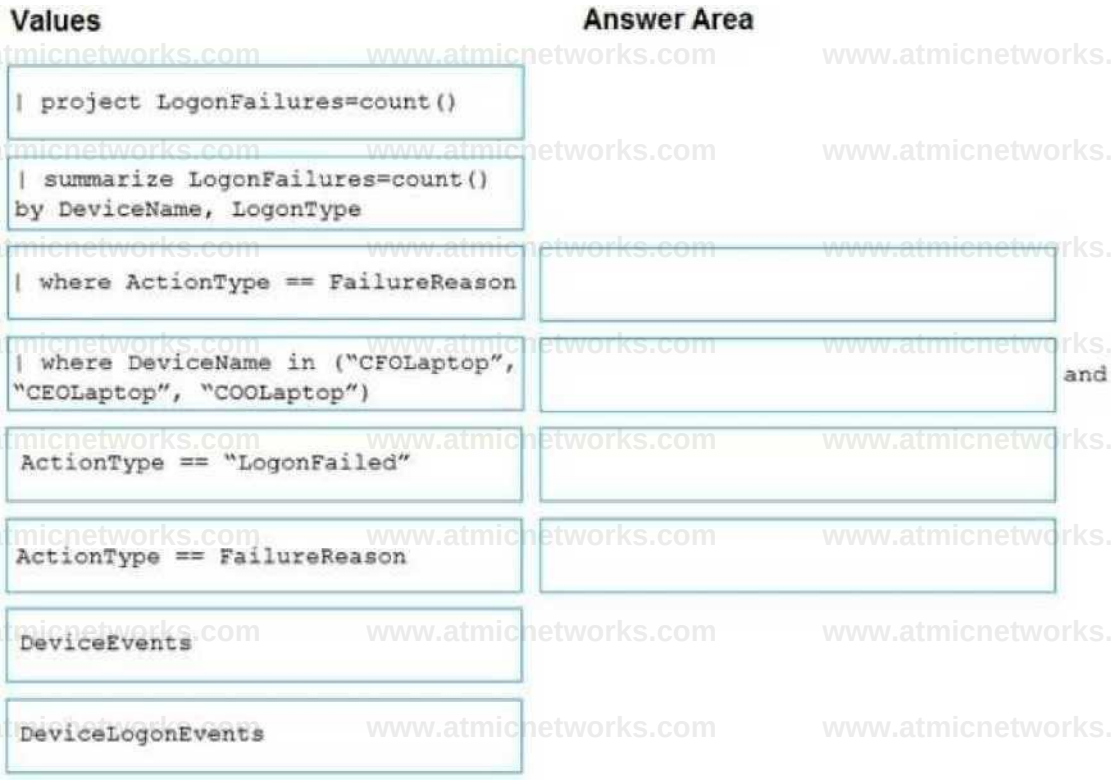
DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count 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



Answer:

Explanation:

```
DeviceLogonEvents
| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop") and
ActionType == FailureReason
| summarize LogonFailures=count() by DeviceName, LogonType
```

Question: 172

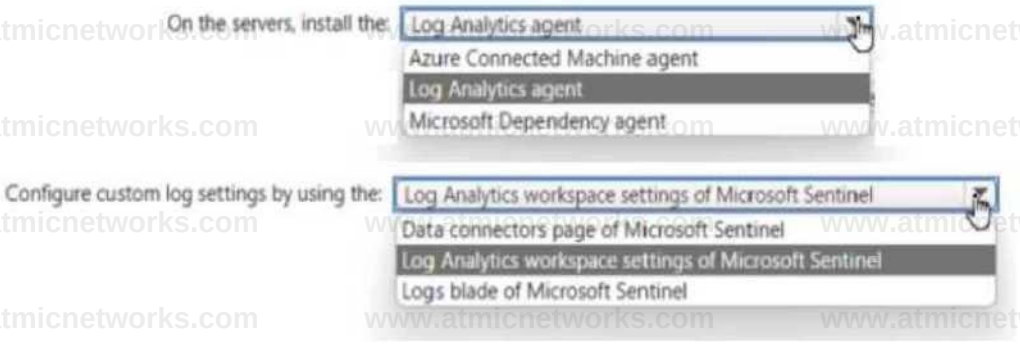
HOTSPOT

Your on-premises network contains 100 servers that run Windows Server.

You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel.

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



Answer:

Explanation:

On the servers, install the log Analytics agent *

Configure custom log settings by using the log Analytics workspace settings of Microsoft Sentinel

To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log Analytics agent on each of the 100 servers. The Log Analytics agent is a lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

Question: 175

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:

Question: 176

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:

Question: 178

You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure AD connector. You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert. What should you create first?

A. a repository connection

B. awatchlist

C. an analytics rule

D. an automation rule

Answer: D

Explanation:

Question: 179

You have an Azure subscription that contains a user named User1.

User1 is assigned an Azure Active Directory Premium Plan 2 license

You need to identify whether the identity of User1 was compromised during the last 90 days.

What should you use?

A. the risk detections report

B. the risky users report

C. Identity Secure Score recommendation s

D. the risky sign-ins report

Answer: B

Question: 180

You have an Azure subscription that uses Microsoft Defender fof Ctoud.

You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.

You need to onboard EC2-1 to Defender for Cloud.

What should you install on EC2-1?

A. the Log Analytics agent

B. the Azure Connected Machine agent

C. the unified Microsoft Defender for Endpoint solution package

D. Microsoft Monitoring Agent

Answer: A

Explanation:

Question: 181

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schem

a. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

A. Copy the parsers to the Azure Monitor Logs page.
B. Create a JSON file based on the DNS template.
C. Create an XML file based on the DNS template.
D. Create a YAML file based on the DNS template.

Answer: A

Explanation:

Question: 182

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: D, E

Explanation:

Question: 183

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 alert status

C. the certainty of the source computer

D. the resolution method of the source computer

Answer: B

Explanation:

Question: 185

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 (1AM) role for Defender for Cloud.

C. Configure AWS Security Hub.

D. Deploy the AWS Systems Manager (SSM) agent

Answer: D

Explanation:

Question: 187

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 Area

Answer:

Explanation:

Answer Area

Groups Contnbutor

Question: 188

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 AnarytKS

B. AzureDalabricks

C. Azure Machine Learning

D. LogAnalytics

Answer: D

Explanation:

Question: 189

You need to correlate data from the SecurityEvent Log Anarytks table to meet the Microsoft Sentinel requirements for using UEB

A. Which Log Analytics table should you use?

A. SentwlAuoNt

B. AADRiskyUsers

C. IdentityOirectoryEvents

D. Identityinfo

Answer: C

Explanation:

Question: 190

You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

A. Analytics Efficiency

B. Security Operations Efficiency

C. Event Analyzer

D. Investigation insights

Answer: C

Explanation:

Question: 191

You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

A. an API connection

B. a trigger

C. an connector

D. authorization

Answer: B

Explanation:

Question: 192

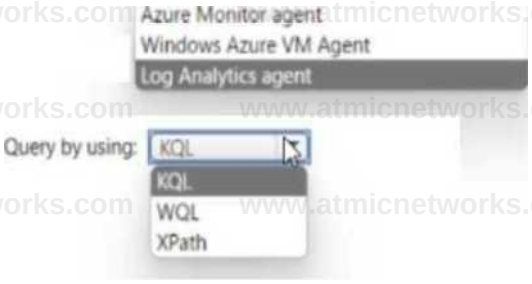
HOTSPOT

You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer are

a. NOTE Each correct selection is worth one point.

Answer Area

Deploy the [Log Analytics agent



Answer:

Explanation:

Answer Area

Deploy the Log Analytics agent

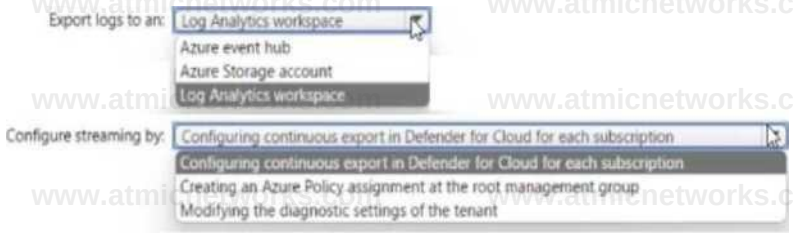
Query by using:

Question: 193

HOTSPOT

You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud togs to a syslog server. The solution must minimize administrative effort What should you do? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point

Answer Area



Answer:

Explanation:

Answer Area

Export logs to art Log Analytics workspace

Configure streaming by Configuring continuous export in Defender for Cloud for each subscriptions

Question: 195

You have an Azure subscription that uses resource type for Cloud. You need to filter the security alerts view to show the following alerts:

- Unusual user accessed a key vault
- Log on from an unusual location

D. High

Answer: C

Explanation:

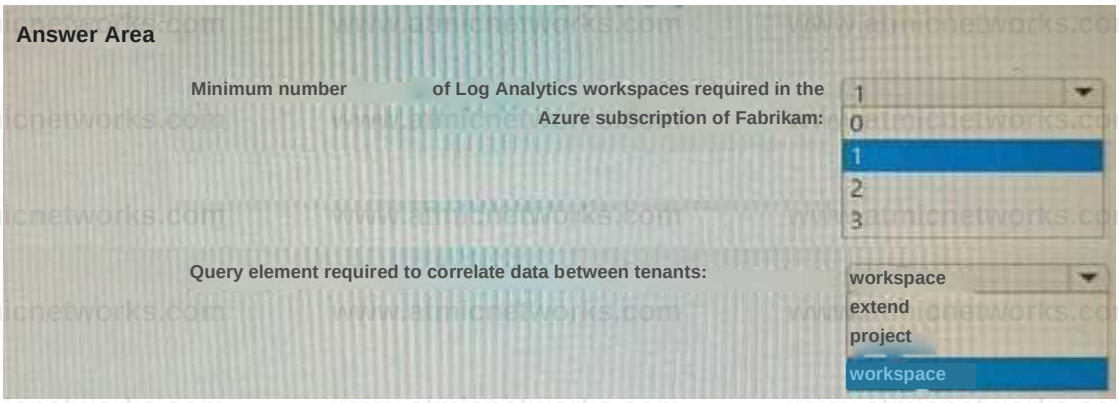
Question: 196

HOTSPOT

You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical requirements.

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area

Minimum number of Log Analytics workspaces required in i the Azure subscription of Fabrikam:

Query element required to correlate data between tenants: workspace

Question: 197

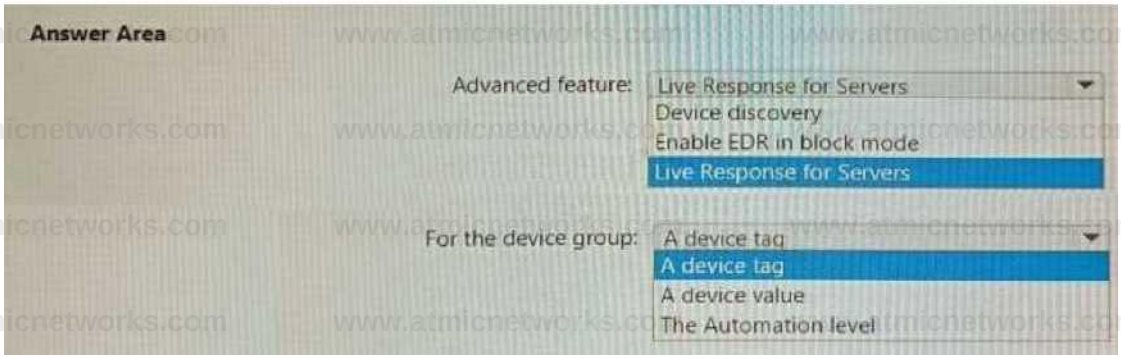
HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.

You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.

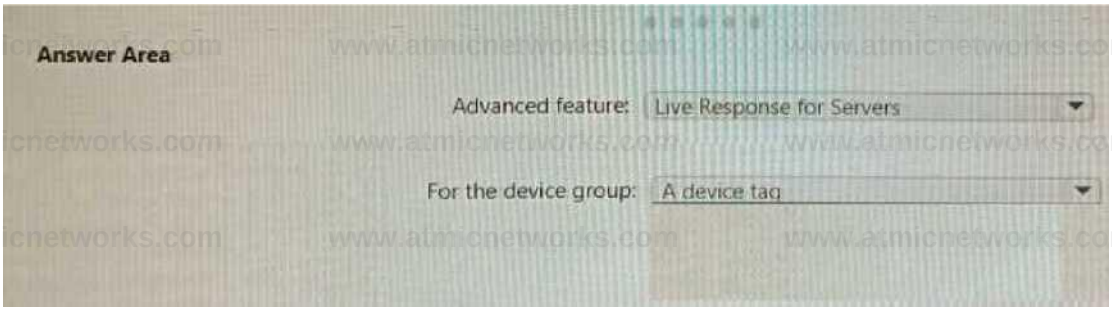
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 198

You have an Azure subscription that contains an Microsoft Sentinel workspace.

You need to create a playbook that will run automatically in response to an Microsoft Sentinel alert.

What should you create first?

A. a trigger in Azure Functions

B. an Azure logic app

C. a hunting query in Microsoft Sentinel

D. an automation rule in Microsoft Sentinel

Answer: D

Explanation:

Question: 199

You have a Microsoft Sentinel workspace.

You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:

- App name: App1
- IP address: 192.168.1.2
- Computer name: Device1
- Used client app: Microsoft Edge
- Email address: user1@company.com
- Sign-in URL: https://www.company.com

Which entities can be investigated by using UEBA?

A. app name, computer name, IP address, email address, and used client app only
B. IP address and email address only
C. used client app and app name only
D. IP address only

Answer: D

Explanation:

Question: 200

You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.

You need to identify the impacted entities in an aggregated alert.

What should you review in the DIP alert management dashboard of the Microsoft Purview compliance portal?

A. the Details tab of the alert
B. Management log

C. the Sensitive Info Types tab of the alert

D. the Events tab of the alert

Answer: D

Explanation:

Question: 201

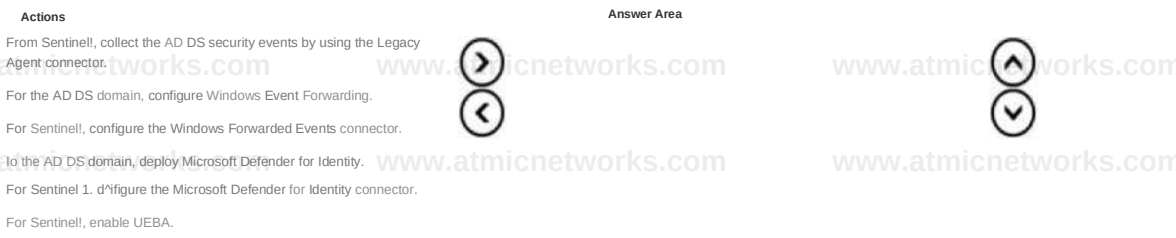
DRAG DROP

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft Sentinel workspace named Sentinel1.

You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel1 and collect security events from the AD DS domain.

Which three 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.



Answer:

Explanation:

Actions

From Sentinel! collect the AD DS security events by using the Legacy Agent connector.

For the AD DS domain, configure Windows Event Forwarding.

For Sentinel! configure the Windows Forwarded Events connector

Answer Area

1 I To the AD DS domain, deploy Microsoft Defender fix Identity.

2 For Sentinel! ^figure the Microsoft Defender for Identity connector.

3 | For Sentinel! enable UEBA.

Question: 202

DRAG DROP

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

- Enable and disable advanced features of Microsoft Defender for Cloud.
- Apply security recommendations to a resource.

The solution must use the principle of least privilege.

Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote 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.

Roles

Resource Group Owner

Security Admin

Subscription Contributor

Subscription Owner

Answer Area

Enable and disable advanced features of Microsoft Defender for Cloud:

Apply security recommendations to a resource:

Answer:

Explanation:

Roles

Security Admin

Subscription Contributor

Subscription Owner

Answer Area

Enable and disable advanced features of Microsoft Defender for Cloud. Security Admin

Apply security recommendations to a resource. Subscription Contributor

Question: 203

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

You have a GitHub account named Account1 that contains 10 repositories.

You need to ensure that Defender for Cloud can assess the repositories in Account1.

What should you do first in the Microsoft Defender for Cloud portal?

A. Add an environment.

B. Enable security policies.

C. Enable integrations.

D. Enable a plan.

Answer: A

Explanation:

Question: 204

You have an Azure subscription that uses Microsoft Defender for Servers Plan 1 and contains a server named Server1.

You enable agentless scanning.

You need to prevent Server1 from being scanned. The solution must minimize administrative effort.

What should you do?

A. Create an exclusion tag.

B. Upgrade the subscription to Defender for Servers Plan 2.

C. Create a governance rule.

D. Create an exclusion group.

Answer: D

Explanation:

Question: 205

HOTSPOT

You have a Microsoft Sentinel workspace named sws1.

You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

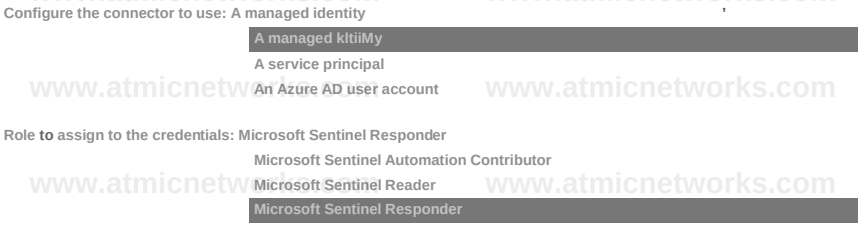
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:

- Minimize administrative effort.
- Use the principle of least privilege.

How should you configure the credentials? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

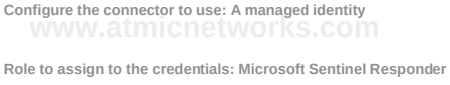
Answer Area



Answer:

Explanation:

Answer Area



Question: 207

HOTSPOT

You have an Azure subscription that contains a quest user named Userl and a Microsoft Sentinel workspace named workspacel.

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Azure role: Microsoft Sentinel Contributor
- Microsoft Sentinel Automation Contributor
- **Microsoft Sentinel Contributor**
- Microsoft Sentinel Respond

Azure AD role: Directory readers
- Attribute assignment reader
- **Directory readers**
- Global reader

Answer:

Explanation:

Answer Area

Azure role: Microsoft Sentinel Contributor

Azure AD role: Directory readers

Question: 208

HOTSPOT

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

```
Alertinfo
| where Severity — "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
I where EvidenteRcIe == "Impacted"
I summarize by Timestamp, AlertId, Ac countName, AccountobjectId, EntityType, DeviceId, SHA256
| join EorailEvents on Sleft.AccouotObjectXd « Sright.RecipientObjectId
| where OeliveryAction ** "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, ftecipientEmeilAddress, EntityType, DeviceId, SHA256
```

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the Sec ipienlEiMilMdress column.		
The custom detection rule can be used to restrict app execution automatically based on the DeviceW Column.		
The custom detection rule can be used to automate the deletion of a file based on the SKA25S column.		

Answer:

Explanation:

Answer Area

Statements	Yes	No

The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEiMilAddress column.	O	•
The custom detection rule can be used to restrict app execution automatically based on the DeviceId column.	0	9
The custom detection rule can be used to automate the deletion ot a file based on the SHAasa column.	O	*

Question: 209

HOTSPOT

You have a Microsoft Sentinel workspace.

You need to configure a report visual for a custom workbook. The solution must meet the following requirements:

- The count and usage trend of AppDisplayName must be included

* The TrendList column must be useable in a sparkline visual,

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

NOTE: Each correct selection is worth one point.

Signinlogs

| where ResultType == 0 and AppDisplayNam? 1= **

| summarize count!) by AppDisplayName

join

join

let

I lookup TrendList = count!) on TimeGenerated in range!(TimeRange:start}, {TimeRange:end}, 4h} by AppOisplayName

. mv-expand

) Of -^_1_^^-^^-*

I top 10 by count, desc

Signiniogs

I make-series ' TrendList = count() on TimeGenerated in range![TimeRange:start}, (TimeRange:end}, 4h) by AppOisplayHame make.bagO

¨nv-expand render

make-series

) on AppDisplayName

I top IO by count, desc

Answer:

Explanation:

Answer Area

signinLogs

| where ResultType == 0 and AppOisplayMame |= ""

I summarize count!) by AppDisplayName

I j^^ — <

SigninLogs

I make-series ' TrendList = count!) cm TimeGenerated in range!(TimeRange:start}, (TimeRange:end}, 4h) by AppDi splay Kame

) on AppDisplayHane

I top 10 by count, desc

Question: 210

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

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

You need to identify all the interactive authentication attempts by the users in the finance department of your company.

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

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

IdentityQueryEyents *

I where Depart ■ent = 'Finance'

I project-renoae objid = Accountobject Id.

I join Auditioqs * on Jleft.objid *■ Fright.AccountCbjectId

Question: 211

HOTSPOT

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

User1 shares a Microsoft Power Bi report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.

You need to identity which Power BI report file was shared.

How should you configure the search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Activities: shared Power BI report
Copied file
Downloaded files to computet
Share file, folder, or site
Shared Power BI report

Record type: Shared Power BI report
MicrosoftTeams
One Drive PowerBiAudit
Shared Power 81 report

Workload: MiciosoftTcams

Answer:

Explanation:

To identify which Power BI report file was shared by User1, you should configure the search with the following parameters:

Activities: Shared Power BI report

Record Type: PowerBiAudit

Workload: PowerBi

These parameters will filter the search results to show only the events where a Power BI report was shared by a user in your organization. You can then look for the event that has User1 as the user ID and an external user as the recipient. The event details will show the name and URL of the Power BI report file that was shared. For more information, see Search the audit log for events in Power BI and Search for content in the Microsoft Purview compliance portal.

Question: 212

DRAG DROP

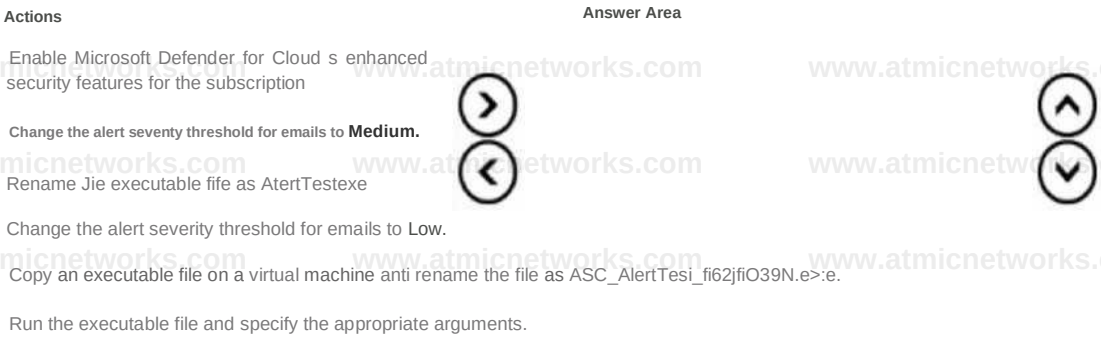
You create a new Azure subscription and start collecting logs for Azure Monitor.

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:

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, you should perform the following three actions in sequence:

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe

Run the executable file and specify the appropriate arguments

Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

These actions will simulate a malicious activity on the virtual machine and generate an alert in Defender for Cloud. You can then verify the alert details and response recommendations in the Azure portal. For more information, see Alert validation - Microsoft Defender for Cloud.

Question: 213

You haw the resources shown in the following Table.

Name	Type	Description	Location
Serveri	Server	hie server that runs Windows Server	On-premtses
Sener2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)

Server}	Virtual machine	Domain controller that runs	Azure
Server4	Server	Windows Server Domain controller that runs Wincows 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 5erver4 only

C. Server 1. Server2. arid Server4 only

D. Server 1, Servec2, Server3. and Seiver4

Answer: B

Explanation:

Question: 214

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 36S.

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.

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

NOTE: Each correct selection is worth one point.

Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union                                    (
    join kind=full outer
    join kind=inner
    union

    IdentityLogonEvents
    IdentityInfo
    IdentityLogonEvents
    IdentityQueryEvents

  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Answer:

Explanation:

Answer Area

DevieeLdfoetveots | extend Table * [1] table![1] | take lao

I union ~ (

Identitytogontwnts [T]

| extend Table * "table!" | take IN

I project*reorder TInestaap, Table, AceountOoaain, iccountKaiae, ActMntUpn, AcccuntSid | order by TImestaep esc

Question: 215

HOTSPOT

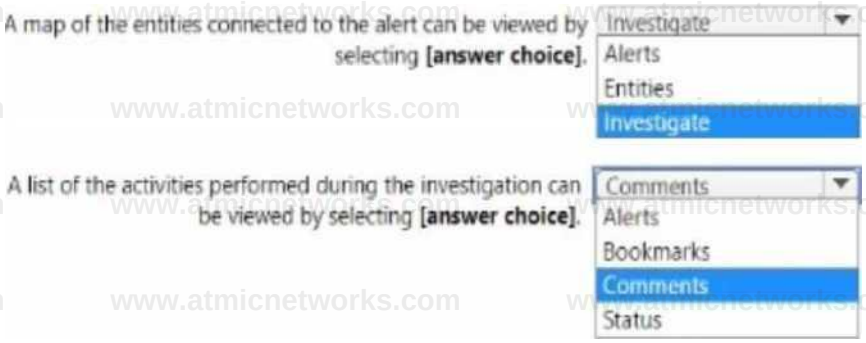
You have a Microsoft Sentinel workspace.

A Microsoft Sentinel incident is generated as shewn in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Areo



Answer:

Explanation:

Answer Area

A map of the entities connected to the alert can be wwd by selecting [answer choice]. lines tig ate

A kt of the activities performed dunng the investigation can be viewed by selecting [answer choice] Comments

Question: 216

HOTSPOT

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

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD The solution must use The principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area

Azure AD role security administrator ~ *]

Global administrator | Identity Governance Administrator j

Security administrator

Security operator

Azure role | Microsoft Sentinel Contributor

Microsoft Sentinel Automation Contributor

Microsoft Sentinel Contributor

Security Admin

Security Assessment Contributor

Answer:

Explanation:

Answer Area

Azure AD role Security administrator

Azure role Microsoft Sentinel Contributor

Question: 217

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

You have a virtual machine named Server! that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

A. the Microsoft Monitoring Agent

B. the Azure Arc agent

C. the Azure Monitor agent

D. the Azure Pipelines agent

Answer: C

Explanation:

Question: 218

You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.

You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the fallowing requirements:

- Minimize administrative effort
- Minimize the parsing required to read log data

What should you configure?

A. REST API integration

B. a SysJog connector

C. a Log Analytics Data Collector API

D. a Common Event Format (CEF) connector

Answer: B

Explanation:

Question: 219

HOTSPOT

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

You create a Google Cloud Platform (GCP) organization named GCP1.

You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded automatically.

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

NOTE: Each correct selection is worth one point.

Answer Arc*

&»» A ' -r - jenent project anc r < ustom role

A management group and an Azure AD service principal

A management project and a custom role

An Azure AD administrative unit and a managed identity

By. Running a scnpt in GCP Cloud Shell Deploying a Bicep template Running a script in Azuie Cloud Shell

Answer:

Explanation:

Answer Area

Create; A management project and a custom role ^

By Running a senpt in GCP Cloud Shell *

Question: 220

HOTSPOT

You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.

You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).

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

NOTE: Each correct selection is worth one point.

Answer Area

To the AO 05 domain control lets, deploy: I pieAzT^C jnriect^TTZTineTi^

- Microsoft Defender for Identity sensors
- The Azure Connected Machine agent
- The Azure Monitor urgent

For Sentinel!, configure (~ne Audit Logs data source

- The Audit Logs data source
- The Security Events data source
- The Signtn logs data source

Answer

Explanation:

Answer Area

To the AD DS domain controllers, deploy The Azure Connected Machine agent

For Sentinel!, configure he Audit Logs data source

Question: 221

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

You plan to create a hunting query from Microsoft Defender.

You need to create a custom tracked query that will be used to assess the threat status of the subscription.

From the Microsoft 365 Defender portal, which page should you use to create the query?

A. Policies & rules

B. Explorer

C. Threat analytics

D. Advanced Hunting

Answer: D

Explanation:

Question: 222

HOTSPOT

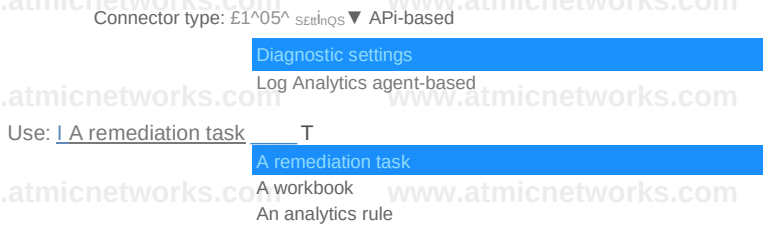
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.

You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.

Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

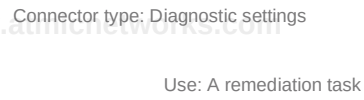
Answer Area



Answer:

Explanation:

Answer Area



Question: 223

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: B

Explanation:

Question: 224

HOTSPOT

You have an Microsoft Sentinel workspace named SW1.

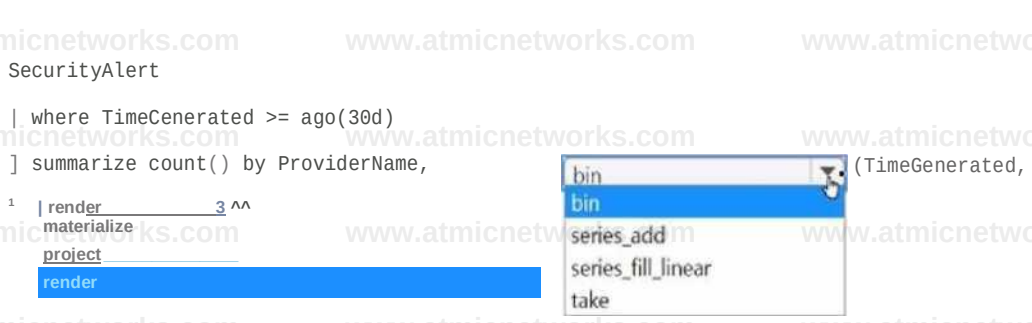
You plan to create a custom workbook that will include a time chart.

You need to create a query that will identify the number of security alerts per day for each provider.

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

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Question: 225

HOTSPOT

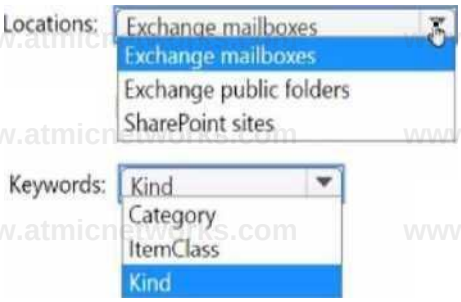
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.

How should you configure the content search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Locations: Exchange mailboxes

Keywords: Kind

Question: 226

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: B, C

Explanation:

Question: 227

You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

A. Run antivirus scan

B. Initiate Automated Investigation

C. Collect investigation package

D. Initiate Live Response Session

Answer: D

Explanation:

Question: 228

You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.

From Microsoft Sentinel, you investigate a Microsoft 365 incident.

You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.

What should you use?

A. the entity side panel of the Timeline card in Microsoft Sentinel

B. the investigation graph on the Incidents page of Microsoft Sentinel

C. the Timeline tab on the Incidents page of Microsoft Sentinel

D. the Alerts page in the Microsoft 365 Defender portal

Answer: A

Explanation:

Question: 229

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: D

Explanation:

Question: 230

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint

You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.

What should you use in the Microsoft 365 Defender portal?

A. Incidents

B. Investigations

C. Advanced hunting

D. Remediation

Answer: A

Explanation:

Question: 231

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint

You need to create a query that will link the AlertInfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.

Which operator should you use?

A. join kind = inner

B. evaluate hint. Remote =

C. search *

D. union kind = inner

Answer: A

Explanation:

Question: 232

You have a Microsoft Sentinel workspace that has user and Entity Behavior Analytics (UEBA) enabled for Sign in Logs.

You need to ensure that failed interactive sign-ins are detected.

The solution must minimize administrative effort.

What should you use?

A. a scheduled alert query

B. a UEBA activity template

C. the Activity Log data connector

D. a hunting query

Answer: B

Explanation:

Question: 233

You have a Microsoft 365 subscription that uses Microsoft Purview.

Your company has a project named Project1.

You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.

What should you do?

A. Create a records management disposition.

B. Perform a user data search.

C. Perform an audit search.

D. Perform a content search.

Answer: D

Explanation:

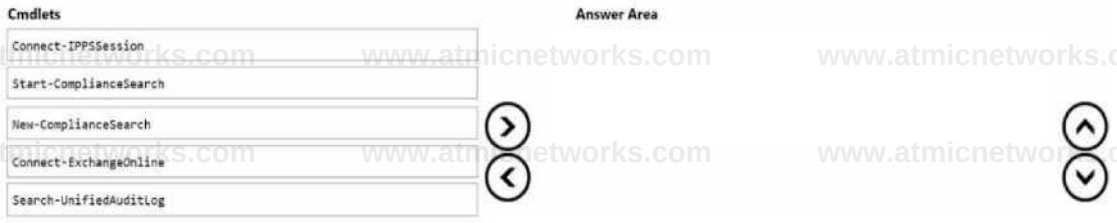
Question: 235

DRAG DROP

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

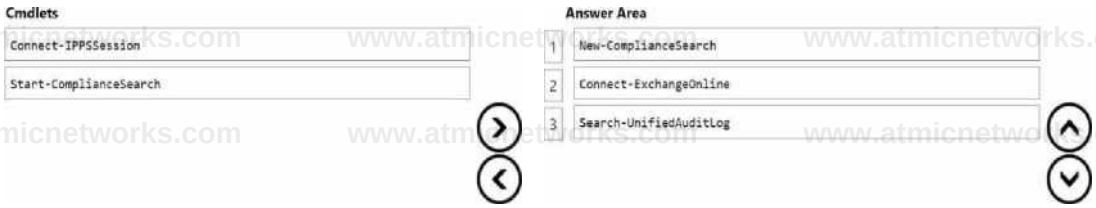
You need to identify phishing email messages.

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



Answer:

Explanation:



Question: 236

HOTSPOT

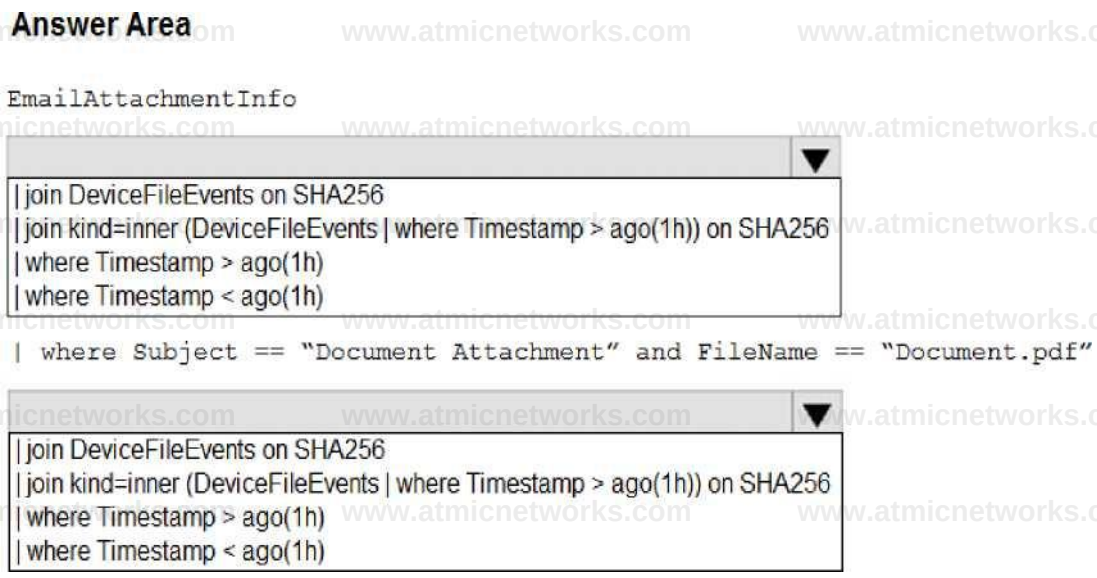
You have a Microsoft 365 E5 subscription.

You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:

- Only show emails sent during the last hour.
- Optimize query performance.

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

a. NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area

EmailAttachmentInfo

j where Timestamp > aqo(1 h)

J where Subject == "Document Attachment" and FileName == "Document.pdf" | join kind=inner (DeviceFileEvents | where Timestamp > aqo(1h)) on SHA256

Question: 237

HOTSPOT

You have a Microsoft Sentinel workspace that contains a custom workbook.

You need to query the number of daily security alerts. The solution must meet the following requirements:

- Identify alerts that occurred during the last 30 days.
- Display the results in a timechart.

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

a. NOTE: Each correct selection is worth one point.

Answer Area

```
SecurityAlert
| where TiaeGenerated >• agodOd)
|             ^ count() by ProviderNaae,                    ’  {TiaeGenerated,  id)
| render tiaechart
```

lookup project summarize

bin

make series

range

Answer:

Explanation:

Answer Area

```
SecurityAlert | where TimeGenerated >= ago(30d)
| summarize count() by ProvidarName, bin (TimeGenerated. Id)
| render timechart
```

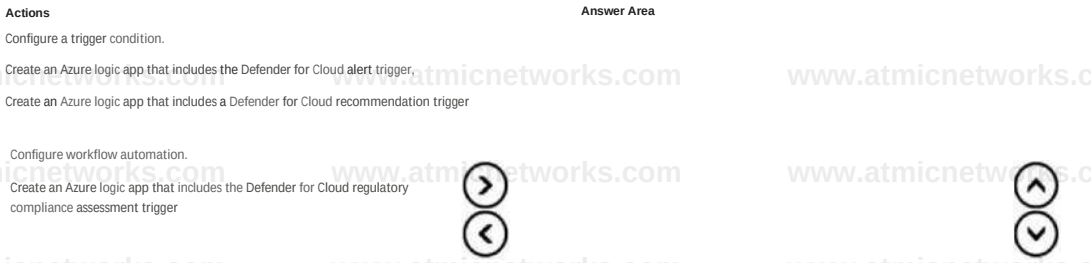
Question: 238

DRAG DROP

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

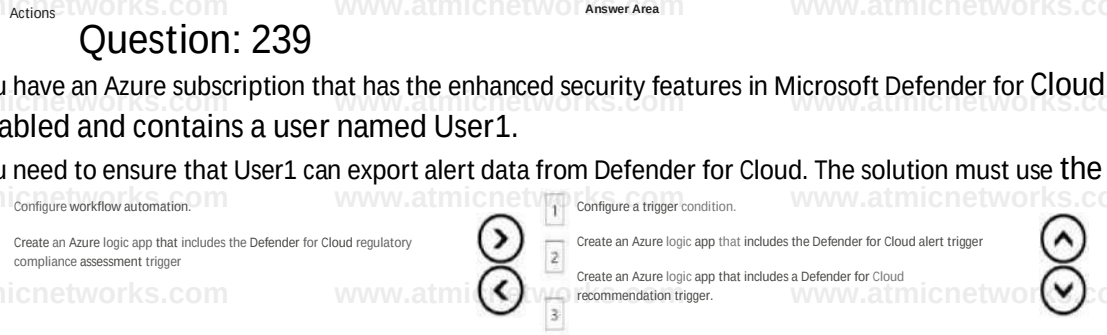
You need to create a workflow that will send a Microsoft Teams message to the IT department of your company when a new Microsoft Secure Score action is generated.

Which three 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.



Answer:

Explanation:



Question: 239

You have an Azure subscription that has the enhanced security features in Microsoft Defender for Cloud enabled and contains a user named User1.

You need to ensure that User1 can export alert data from Defender for Cloud. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Contributor
B. User Access Administrator
C. Owner
D. Reader

Answer: C

Explanation:

Question: 240

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps and has Cloud Discovery enabled.

You need to enrich the Cloud Discovery dat

a. The solution must ensure that usernames in the Cloud Discovery traffic logs are associated with the user principal name (UPN) of the corresponding Microsoft Entra ID user accounts.

What should you do first?

A. From Conditional Access App Control, configure User monitoring.
B. Create a Microsoft 365 app connector.
C. Enable automatic redirection to Microsoft 365 Defender.
D. Create an Azure app connector.

Answer: B

Explanation:

Question: 241

DRAG DROP

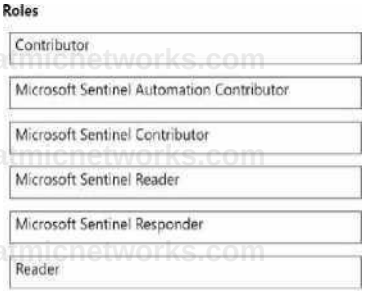
You have an Azure subscription that contains two users named User1 and User2 and a Microsoft Sentinel workspace named workspace1. You need to ensure that the users can perform the following tasks in workspace1:

- 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.

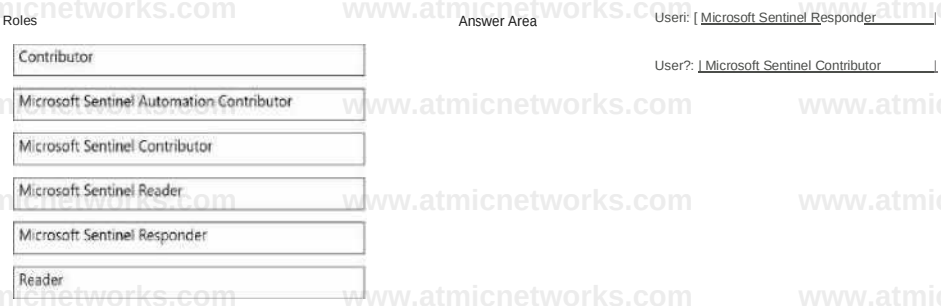
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 242

HOTSPOT

You have an Azure DevOps organization that uses Microsoft Defender for DevOps. The organization contains an Azure DevOps repository named Repo1 and an Azure Pipelines pipeline named Pipeline1. Pipeline1 is used to build and deploy code stored in Repo1.

You need to ensure that when Pipeline1 runs, Microsoft Defender for Cloud can perform secret scanning of the code in Repo1.

What should you install in the organization, and what should you add to the YAML file of Pipeline"!?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Install: [The Microsoft Security Code Analysis (MSCA) extension
Secure DevOps Kit for Azure (AzSK)
The Microsoft Security Code Analysis (MSCA) extension
The Microsoft Security DevOps extension

Add: Steps "
Inputs
Jobs
Steps

Answer:

Explanation:

Answer Area

Install: The Microsoft Security Code Analysis (MSCA) extension

Add: Steps '

Question: 243

HOTSPOT

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 Area

In Defender for Cloud: Add an environment.
Add an environment
Configure workflow automation.
Enable a plan.

In AzDO1: [Install an extension. Configure OAuth. Configure security policies
Install an extension

Answer

Explanation:

Answer Area

In Defender for Cloud: Add an environment.

In AzDOV Install an extension

Question: 244

HOTSPOT

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for WS1. The solution must follow the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra role: [Global Administrator]
- Global Administrator
- Security Administrator
- Security Operator

Role for WS1: [Microsoft Sentinel Contributor]
- Contributor
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor

Answer:

Explanation:

Answer Area

Microsoft Entra role: Global Administrator

Role for WS1: Microsoft Sentinel Contributor

Question: 245

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You need to create a detection rule that meets the following requirements:

- Is triggered when a device that has critical software vulnerabilities was active during the last hour
- Limits the number of duplicate results

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

NOTE: Each correct selection is worth one point.

Answer Area

```
DeviceTvmSoftwareVulnerabilities
| where VulnerabilitySeverityLevel == 'Critical'
| distinct DeviceId
| distinct CveId
| distinct DeviceId
```

```
| project away CveId
| project-keep DeviceId

| join kindsinner Deviceinfo on DeviceId

| where Timestamp between (now(-lh).,now())

. | project Timestamp, DeviceId ReportId
| distinct DeviceId
| distinct DeviceId, ReportId
| project Timestamp. DeviceId, ReportId
| summarize countQ by DeviceId, ReportId
```

Answer:

Explanation:

Answer Area

```
DeviceTvmSoftwareVulnerabilities

| where VulnerabilitySeverityLevel == 'Critical'
| distinct DeviceId

| join kindsinner Deviceinfo on DeviceId

| where Timestamp between Xnow(-lh)..now())

| project Timestamp, DeviceId, ReportId
```

Question: 246

You have a Microsoft Sentinel workspace named SW1.
In SW1, you investigate an incident that is associated with the following entities:

- Host
- IP address
- User account
- Malware name

Which entity can be labeled as an indicator of compromise (IoC) directly from the incident s page?

A. malware name
B. host
C. user account
D. IP address

Answer: D

Question: 247

You have a Microsoft 365 subscription that contains the following resources:

- 100 users that are assigned a Microsoft 365 E5 license
- 100 Windows 11 devices that are joined to the Microsoft Entra tenant

The users access their Microsoft Exchange Online mailbox by using Outlook on the web.
You need to ensure that if a user account is compromised, the Outlook on the web session token can be revoked.

What should you configure?

A. Microsoft Entra ID Protection
B. Microsoft Entra Verified ID
C. a Conditional Access policy in Microsoft Entra
D. security defaults in Microsoft Entra

Answer: C

Explanation:

Question: 248

HOTSPOT

You have a Microsoft Sentinel workspace that has a default data retention period of 30 days. The workspace contains two custom tables as shown in the following table.

Name	Table plan	Interactive retention	Total retention period
Table 1	Bask	Default	Default
Tabled	Analytics	Default	365

Each table ingested two records per day during the past 365 days.

You build KQL statements for use in analytic rules as shown in the following table.

Name	KQL statement
Query 1	**Tablet** **| where TiaeGenerated >■ ato(15)** **| suauurize countO**
Query2	**Tabled** **| where TfaeCenerated >* ago(l?O)** **I siMMrize count()**
Query]	**Tablet** **1 where Ti. teener a ted > - jfo(45)**

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point. Answer Ate*

Statements	Yes	No
For Query 1 to return a value of 3$. you must change Table plan **lo Analytics**		
For Query2 to return a value of 240 you must change Total retention period to **120 days**		
For Query3 to return 90 rows, you must change Total retention period lo **45 days**		

Answer:

Explanation:

Answer Area

Statements	Yes	No
For Query! lo return a value of 30. you must change Table plan **to Analytics**	O	*
For Query2 to return a value of 240 you must change Total retention period to **120 days**	C	*
For Query3 to return 90 rows you must change Total retention period to **45 days**	*	

Question: 249

Your on-premises network contains an Active Directory Domain Services (AD DS) forest.

You have a Microsoft Entra tenant that uses Microsoft Defender for Identity. The AD DS forest syncs with the tenant

You need to create a hunting query that will identify LDAP simple binds to the AD DS domain controllers.

Which table should you query?

A. AADServicePrincipalRiskEventi

B. IdentityLOgonEvents

C. AADDomainServicesAccountLogon

D. Signinlogs

Answer: B

Question: 250

You have a Microsoft Sentinel workspace that contains a custom workbook named Workbook1.

You need to create a visual based on the SecuntyEvent table. The solution must meet the following requirements:

- Identify the number of security events ingested during the past week.
- Display the count of events by day in a timechart

What should you add to Workbook1?

A. a query

B. a metric

C. a group

D. links or tabs

Answer: A

Question: 251

You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1.

You create a hunting query that detects a new attack vector. The attack vector maps to a tactic listed in the MITRE ATT&CK database.

You need to ensure that an incident is created in WS1 when the new attack vector is detected.

What should you configure?

A. a Fusion rule

B. a query bookmark

C. a scheduled query rule

D. a hunting livestream session

Answer: C

Explanation:

Question: 254

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

The security team at your company detects command and control (C2) agent traffic on the network.

Agents communicate once every 50 hours.

You need to create a Microsoft Defender XDR custom detection rule that will identify compromised devices and establish a pattern of communication. The solution must meet the following requirements:

- Identify all the devices that have communicated during the past 14 days.

Question: 255

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.

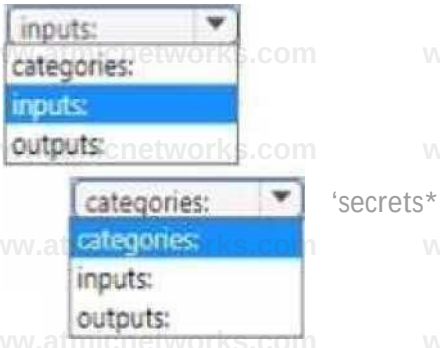
You need to configure Pipeline1 to output the results of secret scanning to Defender for Cloud,

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: C

Answer Area



Answer:

Explanation:

Question: 256

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint and contains a user named user1 and a Microsoft 365 group named Group1. All users are assigned a Defender for Endpoint Plan 1 license.

You enable Microsoft Defender XDR Unified role-based access control (RBAC) for Endpoints & Vulnerability Management.

You need to ensure that User1 can configure alerts that will send email notifications to Group1. The solution must follow the principle of least privilege.

Which permissions should you assign to User1?

A. Alerts investigation

B. Manage security settings

C. Defender Vulnerability Management - Remediation handling

D. Live response capabilities: Basic

Answer: A

Explanation:

Question: 257

You have a Microsoft Sentinel workspace named SW1.

You need to identify which anomaly rules are enabled in SW1.

What should you review in Microsoft Sentine1?

A. Settings

B. Entity behavior

C. Analytics

D. Content hub

Answer: C

Explanation:

Question: 258

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device 1. You initiate a live response session on Device1 and launch an executable file named File1.exe in the background. You need to perform the following actions:

- Identify the command ID of File1 exe.
- InteractwithFile1.exe.

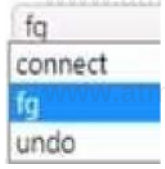
Which live response command should you run for each action? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area

Identify the command ID of Pile' exe:

interact with



Answer:

Explanation:

Answer Area

Identify' the command ID of File! exe: jobs

interact with Filel-exe: fq

Question: 259

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

You need to ensure that you can investigate threats by using data in the unified audit log of Microsoft Defender for Cloud Apps.

What should you configure first?

A. the Azure connector

B. the User enrichment settings

C. the Automatic log upload settings

D. the Microsoft 365 connector

Answer: D

Explanation:

Question: 260

You have a Microsoft 365 E5 subscription that contains a device named Device 1. Device 1 is enrolled in Microsoft Defender for End point.

Device1 reports an incident that includes a file named File1 exe as evidence.

You initiate the Collect Investigation Package action and download the ZIP file.

You need to identify the first and last time File1.exe was executed.

What should you review in the investigation package?

A. Processes

B. Scheduled tasks

C. Autoruns

D. Security event log

E. Prefetch files

Answer: E

Explanation:

Question: 261

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.sysonly

B. File1.sysand File3.docxonly

C. File1.sys. File3.docx, and File4jclsx only

D. File2.pdf. File3.docxr and File4.xlsx only

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

Answer: A

Explanation:

Question: 262

DRAG DROP

You have a Microsoft Sentinel workspace named SW1.

In SW1. you enable User and Entity Behavior Analytics (UEBA).

You need to use KQL to perform the following tasks:

- View the entity data that has fields for each type of entity.
- Assess the quality of rules by analyzing how well a rule performs.

Which table should you use in KQL for each task? To answer, drag the appropriate tables to the correct tasks. Each table 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: 263

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Purview and contains a Microsoft SharePoint Online site named Site1.

Site1 contains the files shown in the following table.

Name	Author
File 1 docx	Useri
File?, docx	User'
File3xlsx	User3

From Microsoft Purview, you create the content search queries shown in the following table.

Name	Query
Search!	Author:"User!" Filetxtensionixlsx
Search?	Author:"User*" ano FileExtension:*
Search 3	Author:("Userl..3")

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE; Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Searchi will return File3.		
Search2 will return Fde1		
Search3 will return File2.		

Answer:

Explanation:

Answer Area Statements	Yes	No
Searchi will return File3.	O	•
Search2 will return Filel.	®	O
Search3 will return File2.	•	

Question: 264

HOTSPOT

You have a Microsoft Sentine1 workspace that contains a custom workbook named Workbook1.

You need to create a visual in Workbook1 that will display the logon count for accounts that have logon event IDs of 4624 and 4634.

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

NOTE Each correct selection is worth one point.

Answer Area

```
SecurityEvent
| where EventID == "4624"
| summarize LogOnCount=count() by EventID, Account
| project LogOnCount, Account
|  [ join / project / summarize / union ]  kind =  [ full / inner / left / right ]  (
    SecurityEvent
    | where EventID == "4634"
    | summarize LogOffCount=count() by EventID, Account
    | project LogOffCount, Account
) on Account
```

Answer:

Explanation:

Answer Area

```
Security:.e-t
| where EventID •• "4624"
| summarize LogOnCount>count() by EventID, Account
| project LogOnCount, Account
I join .                " kind « inner ' {
  SecurityE.ent
  | where EventID •■ "4634"
  | summarize LojOTfCount*count() by EventID, Account
  I project LogOrfCount, Account
) on Account
```

Question: 265

You have an Azure subscription that contains a resource group named RG1. RG1 contains a Microsoft Sentinel workspace. The subscription is linked to a Microsoft Entra tenant that contains a user named User1.

You need to ensure that User1 can deploy and customize Microsoft Sentine1 workbook templates.

The solution must follow the principle of least privilege.

Which role should you assign to User1 for RG1?

A. Workbook Contributor

B. Microsoft Sentinel Contributor

C. Contributor

D. Microsoft Sentinel Automation Contributor

Answer: B

Explanation:

Question: 266

You have 500 on-premises Windows 11 devices that use Microsoft Defender for Endpoint

You enable Network device discovery.

You need to create a hunting query that will identify discovered network devices and return the identity of the onboarded device that discovered each network device.

Which built-in function should you use?

A. current_cluster,endpoint()

B. DeviceFromIP ()

C. next ()

D. SeenBy ()

Answer: B

Explanation:

Question: 268

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

You need to assign the PCI DSS 4.0 initiative to Sub1 and have the initiative displayed in the Defender for Cloud Regulatory compliance dashboard.

From Security policies in the Environment settings, you discover that the option to add more industry and regulatory standards is unavailable.

What should you do first?

A. Enable the Cloud Security Posture Management (CSPM) plan for the subscription.

B. Disable the Microsoft Cloud Security Benchmark (MCSB) assignment.

C. Configure the Continuous export settings for Azure Event Hubs.

D. Configure the Continuous export settings for Log Analytics.

Answer: A

Explanation:

Question: 269

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 1 and contains a macOS device named Device1.

You need to investigate a Defender for Endpoint agent alert on Device1. The solution must meet the following requirements:

- Identify all the active network connections on Device1.
- Identify all the running processes on Device1.
- Retrieve the login history of Device1.
- Minimize administrative effort.

What should you do first from the Microsoft Defender portal?

A. From Advanced features in Endpoints, disable Authenticated telemetry.

B. From Advanced features in Endpoints, enable Live Response unsigned script execution.

C. From Devices, click Collect investigation package for Device 1.

D. From Devices, initiate a live response session on Device1.

Answer: C

Explanation:

Question: 270

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains a Windows device named Device1. You need to investigate a suspicious executable file detected on Device1. The solution must meet the following requirements:

- Identify the image file path of the file.
- Identify when the file was first detected on Device1.

What should you review from the timeline of the detection event? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

To identify the image file path: f_{ntdlw}

Action type

Event entities graph

To identify when the file was first detected Event entities graph

Action type Entities

Event entities graph

Answer:

Explanation:

Answer Area

To identify the image file path: Entities

To identify when the file was first detected Event entities graph

Question: 271

HOTSPOT

You have an Azure subscription that contains a Log Analytics workspace named Workspace1.

You configure Azure activity logs and Microsoft Entra ID logs to be forwarded to Workspace1.

You need to identify which Azure resources have been queried or modified by risky users.

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

NOTE: Each correct selection is worth one point.

Answer Area

I AzureActiV'ty

AzureActnnty

```
MicrosoftGraphActrvitylogs UserRbkEvents     i

| join AADRiskyUser† on (Left.UserId •• (right.Id
```

† Send Prod for further review.

Which live response command should you run for each action? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

You have an on-premises network.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Identity.

From the Microsoft Defender portal, you investigate an incident on a device named Device1 of a user named User1. The incident contains the following Defender for Identity alert.Suspected identity theft (pass-the-ticket) (external ID 2018)

```
| extend resourcePath • replace string(replace_string(nplace regea(tostrlng [parse path(SouKe$y$tem)) K
                                                                                    (parse uH(Requ«tUn) Path)
                                                                                    (parse_xml(ATContenl))
 | suianarize RequestCount»dcount(Requl*stId) by Userid, RiskState, resourcePath, Requesterthod, ResponseStatu;
```

Answer:

Explanation:

Answer Area

AzureAaivity *

| join AADRiskyUsers on {left.Userid -• (right.Id

| extend resourcePath • replacestrinu(replace_string(replace regex(tostring (parse path(SourceSystem))

| stMMMrize RequestCount-dcount(Requ*stId) by Userid, Riskstate, resourcepath, RequestAethod, ResponseStatusCode

Question: 273

What should you do?

A. Disable User 1 only.

B. Quarantine Device1 only.

C. Reset the password for all the accounts that previously signed in to Device1.

D. DisableUser1 and quarantine Device1.

E. Disable User1, quarantine Device1, and reset the password for all the accounts that previously signed in to Device1.

Answer: A

Explanation:

Question: 275

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:

Question: 276

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

You are investigating an attacker that is known to use the Microsoft Graph API as an attack vector.

The attacker performs the tactics shown the following table.

Name	Tactic
Tactic 1	Conditional Access policy reconnaissance
Tactic?	Mailbox reconnaissance
Ta<riH	Invites guest users to the tenant

You need to search for malicious activities in your organization.

Which tactics can you analyze by using the MicrosoftGraphActivityLogs table?

A. Tactic? only

B. Tactic1 and Tactic2 only

C. Tac1ic2 and Tactic3 only

D. Taclic1. Tac1ic2. andTactic3

Answer: B

Explanation:

Question: 278

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:

Question: 279

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:

Question: 280

HOTSPOT

You have on-premises servers that run Windows Server.

You have a Microsoft Sentinel workspace named SW1. SW1 is configured to collect Windows Security log entries from the servers by using the Azure Monitor Agent data connector.

You plan to limit the scope of collected events to events 4624 and 462S only.

You need to use a PowerShell script to validate the syntax of the filter applied to the connector.

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

NOTE: Each correct selection is worth one point.

Answer Area

```
Savants * ' | SecuntY!'l$y$tem[(EventiD=4624 or EventI0=4625)]]
              ©llog='Secun ty*;Evcnt Type=*Systcm*;Evc nt ID=*4624*;EventIO=*4625*
              < Security* < System* <EwntID>4624</EventID> <EventID*4625</EventID* </System*
              ■
              Secunly*[$ystem[(EventID 4624 or EventID 4625)1]
```

Get-WinEvent -LogName 'Security* I FilterXPath ' I Sevents FilterHashtable -FilterXml

FilterXPath

Answer:

Explanation:

Answer Area

Savants • * S«uhtyf*|System[(EventiD=4624 or EventID=4625)]|

Get-WinEvent -LogNoire 'Security' FiitetXPath ^ invents

Question: 282

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1. WS1 uses Microsoft Defender for Cloud.

You have the Microsoft security analytics rules shown in the following table.

Name	Service	Seventy	Action
Rule!	Defender for Cloud	High	Create incident
Rule?	Defender for Cloud	High	Create incident
RuleJ	Defender for Cloud	High	Create incident
Rule4	Defender for Cloud	High	Create incident

User1 performs an action that matches Rule1, Rule2, Rule3, and Rule4. How many incidents will be created in WS1?

A. 1
B. 2
C. 3
D. 4

Answer: A

Explanation:

Question: 283

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices. You plan to create a Microsoft Defender XDR custom deception rule. You need to ensure that the rule will be applied to only 10 specific devices. What should you do first?

A. Add the IP address of each device to the list of decoy accounts and hosts of the rule.
B. Add the devices to a group.
C. Add custom lures to the rule.
D. Assign a tag to the devices

Answer: B

Explanation:

Question: 284

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:

Question: 293

You have an Azure subscription that uses Microsoft Defender XDR.
From the Microsoft Defender portal, you perform an audit search and export the results as a file named Filel.csv that contains 10,000 rows.
You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from Filel.csv. The operations fail to generate columns for specific JSON properties.
You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.
Solution: From Defender, you modify the search criteria of the audit search to reduce the number of returned records, and then you export the results. From Excel, you perform the Get & Transform Data operations by using the new export.
Does this meet the requirement?

A. Yes
B. No

Answer: A

Explanation:

Question: 294

You have an Azure subscription that uses Microsoft Defender XDR.
From the Microsoft Defender portal, you perform an audit search and export the results as a file named Filel.csv that contains 10,000 rows.
You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from Filel.csv. The operations fail to generate columns for specific JSON properties.
You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.
Solution: From Excel, you apply filters to the existing columns in Filel.csv to reduce the number of rows, and then you perform the Get & Transform Data operations to parse the AuditData column. Does this meet the requirement?

A. Yes
B. No

Answer: B

Explanation:

Question: 295

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, Devke2, Device3, and Device4

Answer: B

Question: 298

HOTSPOT
You have the resources shown in the following table.

Name	Type	Description
Server 1	On-premises server	On-boarded to Azure Arc Runs Windows Server 2022 Has Microsoft SQL Server 2022 installed
VM1	SQL Server on Azote Virtual Machines	Runs Windows Seiver 2022 Has Microsoft SQL Serve? 2022 installed

You have an Azure subscription that uses Mictosoft Defender for Cloud.
You need to use Defender for Cloud to protect VM1 and Server1. The solution must meet the following requirements:

- Support Advanced Threat Protection and vulnerability assessment
- Register each SQL Server 2022 instance as a SQL virtual machine.
- Minimize implementation and administrative effort

What should you deploy to each server? To answer, select the appropriate options in the answer

area.

NOTE: Each correct selection is worth one point.

Answer Are*

VM1 The Azure Monde Agent and an Azure virtual reach ne cxte'ision

An Azure virtual machine extension

The Log Analytics agent and an Azure virtual machine extension

Served The Azure Monitpi Agen; and in Azu'e virtual machine extension

An Azure virtual machine extension

The Azure Monitor Agent and an Azure virtual machine extension

The log Analytics agent and an Azure virtual machine extension

Answer:

Explanation:

Answer Area

VM1 | The Azure Monitor Agent and an Azure virtual reach ne e<temion *

Serveri The Azure Monitor Agent and an Azure virtual machine extension '

Question: 299

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

Question: 300

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 configure endpoint detection and response (EDR) in block mode.

Does this meet the goal?

A. Yes
B. No

Answer: A

Question: 301

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 configure Controlled folder access. Does this meet the goal?

A. Yes
B. No

Answer: B

Question: 302

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

Question: 303

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
A. device groups

B. device tags
C. honeytoken entity tags
D. sensitive entity tags

Answer: A

Question: 304

You have 500 on-premises devices.
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You onboard 100 devices to Microsoft Defender XDR.
You need to identify any unmanaged on-premises devices. The solution must ensure that only specific onboarded devices perform the discovery.
What should you do first?

A. Set Discovery mode to Basic
B. Create a device group.
C. Create a tag.
D. Create an exclusion.

Answer: D

Question: 307

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.
You are investigating an incident.
You need to review the incident tasks that were performed. The solution must include a query that will display the incidents in a workbook, and then display the tasks of each incident in another grid. Which table should you target in the query?

A. SecurityIncident

B. SecurityEvent
C. Sentine1Audit
D. SecurityAlert

Answer: A

Explanation:

Question: 309

You have 1,000 on-premises Windows 11 Pro devices that are onboarded to Microsoft Defender for Endpoint. You have a Microsoft 365 subscription that uses Microsoft Defender XDR. You identify that an attacker performed the following actions on a device:

- Modified the file system path of a registry-based antivirus exclusion
- Downloaded a malicious file to the file system path

You initiate a live response session on the device. You need to undo the registry change. Which command should you run?

A. analyze
B. registry
C. remediate
D. scan

Answer: B

Explanation:

Question: 310

You have a Microsoft 365 B5 subscription. You have a PowerShell script that queries the unified audit log. You discover that the query returns only the first page of results due to server-side paging. You need to ensure that you get all the results. Which property should you query in the results?

A. @odata.nextlink
B. @odata.deltaLink
C. @odata.context
D. @odata.count

Answer: A

Explanation:

Question: 311

You have a Microsoft 365 subscription. You have the following KQL query. DeviceEvents
| where ActionType == "AntivirusDetection‡
You need to ensure that you can create a Microsoft Defender XDR custom detection rule by using the query.
What should you add to the query?

A. summarize (Timestamp, DeviceHanw)=arg_min(Timestampf DeviceName), count() by DeviceId
B. sumarize (Timestamp, ReportId)>arg_max(Timestanp, ReportId), C. count{) by DeviceId
summarize (Timestamp)=range(Timestatip), count() by DeviceId D.
sumarize (ReportId)=make_set(ReportId), count() by DeviceId

Answer: B

Explanation:

Question: 321

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

Question: 316

You have an Azure subscription that contains a Microsoft Sentinel workspace named Workspace1 and a user named User1.
You need to ensure that User1 can investigate incidents by using Workspace1. The solution must follow the principle of least privilege.
Which role should you assign to User1?

A. Microsoft Sentinel Responder
B. Microsoft Sentinel Reader

C. Microsoft Sentinel Automation Contributor
D. Microsoft Sentinel Contributor

Answer: A

Question: 317

You have a Microsoft 365 B5 subscription that contains a user named User1. The subscription uses Microsoft 365 Copilot for Security. Copilot for Security uses the Sentinel plugin. User1 is assigned the Copilot Contributor role.
During an investigation, User1 submits a prompt and receives a notification that Copilot for Security cannot respond to requests because the security compute unit (SCU) usage is nearing the provisioned capacity limit.
You need to ensure that User1 can use Copilot for Security to generate a successful response. What should User1 do?

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

Answer: D

Explanation:

Question: 319

You have a Microsoft 365 B5 subscription that uses Microsoft Defender XDR. You are investigating an incident
You need to review the incident tasks that were performed. What can you use on the Incident page?

A. Tasks only
B. Tasks and Activity log only
C. Tasks and Alert timeline only
D. Tasks, Activity log, and Alert timeline

Answer: D

Explanation:

Question: 322

You have a Microsoft 365 E5 subscription.
You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode.
All Windows devices are on boarded to Microsoft Defender for Endpoint.

You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product. Solution: You enable Live Response. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Question: 323

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

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

Answer: C

Explanation:

Question: 324

You have a Microsoft 365 E5 subscription and a Microsoft Sentinel workspace. You need to create a KQL query that will combine data from the following sources:

- Microsoft Graph
- Risky users detected by using Microsoft Entra ID Protection

The solution must minimize the volume of data returned. How should the query start?

A. MicrosoftGraphActivityLogs
lookup kind=leftouter AADRiskyUsers on $left.UserId == $right.Id
B. MicrosoftGraphActivityLogs
join AADRiskyUsers on $left.UserId == $right.Id
C. MicrosoftGraphActivityLogs
join AADUserRiskEvents on $left.UserId == $right.Id
D. find in (MicrosoftGraphActivityLogs, AADUserRiskEvents) where

Answer: B

Explanation:

Question: 325

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

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

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

Answer: A

Explanation:

Question: 329

Your company stores the data of every project in a different Azure subscription. All the subscriptions use the same Microsoft Entra tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Microsoft Sentinel to a new Azure subscription.

You need to perform hunting queries in Microsoft Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

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 query that uses the resource expression and the alias operator.
B. Use the alias statement.
C. Add the Microsoft Sentinel solution to each workspace.
D. Create a query that uses the workspace expression and the union operator.
E. Add the Security Events connector to the Microsoft Sentinel workspace.

Answer: CD

Explanation:

Question: 330

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

- Prompt1: Provides access to the Entra plugin
- Prompt2: Provides access to the Intune plugin
- Prompt3: Provides access to the Entra plugin
- User1 shares the session with User2.

User2 does NOT have access to Microsoft Intune.

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

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

Answer: D

Explanation:

must meet the following requirements:

- Ensure that you can build a tailored list of actions for each type of incident.
- Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Question: 332

HOTSPOT

You have a Microsoft Sentinel workspace.

You need to configure the Fusion analytics rule to temporarily supress incidents generated by a Microsoft Defender connector. The solution must meet the following requirements:

- Minimize impact on the ability to detect multistage attacks.
- Minimize administrative effort.

How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Trigger: When incident is updated

Actions: Run playbook '

Question: 333

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

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

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

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

Answer: D

Explanation:

Question: 334

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains two users named User1 and User2.

You need to ensure that the users can perform searches by using the Microsoft Purview portal. The solution must meet the following requirements:

- Ensure that User1 can search the Microsoft Purview Audit service logs and review the Microsoft Purview Audit service configuration.
- Ensure that User2 can search Microsoft Exchange Online mailboxes.
- Follow the principle of least privilege.

To which Microsoft Purview role group should you add each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Useri; Audit Reader

User2: Data Investigator

Question: 335

HOTSPOT

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

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

You need to review the following forensic data points:

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

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

Is an attacker currently accessing Device! remotely. *

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Scheduled tasks
- Services
- Security event log

When was Frielexe first executed: *

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Scheduled tasks
- Services
- Security event log

Answer:

Explanation:

Question: 336

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

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

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

Which files can you submit?

A. File1.ps1 only

B. File2.exe only

C. File3.dll only

D. File2.exe and File3.dll only

E. File1.ps1 and File2.exe only

F. File1.ps1, File2.exe, and File3.dll

Answer: D

Explanation:

Question: 338

HOTSPOT

You have an Azure subscription that contains the users shown in the following table.

Name	Role	Scope
Used	Contributor	Subscription
User2	Contributor	Subscription
User3	Security Reader	Resource group

The subscription contains instances of Azure Firewall as shown in the following table.

Name	Log configuration	Destination
AFW1	Unstructured logs	Log Analytics
AFW2	Structured intrusion detection and prevention system (IDPS) logs	Azure Event Hubs

AFW3	Structured intrusion detection and prevention system (IDPS) logs	Log Analytics

You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security. You have the Copilot for Security role assignments shown in the following table.

User	Role
Useri	Copilot Owner
User2	Copilot Contributor
User3	Copilot Owner

Each user runs a Copilot for Security session.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Used can use prompts to retrieve information from AFW1.	O	O
User2 can use prompts to retneve information from AFW2	0	0
User3 can use prompts to retneve i nformation from AFW3	O	O

Answer:

Explanation:

Yes No Yes

Answer:

Explanation:

Questio n Part 1: Which types of files can you use for the custom lure? Answer:

EXE, XLSX, and PDF

According to your screenshot (File types drop-down), you can use the following file types for a custom lure in Microsoft Defender XDR deception rules:

EXE

XLSX

PDF

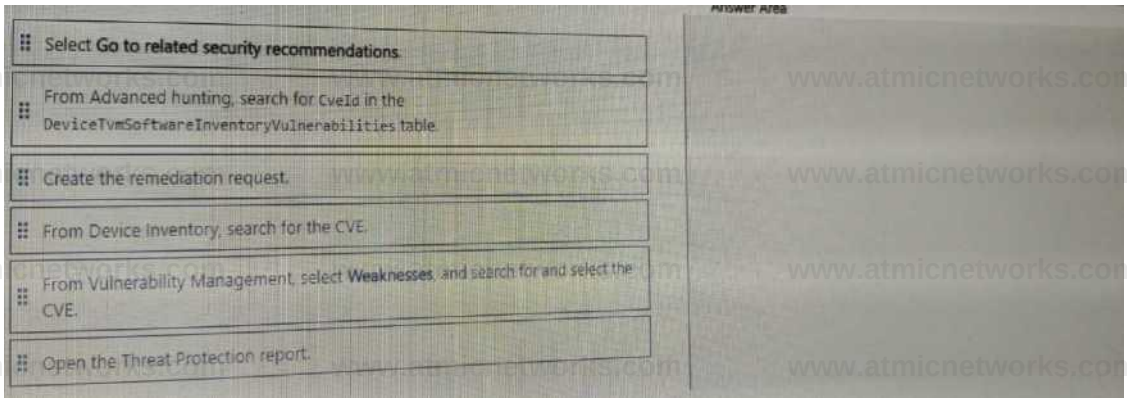
Question: 340

DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use the Microsoft Defender portal to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three 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.



Answer:

Explanation:

From Vulnerability Management, select Weaknesses, and search for and select the CVE.
Select Go to related security recommendations.
Create the remediation request.

Question: 341

HOTSPOT

You have multiple Azure subscriptions that contain multiple Microsoft Sentinel workspaces.

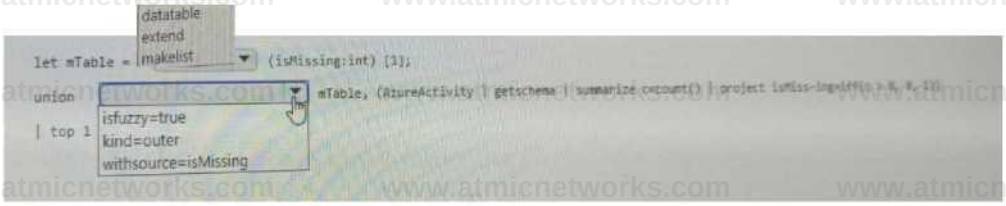
You are creating a Microsoft Sentinel workbook that will include references to the AzureActivity table.

You need to create a KQL query that will perform the following actions:

. Check whether the AzureActivity table exists in each workspace.
. If the table exists, return a single row that has the isMissing column set to 0.
. If the table does NOT exist, return a single row that has the isMissing column set to 1.

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

let mTable = makelist(isMissing:int) [1];
The union kind=outer statement combines results from both branches.

Question: 342

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

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

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

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

What should you include in the solution?

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

Answer: C

Explanation:

Question: 343

You have a Microsoft 365 E5 subscription that contains 500 Windows 11 devices.

You have a Microsoft Defender for Endpoint deployment that has the following settings:

Discovery mode: Basic
Live Response: Disabled
Enable EDR in block mode: Off
Tamper Protection: Off

You need to implement automatic attack disruption in Microsoft Defender XDR.

What should you do?

A. Set Enable EDR in block mode to On.
B. Set Live Response to On.
C. Change Discovery mode to Standard discovery.
D. Set Tamper Protection to On.

Answer: A

Explanation:

Question: 344

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You have a custom detection rule named Rule1 that generates an alert if more than five antivirus detections are identified on a device. Rule1 has a loopback period of 12 hours.
You need to change the loopback period to 48 hours.
What should you modify for Rule1?

A. the frequency
B. the summarize operator of the KQL query
C. the where operator of the KQL query
D. the scope

Answer: A

Explanation:

Question: 345

HOTSPOT
You have an Azure subscription named Sub1 that is linked to a Microsoft Entra tenant named contoso.com.
Contoso.com contains a user named User1. Sub1 contains a Microsoft Sentinel workspace.

You provision a Microsoft Copilot for Security capacity.

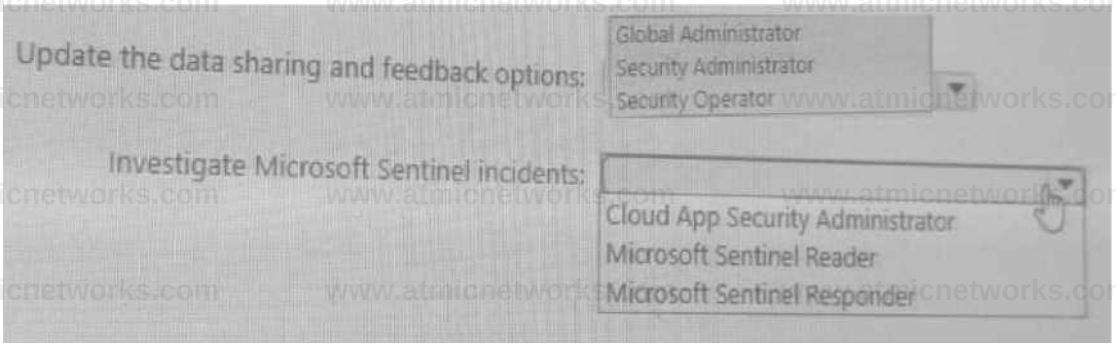
You need to ensure that User1 can use Copilot for Security to perform the following tasks:

. Update the data sharing and feedback options.
. Investigate Microsoft Sentinel incidents.

The solution must follow the principle of least privilege.

Which role should you assign to User1 for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point



Answer:

Explanation:

Task	Role
Update the data sharing and feedback options	Security Administrator
Investigate Microsoft Sentinel incidents	Microsoft Sentinel Responder

Question: 346

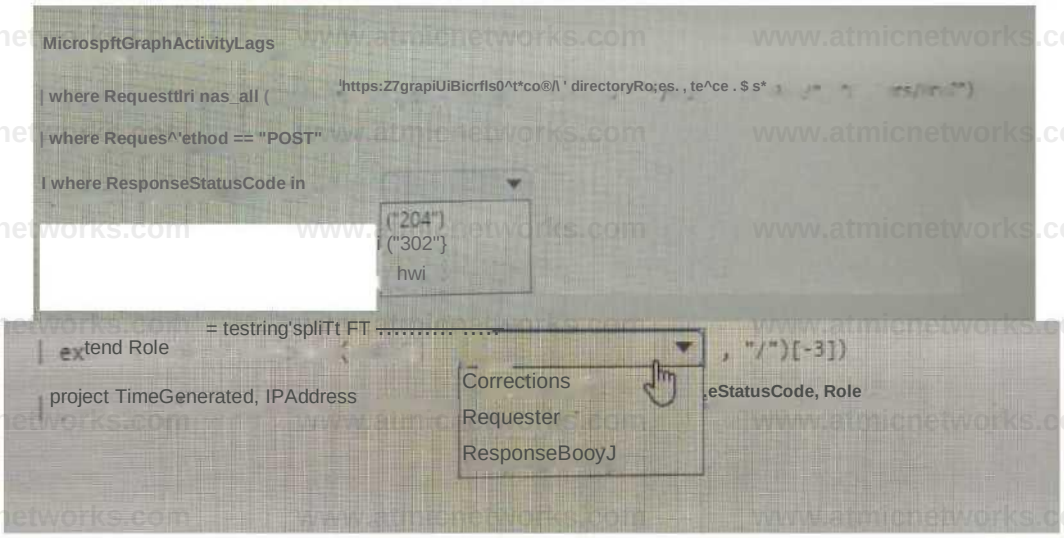
HOTSPOT

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

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

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

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Dropdown/Step	Value to Select
where ResponseStatusCode in (...) ("204") split([dropdown], "/")[-3]	RequestUri

Question: 347

You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security.

You start a Copilot for Security session and enter five prompts that each provide responses.

You need to create a promptbook that will use the prompts but will NOT contain the responses. The solution must minimize administrative effort.

What should you do?

A. Enter a new prompt that has the following input: Create a promptbook from my session prompts.
B. Select each prompt, and then select Create promptbook.
C. Share the session, and then select Create promptbook.
D. Create a new promptbook and include each prompt.

Answer: A

Explanation:

Question: 348

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:

Question: 349

You need to update the threat intelligence list to include the entities. Which entities can you add on the Incident page?

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

Answer: A

Explanation:

Question: 350

HOTSPOT

You have an Azure subscription named Sub1 that contains a Microsoft Sentinel workspace named WS1. You need to create a hunting query in WS1 that meets the following requirements:

- Returns the number of changes performed daily by each Microsoft Entra security principal during a seven-day period
- Identifies all the successful changes to the resources in Sub1
- Substitutes any missing data points with 0

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

a. NOTE: Each correct selection is worth one point.

Answer Area


```
| where OperationNameValue endswith "write"

| where ActivityStatusValue == "Succeeded"

| make-series_____ * dcount(ResourceId) defaults® on EventSubmissionTimestainp in range(ago(7
| make-series
| mv-expand | summarize
```

Answer:

Explanation:

Answer Area


```
lue endswith "write"
alue == "Succeeded"
```

|make-senes ᵛ dCOunt(ResourceId) defaults on Event5ubmi$$ionTim«$tamp in range(ago(7

Question: 351

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:

Question: 352

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

Question: 354

HOTSPOT

You have a Microsoft Sentinel workspace.

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

You need to create a Microsoft Sentinel workbook that will include a visualization of the query. To what should you set Data source and Resource type for the workbook? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

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

Logs (Analytics)

Logs (Basic)

Resource type: Microsoft Sentinel

Application insights Log Analytics

Microsoft Sentinel

Security Alert Workspace

Answer:

Explanation:

Answer Area

Data source: Logs (Analytics)

Resource type: Microsoft Sentinel

Question: 355

HOTSPOT

You have an on-premises Linux server that runs a background process named App1 and has the Azure Connected Machine agent installed.

You have a Microsoft Sentinel workspace named WS1.

You need to configure a data collection rule (DCR) named DCR1 that will use the Syslog via AMA connector to collect messages related to App1. The solution must meet the following requirements:

- Only collect messages that have a priority level of critical.
- Minimize the volume of data collected.

Which facility and log level should you configure for DCR1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Question: 356

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:

Question: 357

You plan to review Microsoft Defender for Cloud alerts by using a third-party security information and event management (SIEM) solution.
You need to locate alerts that indicate the use of the Privilege Escalation MITRE ATT&CK tactic.
Which JSON key should you search?

A. Intent
B. Description
C. ExtendedProperies
D. Entities

Answer: A

Explanation:

Question: 358

You have a Microsoft 365 subscription that uses Microsoft Copilot for Security.
You create a promptbook named Book1.
For Book1, you need to create a prompt that contains an input named IncidentID.
How should you format IncidentID?

A. <IncidentID>
B. SIncidentID$

C. ##IncidentID##
D. [IncidentID]

Answer: A

Explanation:

Question: 359

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:

Question: 360

DRAG DROP

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

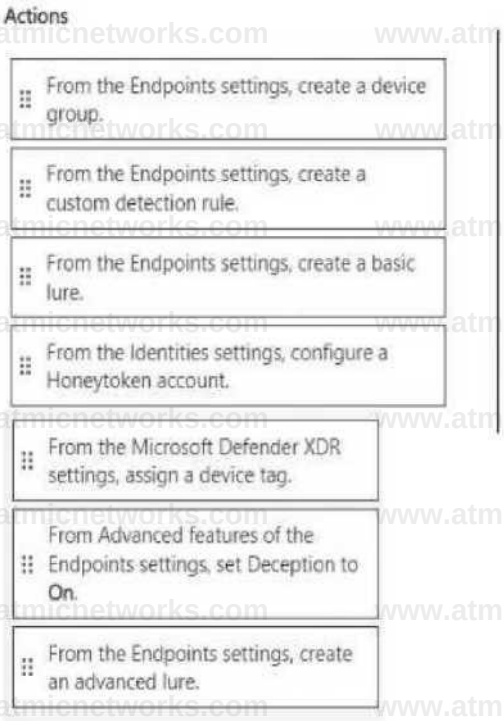
You need to perform the following actions in Microsoft Defender XDR:

- For your company's finance department, populate random endpoints with fake cached credentials.
- Ensure That an incident is created in Microsoft Defender XDR if an attacker attempts to use the fake cached credentials.

The solution must ensure that the fake cached credentials are planted only on endpoints of the finance department.

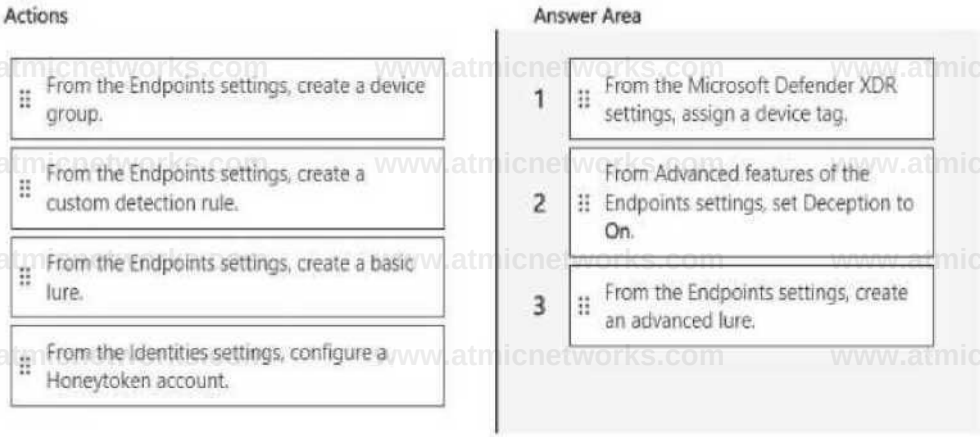
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

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



Answer:

Explanation:



Question: 361

You have a Microsoft 365 E5 subscription.

You need to search the Microsoft Purview audit log by using PowerShell on a Windows device. What should you do first?

A. Modify the TrustedHosts list
B. Install the Microsoft Exchange Online PowerShell module.
C. Install the Microsoft Graph PowerShell module.
D. Enable PowerShell remoting.

Answer: B

Explanation:

Question: 362

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. Microsoft Purview, and Exchange Online.

You have a partner company named Contoso, Ltd.

You need to review all the emails that contain PDF attachments and were received from Contoso during the past month. The solution must minimize administrative effort.

What should you use?

A. Advanced Hunting
B. Content explorer
C. Content search
D. Activity explorer

Answer: C

Explanation: