Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **SC-200**

Title : Microsoft Security Operations Analyst

Version : DEMO

1. 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

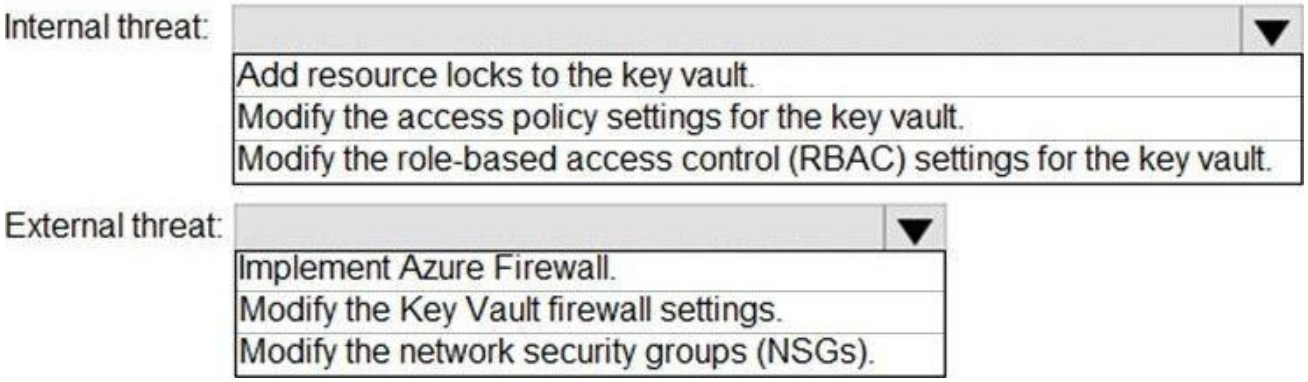
The issue for which team can be resolved by using Microsoft Defender for Endpoint?
A. executive
B. sales
C. marketing
Answer: B
Explanation:
According to Microsoft Security Operations documentation, Microsoft Defender for Endpoint is designed to protect endpoint devices—including Windows, macOS, Android, and iOS—against cyberattacks through advanced behavioral analysis, threat intelligence, and automated investigation and remediation.

In the given case study, the sales team exclusively uses iOS devices and has previously experienced attacks while exchanging files using third-party applications. These unmanaged file-sharing methods exposed the team to malware, phishing, and data leakage threats.
By implementing Microsoft Defender for Endpoint on iOS, Contoso can apply unified endpoint protection across all mobile devices. Defender for Endpoint's mobile threat defense (MTD) capabilities detect malicious apps, risky network connections, jailbroken devices, and phishing attempts. It also integrates with Microsoft Intune for compliance enforcement and conditional access—ensuring only secure, compliant devices can access corporate resources. This directly mitigates the security challenges faced by the sales team while minimizing manual investigation effort through automated response.
Therefore, the issue affecting the sales team (mobile device attacks and unsafe file transfers) can be effectively resolved using Microsoft Defender for Endpoint.

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:
As outlined in Microsoft's official Defender for Office 365 documentation, this service provides comprehensive protection against threats targeting Microsoft 365 collaboration tools—such as SharePoint Online, OneDrive for Business, and Microsoft Teams. The marketing team uses SharePoint Online for vendor collaboration and has experienced incidents in which vendors uploaded malicious files. Microsoft Defender for Office 365 specifically addresses this scenario through features like Safe Attachments and Safe Links, which automatically scan uploaded or shared files for malware and block access to harmful content.
When a vendor uploads a file to SharePoint Online, Defender for Office 365 inspects the file in real time within a virtual sandbox environment before allowing users to open or share it. If malware is detected, the system quarantines or removes the file and notifies administrators. These detection and remediation capabilities prevent infection propagation, protect sensitive marketing data, and maintain compliance with Contoso's security posture.
By leveraging Defender for Office 365, Contoso's marketing team can continue external collaboration safely, ensuring that all uploaded files are scanned and validated before internal access—thereby resolving their specific malware-related issue.

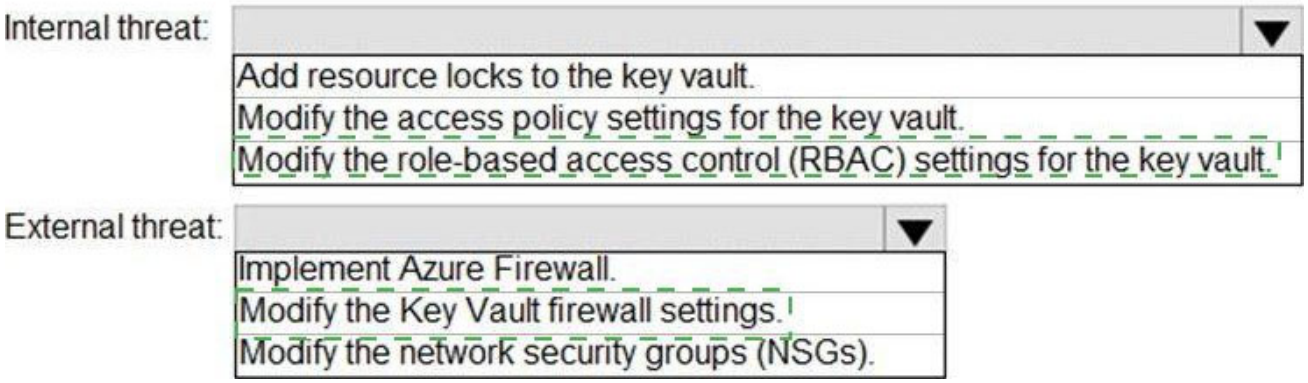
3.HOTSPOT
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Internal threat: Modify the access policy settings for the key vault.

External threat: Modify the Key Vault firewall settings.

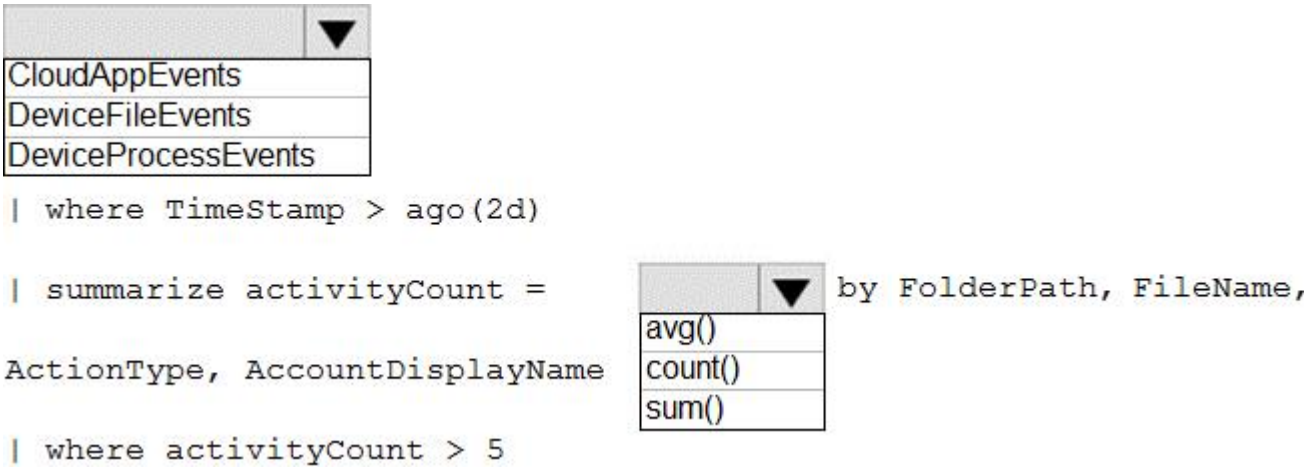
For internal threats involving a potential compromise of Fabrikam's own Azure AD applications, the most direct and least disruptive remediation is to modify the Key Vault access policies (or RBAC assignments, if RBAC for Key Vault data-plane is in use) to immediately remove or reduce the compromised service principal's permissions (Get/List/Decrypt/Sign/Wrap). Microsoft guidance for Key Vault access emphasizes least privilege and promptly revoking credentials or app permissions when compromise is suspected. Access policies (or data-plane RBAC) govern which identities can access secrets, keys, and certificates; adjusting these stops further data-plane actions by the compromised app. "Resource locks" protect against deletion or configuration changes at the management plane, but they do not remove a compromised identity's ability to read or use vault objects, so they are not an appropriate first response for this scenario.

For external threats, Microsoft recommends hardening Key Vault firewall and networking: restrict public network access, allow only required IPs, use virtual network rules, and prefer private endpoints. Key Vault includes a built-in firewall for IP and VNet ACLs; tuning these controls reduces exposure to the public internet and blocks unauthorized traffic. NSGs apply to IaaS subnets/nics and don't directly secure

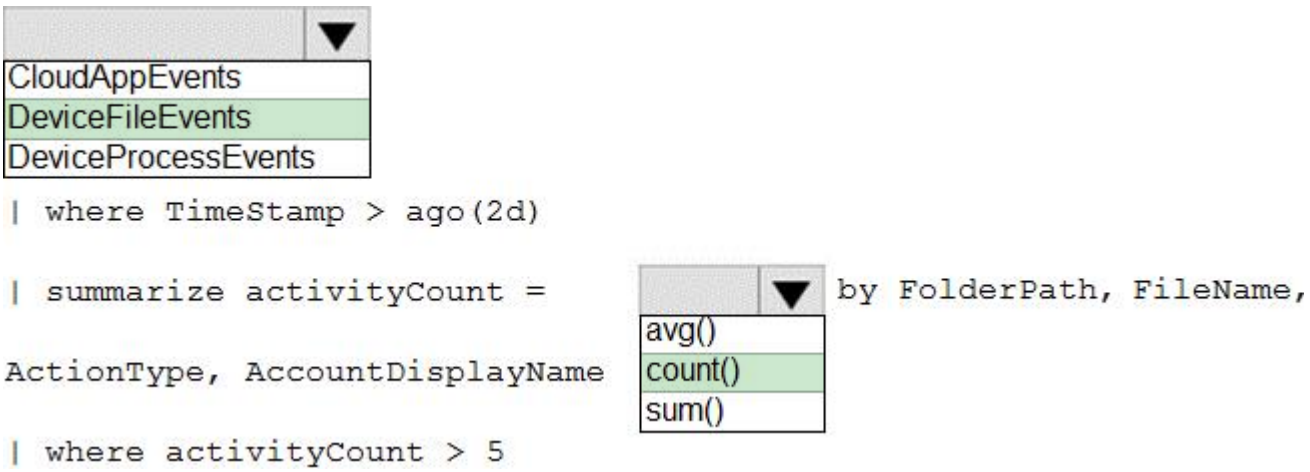
the public Key Vault endpoint. Azure Firewall can add perimeter control, but it is not necessary for remediating a specific Key Vault Defender alert; the most effective and immediate remediation is tightening the Key Vault firewall settings to limit external access pathways.

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: To meet the requirement “Receive alerts if an Azure virtual machine is under brute force attack,” you should enable Azure Defender (now Microsoft Defender for Cloud plans for Servers). Defender continuously collects and analyzes security telemetry from your VMs (RDP/SSH sign-in attempts, process and network signals, and OS logs) and raises security alerts for patterns that indicate attacks such as RDP/SSH brute force. These alerts include rich context (attacked host, source IPs, timeframe, and recommended remediation) and natively integrate with Microsoft Sentinel, allowing incidents, automation rules, and playbooks to be triggered with minimal administration.
While Just-in-Time (JIT) VM access is an important hardening control—also provided through Defender for Cloud—it primarily reduces exposure by closing management ports and opening them only on request; it does not itself generate analytics-based brute-force alerts. Azure Firewall and Azure Application Gateway are perimeter controls (L3–L7 filtering and web application firewall, respectively) and do not provide host-level brute-force detection on VM sign-ins.
Therefore, the solution that directly satisfies the technical requirement to detect and alert on brute-force activity against Azure VMs—and integrates seamlessly with Sentinel for rapid remediation—is Azure Defender (Microsoft Defender for Cloud).
Reference: Microsoft Defender for Cloud documentation on VM threat protection and brute-force (RDP/SSH) detection and alerting, and integration with Microsoft Sentinel for incident creation and response.

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.



Answer:



Explanation:

Table: DeviceFileEvents

Aggregation function: count()

In Microsoft Defender XDR advanced hunting, data tables such as DeviceFileEvents, DeviceProcessEvents, and CloudAppEvents are used to investigate various types of activities. Since this query aims to investigate an issue related to file activity—specifically identifying when files have been accessed, modified, or created repeatedly—the correct data source table is DeviceFileEvents. This table contains information about file-level activities recorded by Defender for Endpoint sensors, including file path, file name, action type, and user account involved.

The KQL structure shown in the image follows standard hunting query syntax:

DeviceFileEvents

| where Timestamp > ago(2d)

| summarize activityCount = count() by FolderPath, FileName, ActionType, AccountDisplayName

| where activityCount > 5

Here's why:

The where Timestamp > ago(2d) clause filters results from the last 2 days, a typical timeframe for immediate investigations.

The summarize operator groups events by FolderPath, FileName, ActionType, and AccountDisplayName, then uses count() to determine how many times each file was acted upon.

Finally, where activityCount > 5 filters to show only unusually high-frequency activity, which might indicate suspicious or automated file manipulation.
Microsoft Defender XDR documentation highlights that DeviceFileEvents is the correct schema for file activity investigations, while DeviceProcessEvents focuses on process creation and execution, and CloudAppEvents targets cloud application usage.
Thus, the verified and documented correct completions are:
Table: DeviceFileEvents
Aggregation function: count()