Microsoft

SC-200

Microsoft Security Operations Analyst

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 28.4

Question: 1

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.

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

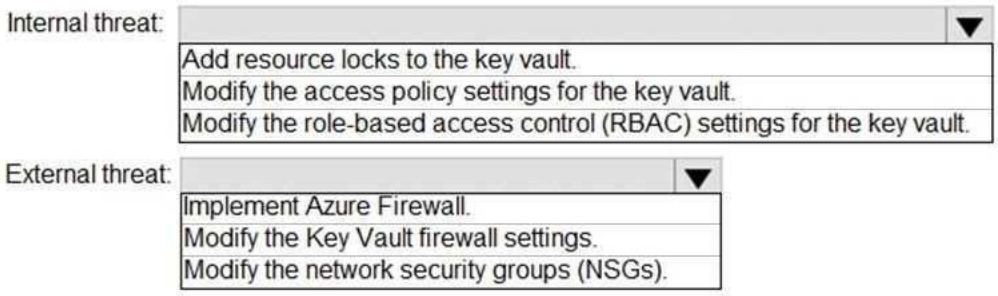
Explanation:
As outlined in Microsoft's official Defender for Office 365 documentation, this service provides

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.

Question: 3

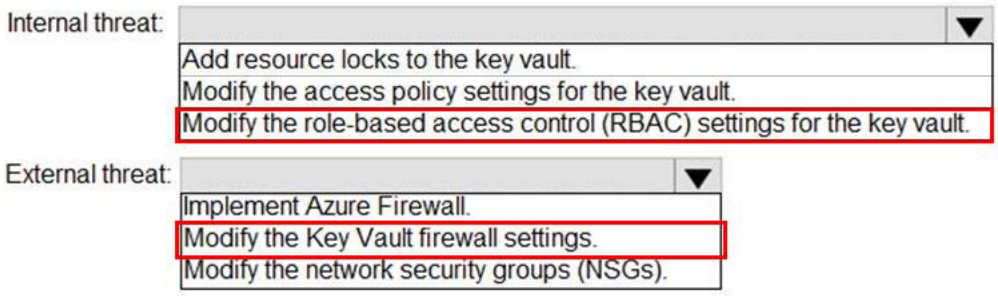
HOTSPOT
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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.

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?

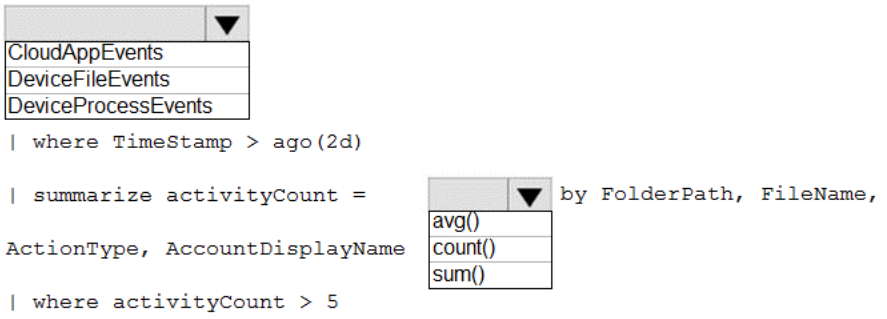
A. just-in-time (JIT) access
B. Azure Defender
C. Azure Firewall
D. Azure Application Gateway

Answer: B

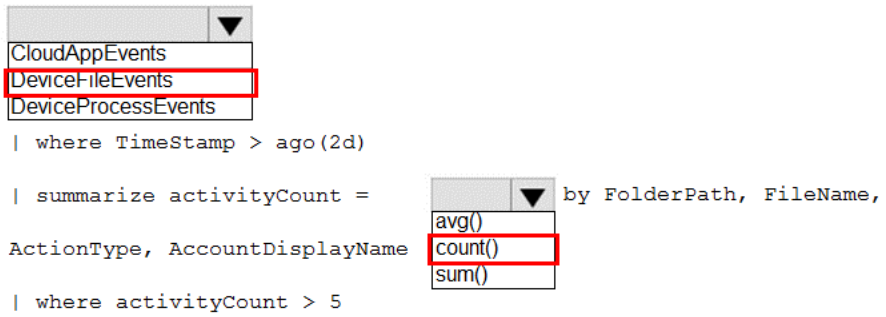
Explanation:
Reference:
To meet the requirement “Receive alerts if an Azure virtual machine is under brute force attack,” you should enable Azure Defender (now Microsoft Defender for Cloud plans for Servers). Defender continuously collects and analyzes security telemetry from your VMs (RDP/SSH sign-in 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 bruteforce 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.

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.



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()

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/