SC-100 Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze log, audit activity, and hunt for potential threats across all deployed services.

You need to recommend a solution for the customer. The solution must minimize costs.

What should you include in the recommendation?

A. Microsoft 365 Defender

B. Microsoft Defender for Cloud

C. Microsoft Defender for Cloud Apps

D. Microsoft Sentinel

Correct Answer: D

Microsoft Sentinel is a scalable, cloud-native solution that provides:

Security information and event management (SIEM)

Security orchestration, automation, and response (SOAR)

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Microsoft Sentinel is your bird\\'s-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously undetected threats, and minimize false positives using Microsoft\\'s analytics and unparalleled threat intelligence.

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Microsoft Sentinel natively incorporates proven Azure services, like Log Analytics and Logic Apps. Microsoft Sentinel enriches your investigation and detection with AI. It provides Microsoft\\'s threat intelligence stream and enables you to bring

your own threat intelligence.

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

QUESTION 2

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity.

You are informed about incidents that relate to compromised identities.

You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered.

Which Defender for Identity feature should you include in the recommendation?

A. sensitivity labels

B. custom user tags

C. standalone sensors

D. honeytoken entity tags

Correct Answer: D

Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.

Incorrect:

Not B: custom user tags

After you apply system tags or custom tags to users, you can use those tags as filters in alerts, reports, and investigation.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-identity/entity-tags

QUESTION 3

Your company is moving all on-premises workloads to Azure and Microsoft 365.

You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:

1.

Minimizes manual intervention by security operation analysts

2.

Supports triaging alerts within Microsoft Teams channels What should you include in the strategy?

A. KQL

B. playbooks

C. data connectors

D. KQLworkbooks

Correct Answer: B

Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.

A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to

specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.

Incorrect:

Not A: Kusto Query Language is a powerful tool to explore your data and discover patterns, identify anomalies and outliers, create statistical modeling, and more. The query uses schema entities that are organized in a hierarchy similar to

SQL\\'s: databases, tables, and columns.

Not D: Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive

experiences.

Workbooks allow users to visualize the active alerts related to their resources.

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

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

QUESTION 4

Your company is developing a new Azure App Service web app.

You are providing design assistance to verify the security of the web app.

You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection.

What should you include in the recommendation?

A. dynamic application security testing (DAST)

B. static application security testing (SAST)

C. interactive application security testing (IAST)

D. runtime application self-protection (RASP)

Correct Answer: A

Dynamic application security testing (DAST) is a process of testing an application in an operating state to find security vulnerabilities. DAST tools analyze programs while they are executing to find security vulnerabilities such as memory

corruption, insecure server configuration, cross-site scripting, user privilege issues, SQL injection, and other critical security concerns.

Incorrect:

Not B: SAST tools analyze source code or compiled versions of code when the code is not executing in order to find security flaws.

Not C: IAST (interactive application security testing) analyzes code for security vulnerabilities while the app is run by an automated test, human tester, or any activity “interacting” with the application functionality.

IAST works inside the application, which makes it different from both static analysis (SAST) and dynamic analysis (DAST). This type of testing also doesn\\'t test the entire application or codebase, but only whatever is exercised by the

functional test.

Not D: Runtime Application Self Protection (RASP) is a security solution designed to provide personalized protection to applications. It takes advantage of insight into an application\\'s internal data and state to enable it to identify threats at

runtime that may have otherwise been overlooked by other security solutions.

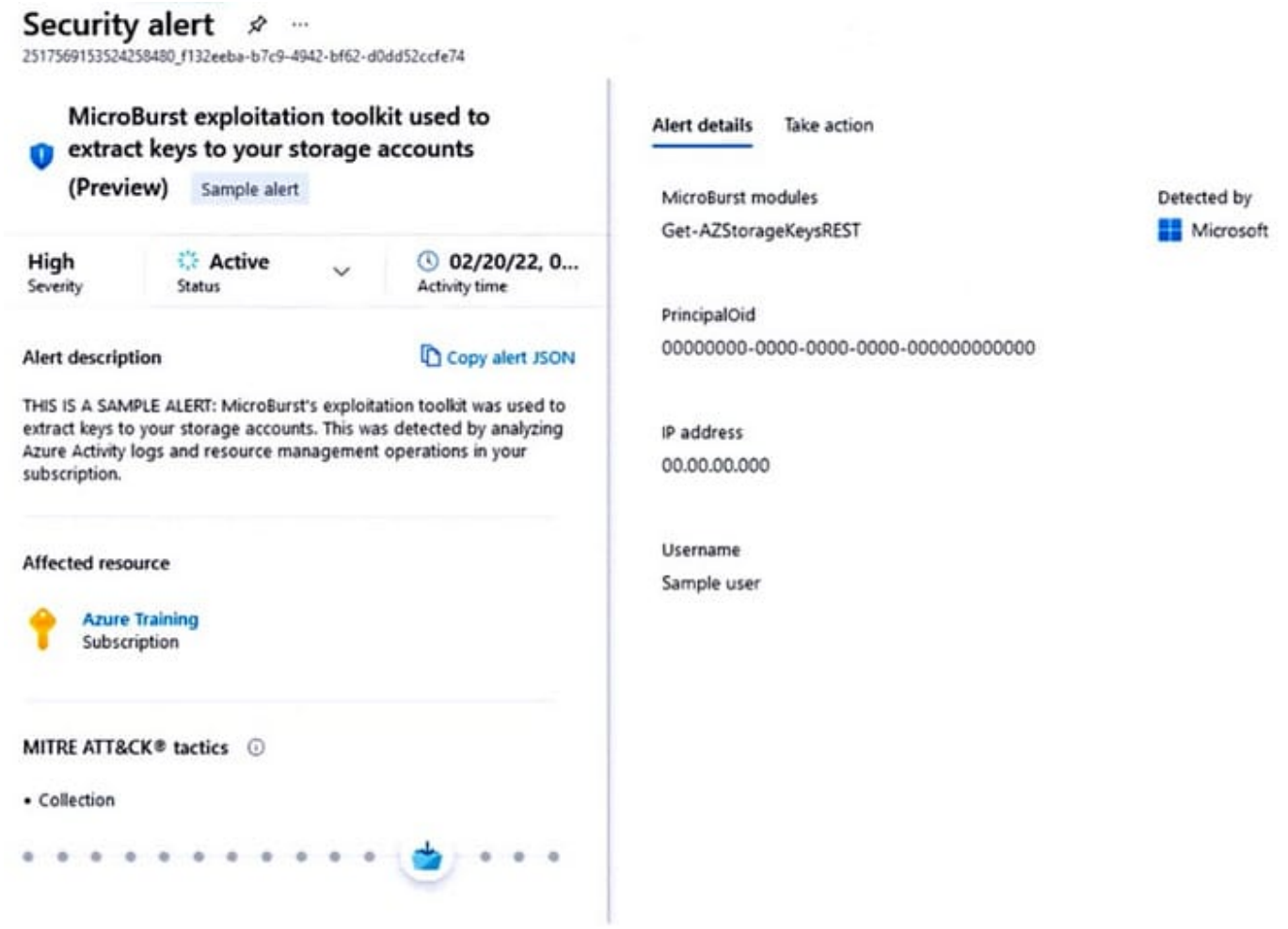
RASP\\'s focused monitoring makes it capable of detecting a wide range of threats, including zero-day attacks. Since RASP has insight into the internals of an application, it can detect behavioral changes that may have been caused by a novel

attack. This enables it to respond to even zero-day attacks based upon how they affect the target application.

Reference: https://docs.microsoft.com/en-us/azure/security/develop/secure-develop

QUESTION 5

You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



After remediating the threat which policy definition should you assign to prevent the threat from reoccurring?

A. Storage account public access should be disallowed

B. Azure Key Vault Managed HSM should have purge protection enabled

C. Storage accounts should prevent shared key access

D. Storage account keys should not be expired

Correct Answer: A

Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but may also present a security risk. It\\'s important to manage anonymous access judiciously and to understand how to evaluate anonymous access to your data. Operational complexity, human error, or malicious attack against data that is publicly accessible can result in costly data breaches. Microsoft recommends that you enable anonymous access only when necessary for your application scenario.

Note: Attackers have been crawling for public containers using tools such as MicroBurst.

Exploiting Anonymous Blob Access Now, there are thousands of articles explaining how this can be abused and how to search for insecure storage in Azure. One of the easiest way is to use MicroBurst, provide the storage account name to search for, and it'll check if the containers exists based on a wordlist saved in the Misc/permutations.txt

Reference: https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent

https://hackingthe.cloud/azure/anonymous-blob-access/