SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: A

How are regulatory compliance standards represented in Defender for Cloud?

Industry standards, regulatory standards, and benchmarks are represented in Defender for Cloud\\'s regulatory compliance dashboard. Each standard is an initiative defined in Azure Policy.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

QUESTION 2

HOTSPOT

You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure.

During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Threat modeling: [▼]
- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

Actionable intelligence: [▼]
- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

Dynamic application security testing (DAST): [▼]
- Build and test
- Commit the code
- Go to production
- Operate
- Plan and develop

Correct Answer:

Answer Area

Threat modeling:

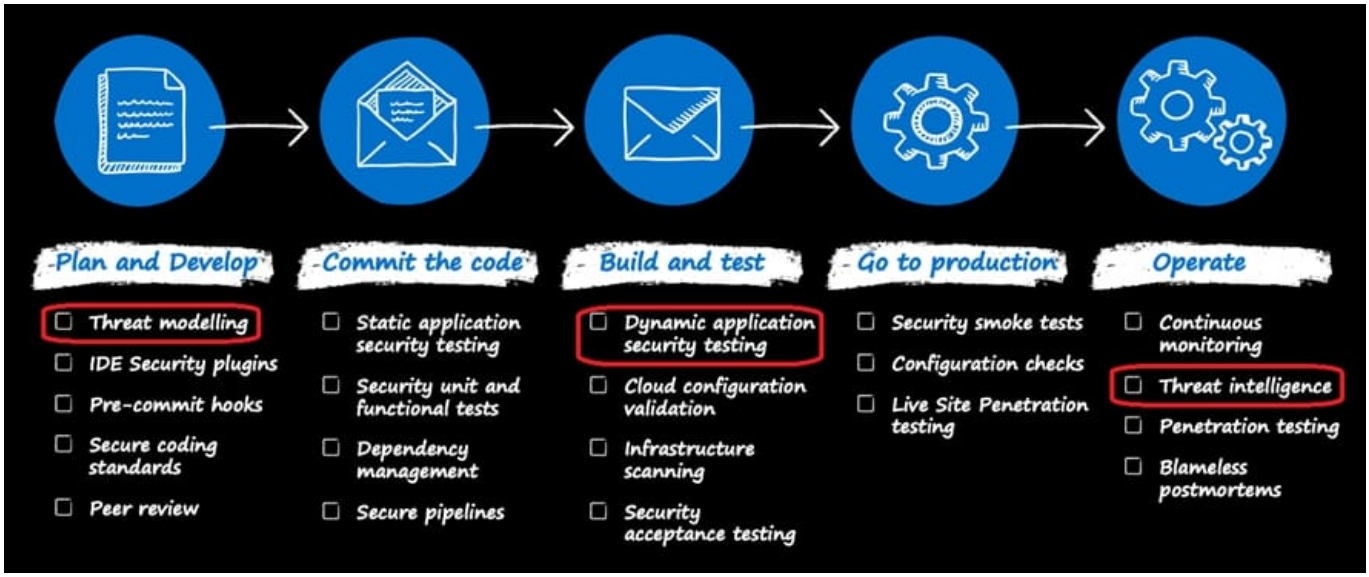
- Build and test
- Commit the code
- Go to production
- Operate
- **Plan and develop**

Actionable intelligence:

- Build and test
- Commit the code
- Go to production
- **Operate**
- Plan and develop

Dynamic application security testing (DAST):

- **Build and test**
- Commit the code
- Go to production
- Operate
- Plan and develop



Plan and develop

Box 1: Plan and develop

Typically, modern development follows an agile development methodology. Scrum is one implementation of agile methodology that has every sprint start with a planning activity. Introducing security into this part of the development process should focus on:

*

Threat modeling to view the application through the lens of a potential attacker

*

IDE security plug-ins and pre-commit hooks for lightweight static analysis checking within an integrated development environment (IDE).

*

Peer reviews and secure coding standards to identify effective security coding standards, peer review processes, and pre-commit hooks. It\\'s not mandatory to add all these steps. But each step helps reveal security issues early, when they\\'re much cheaper and easier to fix.

Box 2: Operate

Go to production and operate

When the solution goes to production, it\\'s vital to continue overseeing and managing the security state. At this stage in the process, it\\'s time to focus on the cloud infrastructure and overall application.

Configuration and infrastructure scanning

Penetration testing

Actionable intelligence

The tools and techniques in this guidance offer a holistic security model for organizations who want to move at pace and experiment with new technologies that aim to drive innovation. A key element of DevSecOps is data-driven, event-driven

processes. These processes help teams identify, evaluate, and respond to potential risks. Many organizations choose to integrate alerts and usage data into their IT service management (ITSM) platform. The team can then bring the same

structured workflow to security events that they use for other incidents and requests.

Box 3: Build and test

Build and test

Many organizations use build and release pipelines to automate and standardize the processes for building and deploying code. Release pipelines let development teams make iterative changes to sections of code quickly and at scale. The

teams won\\'t need to spend large amounts of time redeploying or upgrading existing environments.

Using release pipelines also lets teams promote code from development environments, through testing environments, and ultimately into production. As part of automation, development teams should include security tools that run scripted,

automated tests when deploying code into testing environments. The tests should include unit testing on application features to check for vulnerabilities or public endpoints. Testing ensures intentional access.

Dynamic application security testing (DAST)

In a classical waterfall development model, security was typically introduced at the last step, right before going to production. One of the most popular security approaches is penetration testing or pen testing. Penetration testing lets a team

look at the application from a black-box security perspective, as in, closest to an attacker mindset.

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-devops-security

QUESTION 3

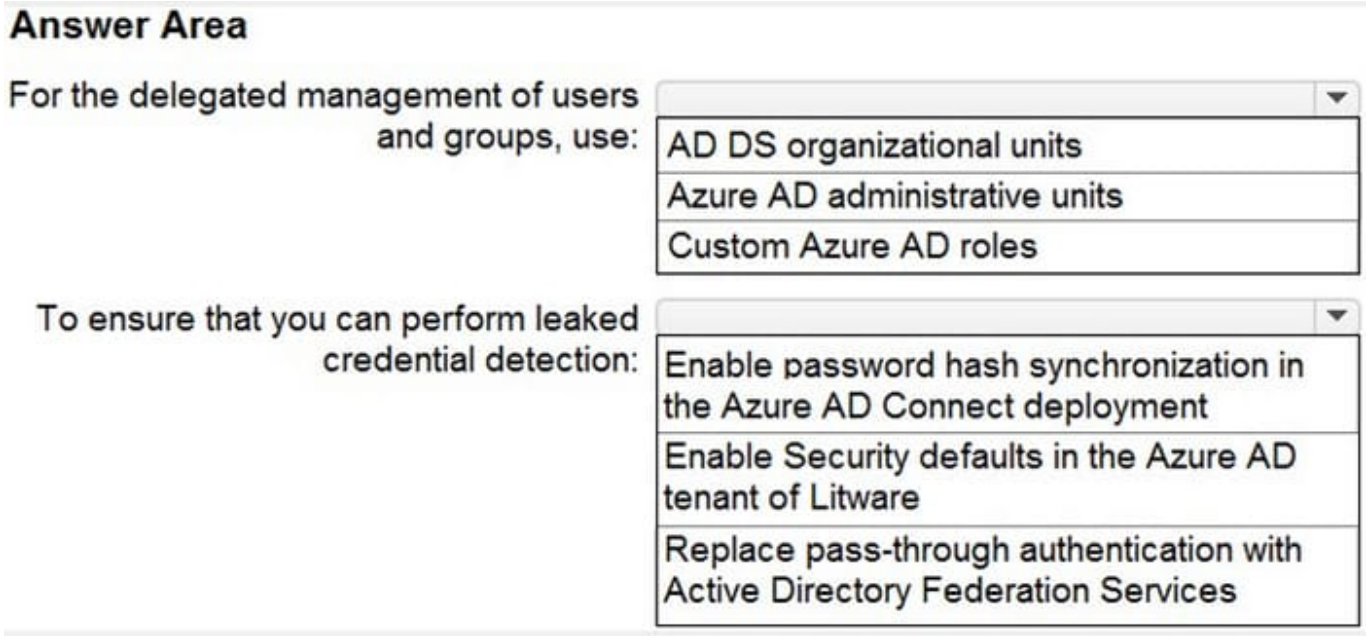
HOTSPOT

You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

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

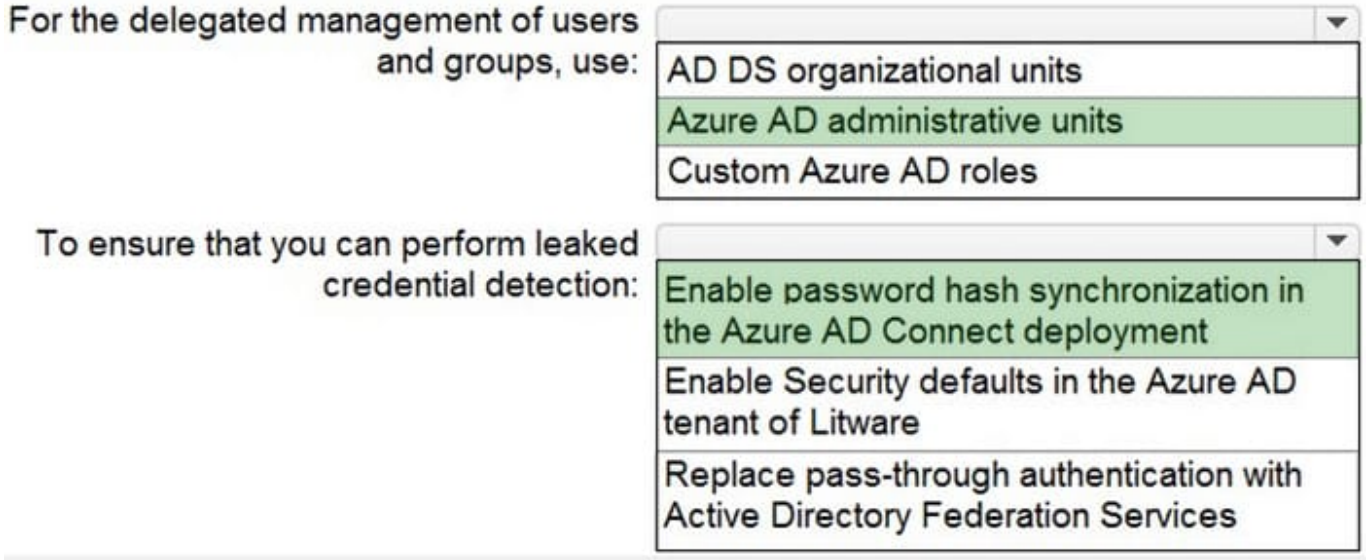
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Box 1: Azure AD administrative units

Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:

* The delegation of user management based on business units

Without Azure AD administrative units, assigning a user to the User Administrator role in Azure AD gives them rights to manage all Azure AD users. With administrative units, the user is delegated the same role, User Administrator, but that role only applies to the specified administrative unit. The administrative unit contains the users and groups that are under the scope of management. Box 2: Enable password hash synchronization in the Azure AD Connect deployment Existing environment: Azure AD Connect is used to implement pass-through authentication. Password hash synchronization

Risk detections like leaked credentials require the presence of password hashes for detection to occur.

Reference: https://4sysops.com/archives/an-introduction-to-azure-ad-administrative-units/

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization

QUESTION 4

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription. The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

A. From Microsoft Defender for Endpoint, perform a security scan.

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. Disable Microsoft OneDrive sync and Exchange ActiveSync.

Correct Answer: D

The following containment steps can be done concurrently as new threat vectors are discovered.

Step 1: Assess the scope of the situation

Which user accounts were compromised?

Which devices are affected? Which applications are affected? Step 2: Preserve existing systems

*

Disable all privileged user accounts except for a small number of accounts used by your admins to assist in resetting the integrity of your AD DS infrastructure. If a user account is believed to be compromised, disable it immediately.

*

Isolate compromised systems from the network, but do not shut them off.

*

Etc.

Note:

With OneDrive, you can sync files between your computer and the cloud, so you can get to your files from anywhere - your computer, your mobile device, and even through the OneDrive website at OneDrive.com.

ActiveSync is a client protocol that lets users synchronize their Exchange mailbox with a mobile device.

Reference: https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

QUESTION 5

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