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

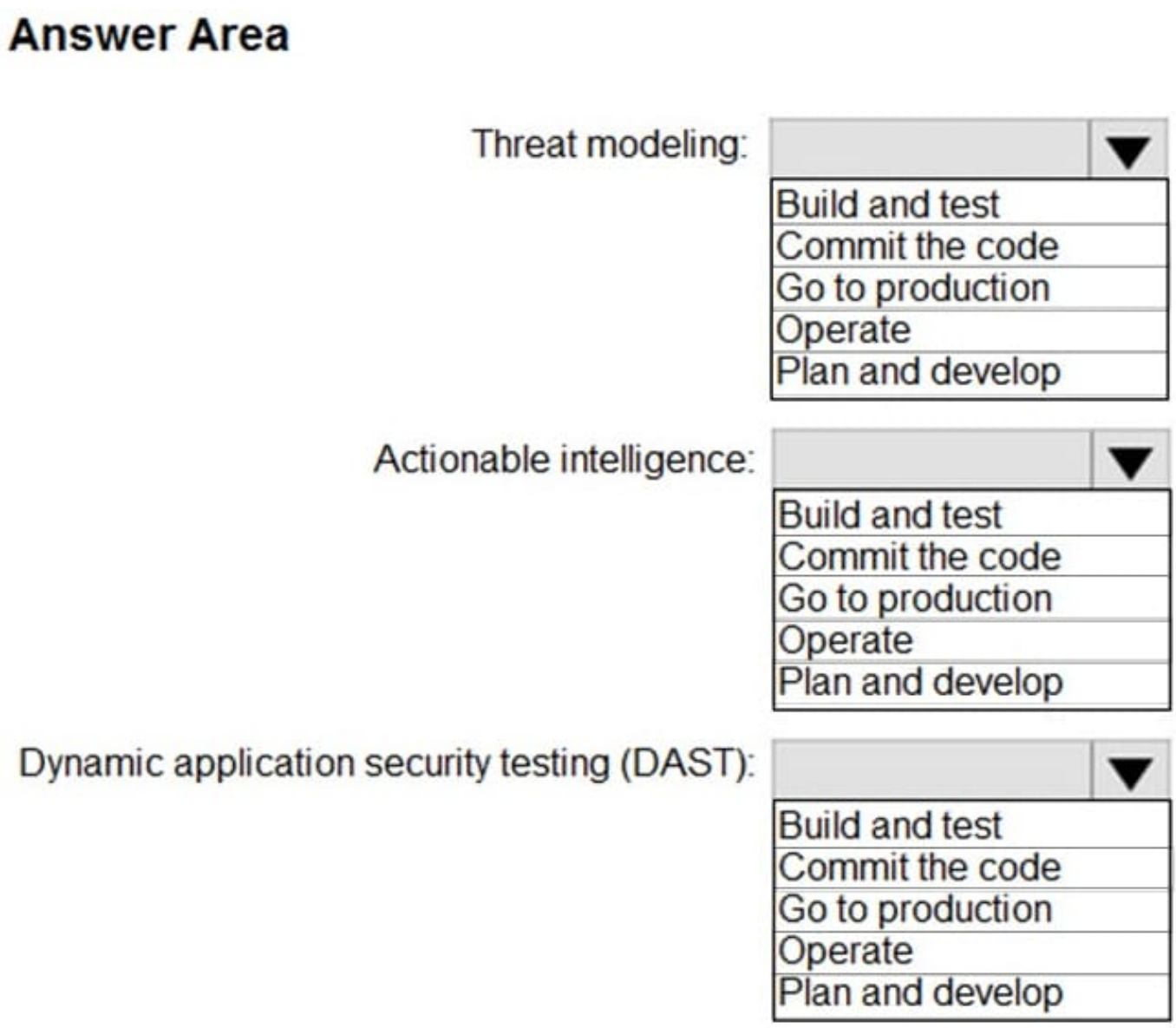
HOTSPOT

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:



Correct Answer:

Answer Area

Threat modeling:

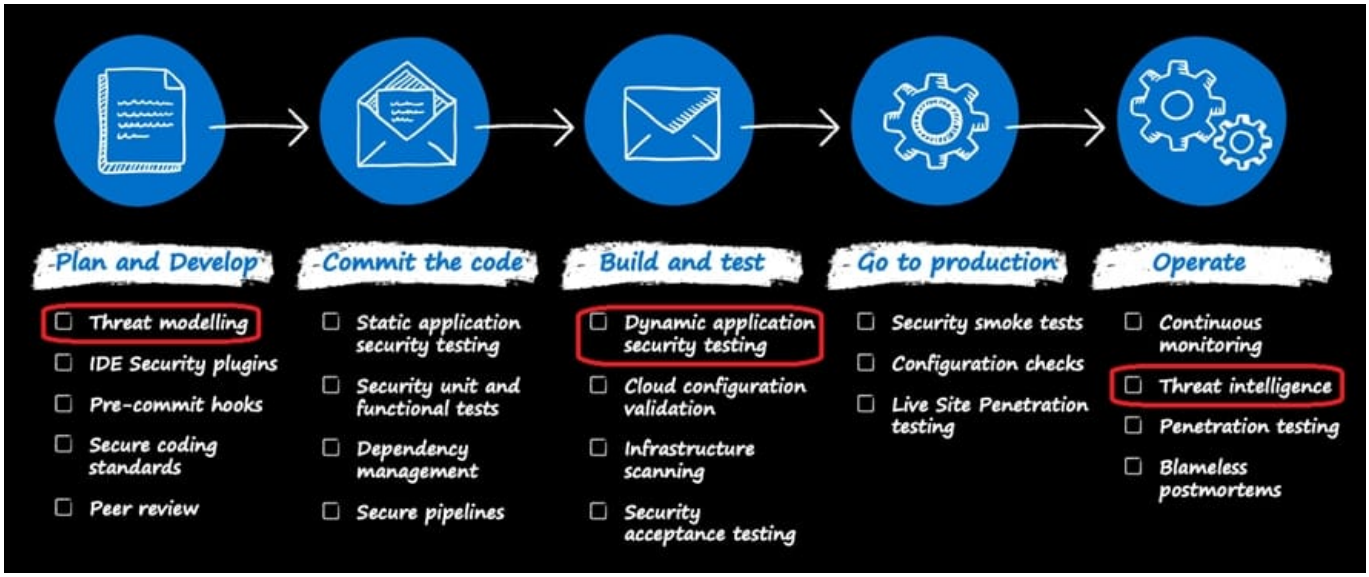
- Build and test
- Commit the code
- Go to production
- Operate
- **Plan and develop**

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 2

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

You have an Amazon Web Services (AWS) implementation.

You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc.

Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Containers

B. Microsoft Defender for servers

C. Azure Active Directory (Azure AD) Conditional Access

D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

E. Azure Policy

Correct Answer: ACE

Environment settings page (in preview) (recommended) - This preview page provides a greatly improved, simpler, onboarding experience (including auto provisioning). This mechanism also extends Defender for Cloud\\'s enhanced security features to your AWS resources:

*(A) Microsoft Defender for Containers brings threat detection and advanced defenses to your Amazon EKS clusters. This plan includes Kubernetes threat protection, behavioral analytics, Kubernetes best practices, admission control recommendations and more.

* Microsoft Defender for Servers, though it requires Arc.

C: AWS installations can benefit from Conditional Access. Defender for Cloud Apps integrates with Azure AD Conditional Access to enforce additional restrictions, and monitors and protects sessions after sign-in. Defender for Cloud Apps

uses user behavior analytics (UBA) and other AWS APIs to monitor sessions and users and to support information protection.

E: Kubernetes data plane hardening.

For a bundle of recommendations to protect the workloads of your Kubernetes containers, install the Azure Policy for Kubernetes. You can also auto deploy this component as explained in enable auto provisioning of agents and extensions.

With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure to enforce the best practices and

mandate them for future workloads.

Incorrect:

Not B: To enable the Defender for Servers plan you need Azure Arc for servers installed on your EC2 instances.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

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

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-security-solutions

QUESTION 3

You have a Microsoft 365 subscription.

You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.

Which two services should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. Azure Data Catalog

C. Microsoft Purview Information Protection

D. Azure AD Application Proxy

E. Microsoft Defender for Cloud Apps

Correct Answer: AE

Explanation:

Blocking or limiting access on unmanaged devices relies on Azure AD conditional access policies.

Create a block download policy for unmanaged devices

Defender for Cloud Apps session policies allow you to restrict a session based on device state. To accomplish control of

a session using its device as a condition, create both a conditional access policy AND a session policy.

Incorrect:

Not B: Azure Data Catalog is an enterprise-wide metadata catalog that makes data asset discovery straightforward. It\\'s a fully-managed service that lets you — from analyst to data scientist to data developer — register, enrich, discover,

understand, and consume data sources.

Not C: Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.

Reference:

https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

https://learn.microsoft.com/en-us/defender-cloud-apps/use-case-proxy-block-session-aad

---

QUESTION 4

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. a managed identity in Azure

B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

C. a group managed service account (gMSA)

D. an Azure AD user account that has a password stored in Azure Key Vault

Correct Answer: D

QUESTION 5

You have an Azure subscription that contains virtual machines.

Port 3389 and port 22 are disabled for outside access.

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

1.

Prevent the need to enable ports 3389 and 22 from the internet.

2.

Only provide permission to connect the virtual machines when required.

3.

Ensure that administrators use the Azure portal to connect to the virtual machines.

Which two actions should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure Azure VPN Gateway.

B. Enable Just Enough Administration (JEA).

C. Configure Azure Bastion.

D. Enable just-in-time (JIT) VM access.

E. Enable Azure AD Privileged Identity Management (PIM) roles as virtual machine contributors.

Correct Answer: CD

C: Bastion provides secure remote access.

It uses RDP/SSH session is over TLS on port 443.

Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network.

It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don\\'t need a public IP address, agent, or special client

software.

D: Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud\\'s just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect

to a VM.

Meets the requirement: Only provide permission to connect the virtual machines when required

Incorrect:

Not B: Does not address: Only provide permission to connect the virtual machines when required

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell. With JEA, you can:

Reduce the number of administrators on your machines using virtual accounts or group-managed service accounts to perform privileged actions on behalf of regular users.

Limit what users can do by specifying which cmdlets, functions, and external commands they can run.

Better understand what your users are doing with transcripts and logs that show you exactly which commands a user executed during their session.

Not E: Does not help with the remote access.

Note: Classic Virtual Machine Contributor: Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they\\'re connected to.

Reference: https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles