

# SC-100 Microsoft Cybersecurity Architect

## Practice Questions

[SC-100: Microsoft Cybersecurity Architect \(Pearson Practice Test\) - O'Reilly Online Learning \(oreilly.com\)](#)

### Contents

- Objective 1: Design a Zero Trust strategy and architecture ..... 2
  - 1. Factors included in Conditional Access ..... 2
  - 2. Entitle Management ..... 3
  - 3. The Cloud Adoption Framework (CAF)..... 3
  - 4. Microsoft Sentinel – Enable relevant data connectors ..... 4
  - 5. Azure Arc ..... 4
  - 6. Entitle Management ..... 5
  - 7. Microsoft Cybersecurity Reference Architecture (MCRA)..... 5
  - 8. Network Security Groups ..... 6
  - 9. Application Insights ..... 6
  - 10. Activity Logs track changes that are made to Azure resources..... 6
  - 11. DMZ..... 7
  - 12. The mean time to acknowledge (MTTA) ..... 7
  - 13. Designing security with resiliency in mind ..... 8
  - 14. Defender for Cloud..... 8
  - 15. Logging Categories ..... 9
  - 16. Network Watcher ..... 9
  - 17. Conditional Access ..... 10
  - 18. Workflow automation tools ..... 11
  - 19. Zero Trust Rapid Modernization Plan (RaMP) components ..... 11
  - 20. Azure AD Privileged Identity Management includes the ability to create access reviews..... 12
  - 21. Privileged Identity Management..... 12
  - 22. The mean time to remediate (MTTR) ..... 13
  - 23. Access Packages ..... 13
  - 24. Foundational design principles included in a Zero Trust architecture ..... 13
  - 25. Azure Logic Apps is a resource type that allows you to create and run workflows ..... 14

26. The Defender for Cloud Secure Score .....	14
27. Azure AD DS requires the use of Azure AD password hash synchronization with Azure AD Connect. .....	15
28. The company security policy states that authentication for cloud services must occur in the cloud. .....	15
29. Azure AD Pass-through Authentication.....	15
30. You are designing a hub and spoke network architecture for an Azure environment.....	16
31. Access reviews enable administrators and group owners to review membership and privileged role activation.....	16
32. A firewall can act as a Layer 7 IDS .....	17
33. Zero Trust principles.....	18
34. Report Reader .....	18
35. Azure Policy.....	19
36. Federated Authentication .....	19

## Objective 1: Design a Zero Trust strategy and architecture

### 1. Factors included in Conditional Access

Question 1 of 36

Question Id : SC-100-CP-1-030

Which two factors can be included when configuring a conditional access policy?

- Data loss prevention
- Device compliance state
- Multifactor authentication
- Network security groups

Select 2 answers

You answered this question correctly.

**Explanation:**

Conditional access policies can include both user and device requirements that can then grant or deny a user access to a cloud application.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/5-secure-conditional-access>

## 2. Entitle Management

Question 2 of 36

Question Id : SC-100-CP-1-036

You are planning to review the membership and permissions to an access package assignment. What should you use?

- Conditional access
- Entitlement management
- Identity Protection
- Privileged Identity Management

You answered this question correctly. ×

**Explanation:**

Access packages are created and reviewed using entitlement manager.

Review: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/7-define-identity-governance-for-access-reviews-entitlement-management>

## 3. The Cloud Adoption Framework (CAF)

Question 3 of 36

Question Id : SC-100-CP-1-005

The **Cloud Adoption Framework** provides best practices, tools, and documentation for using the cloud.

Possible answers : **Cloud Adoption Framework,CAF**

You answered this question correctly. ×

**Explanation:**

The Cloud Adoption Framework (CAF) provides best practices, tools, and documentation for using the cloud.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/4-develop-security-requirements-based-business-goals>

## 4. Microsoft Sentinel – Enable relevant data connectors

Question 4 of 36

Question Id : SC-100-CP-1-021

You are planning to use Microsoft Sentinel for visibility, automation, and orchestration of security monitoring. You need to ensure that you can establish visibility of third-party virtual appliances in Sentinel. What should you do?

Create an automation rule.

Create a playbook.

Enable incident notifications.

Enable relevant data connectors.

You answered this question correctly. ×

**Explanation:**

To ensure visibility into third-party events and monitoring, the relevant data connector must be configured so that data is captured into the underlying Log Analytics workspace.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/5-design-strategy-security-information-event-management>

## 5. Azure Arc

Which Azure service provides centralized management of Azure and on-premises resources?

Azure Arc

Azure Active Directory

Azure Lighthouse

Azure Policy

You answered this question correctly. ×

**Explanation:**

Azure Arc provides hybrid management of resources, whether they are in Azure, on premises, or in other cloud environments.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/7-design-for-hybrid-multi-tenant-environments>

## 6. Entitle Management

You are planning an identity strategy and need to simplify the onboarding of new user accounts. New accounts should have a bundle of appropriate permissions based on the department they are joining. What should you use?

- Conditional access
- Entitlement management
- Identity protection
- Privileged Identity Management

You answered this question correctly. ×

**Explanation:**

Entitlement management includes the ability to create access packages, which can be used to bundle group and permission membership for new and external users.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/7-define-identity-governance-for-access-reviews-entitlement-management>

## 7. Microsoft Cybersecurity Reference Architecture (MCRA)

Which Microsoft guidance describes how security capabilities integrate with other services and applications?

- Cloud Adoption Framework (CAF)
- Microsoft Cybersecurity Reference Architectures (MCRA)
- Well-Architected Framework
- Zero Trust Architecture

You answered this question correctly. ×

**Explanation:**

The Microsoft Cybersecurity Reference Architectures (MCRA) describes how Microsoft security capabilities integrate with Microsoft services, including Azure and Office 365, as well as third-party applications.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/3-develop-integration-points-architecture>

## 8. Network Security Groups

You are designing the security architecture of an Azure virtual network and subnets in a hub and spoke configuration. You need to provide Layer 4 security between subnets to restrict certain types of traffic. What should you use?

- Application security groups
- Host groups
- Network security groups
- Proximity placement groups

You answered this question correctly. ×

**Explanation:**

You should include network security groups between the subnets in order to filter traffic based on protocol, port, or IP address.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/8-design-technical-governance-strategies-for-traffic-filtering-segmentation>

## 9. Application Insights

Question 9 of 36

Question Id : SC-100-CP-1-017

You are planning the logging strategy for an application. You need to collect performance monitoring and custom diagnostics from the application. Which service logs should you use?

- Activity logging
- Application Insights
- Azure Active Directory
- Resource logging

You answered this question correctly. ×

**Explanation:**

Azure Application Insight allows developers to capture exceptions and custom diagnostics for an application running on Azure.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/3-design-log-audit-security-strategy>

## 10. Activity Logs track changes that are made to Azure resources

You are planning the logging strategy for an application. You need to ensure that you can track change operations to resources deployed in your Azure subscription. Which logs should you monitor?

- Activity logs
- Application insight logs
- Azure Active Directory logs
- Resource logs

You answered this question correctly. x

**Explanation:**

The Azure activity logs track changes that are made to Azure resources within a subscription at the control plane level.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/3-design-log-audit-security-strategy>

## 11. DMZ

A  is a type of network that exists between the Internet and a hub network to provide security segmentation between the two environments.

Possible answers :

You answered this question correctly. x

**Explanation:**

A DMZ or perimeter network is a type of network that exists between the Internet and a hub network that typically includes security services, such as a firewall, to protect the hub network from Internet traffic.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/8-design-technical-governance-strategies-for-traffic-filtering-segmentation>

In this context the Hub Network is the LAN.

## 12. The mean time to acknowledge (MTTA)

The  is the time between receiving an alert and a security analyst beginning their investigation.

Possible answers :

You answered this question correctly. x

**Explanation:**

The mean time to acknowledge (MTTA) is how a security operations team measures the time between when systems generate an alert and the time that a security analyst begins their investigation of that alert.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/2-understand-frameworks-processes-procedures>

### 13. Designing security with resiliency in mind

When designing security with resiliency in mind, which two goals should be included?

- Isolate all business functions.
- Isolate all technical functions.
- Prevent further damage.
- Protect critical operations.

Select 2 answers

You answered this question correctly. x

**Explanation:**

During an incident, it is important to prevent further damage to the environment and protect the critical operations of the business.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/6-design-security-for-resiliency-strategy>

### 14. Defender for Cloud

You plan to deploy on Azure an application that meets PCI compliance. As part of the solution, you need to be able to create alerts and automate notifications based on this compliance. What should you use?

- Defender for Cloud
- Log Analytics
- Logic Apps
- Microsoft Sentinel

You answered this question correctly. x

**Explanation:**

Defender for Cloud enables you to monitor the security posture of your Azure subscription based on the Microsoft Cloud Security Benchmark as well regulatory compliance standards, including those for PCI compliance.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/5-design-strategy-security-information-event-management>



## 15. Logging Categories

Drag the Azure logging category on the left to the correct definition on the right.

### Correct Answers

Activity logs

Azure Active Directory reporting

Resource logs

Application Insights

### Matching items here:

Change tracking for actions performed on resources deployed to Azure

Activity logs ✓

User sign-in activities

Azure Active Directory reporting ✓

Tracks operations that were performed by the individual Azure resource

Resource logs ✓

Application performance monitoring service for web developers

Application Insights ✓

You answered this question correctly. ×

#### Explanation:

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/3-design-log-audit-security-strategy>

## 16. Network Watcher

You manage a hybrid Azure/on-premises environment that is connected using a virtual private network (VPN). The VPN tunnel has failed, and you need to diagnose the connection issues. What should you use?

- Diagnostic logging
- Log Analytics
- Network Security Group flow logs

Network Watcher

You answered this question correctly. ×

#### Explanation:

The Network Watcher service includes a tool that provides VPN connection troubleshooting. This service can be used to diagnose IPsec and L2TP VPN tunnel connection issues.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/5-design-strategy-security-information-event-management>

[\(151\) What is Network Watcher and How Did It Get In My Subscription! - YouTube](#)

### Azure services



Network Watcher

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 16 of 16 records.

Name	Subscription	Location	Resource group
NetworkWatcher_centralus	Microsoft Azure Sponsorship	Central US	NetworkWatcherRG
NetworkWatcher_centralus	Visual Studio Enterprise Subscr--	Central US	NetworkWatcherRG
NetworkWatcher_centralus	Pay-As-You-Go (MSDN)	Central US	NetworkWatcherRG
NetworkWatcher_eastus	Microsoft Azure Sponsorship	East US	NetworkWatcherRG
NetworkWatcher_eastus	Pay-As-You-Go (MSDN)	East US	NetworkWatcherRG
NetworkWatcher_eastus2	Microsoft Azure Sponsorship	East US 2	NetworkWatcherRG
NetworkWatcher_northeurope	Microsoft Azure Sponsorship	North Europe	NetworkWatcherRG
NetworkWatcher_northeurope	Visual Studio Enterprise Subscr--	North Europe	NetworkWatcherRG
NetworkWatcher_southcentralus	Microsoft Azure Sponsorship	South Central US	NetworkWatcherRG
NetworkWatcher_southeastasia	Pay-As-You-Go (MSDN)	Southeast Asia	NetworkWatcherRG
NetworkWatcher_westeurope	Microsoft Azure Sponsorship	West Europe	NetworkWatcherRG
NetworkWatcher_westus	Microsoft Azure Sponsorship	West US	NetworkWatcherRG
NetworkWatcher_westus	Pay-As-You-Go (MSDN)	West US	NetworkWatcherRG

## 17. Conditional Access

Question 17 of 36

Question Id : SC-100-CP-1-029

Conditional access provide(s) the ability to grant or deny access to cloud applications based on multiple requirements.

Possible answers : Conditional access, Conditional access policies

You answered this question correctly.

**Explanation:**

Conditional access allows you to create policies that specify multiple policies for the authentication process to succeed or require additional conditions to be met to allow a user to connect.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/5-secure-conditional-access>

## 18. Workflow automation tools

Drag the workflow automation tool on the left to the correct definition on the right.

### Correct Answers

Azure Logic Apps

Microsoft Defender for Cloud

Microsoft Sentinel

### Matching items here:

Provides designer-based workflow automation using connectors.

**Azure Logic Apps** ✓

Can trigger workflow automation based on changes to regulatory compliance.

**Microsoft Defender for Cloud** ✓

Provides automation rules and playbooks to facilitate incident management and orchestrated response.

**Microsoft Sentinel** ✓

You answered this question correctly. ×

### Explanation:

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/6-evaluate-security-workflows>

## 19. Zero Trust Rapid Modernization Plan (RaMP) components

You are designing the security architecture for a hybrid environment with Azure and on-premises resources. You need to include the Zero Trust Rapid Modernization Plan (RaMP) components in your design. What should you use?

Cloud Adoption Framework (CAF)

Microsoft Cybersecurity Reference Architectures (MCRA)

Well-Architected Framework

Zero-Trust Architecture

You answered this question correctly. ×

### Explanation:

The Microsoft Cybersecurity Reference Architectures includes the Rapid Modernization Plan (RaMP), which includes specifics on security operations for a Zero Trust environment.

## 20. Azure AD Privileged Identity Management includes the ability to create access reviews

You are planning to review the privileged access of Azure resource roles. What should you use to create the access review?

- Conditional access
- Entitlement management
- Identity Protection

Privileged Identity Management

You answered this question correctly. ×

**Explanation:**

Azure AD Privileged Identity Management includes the ability to create access reviews for Azure resource and Azure Active Directory role assignments.

Review: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/7-define-identity-governance-for-access-reviews-entitlement-management>

## 21. Privileged Identity Management

You are planning a privileged identity strategy and need to ensure that privileged accounts have elevated permissions for only a specific period of time. What should you use?

- Conditional access
- Custom attributes
- Identity Protection

Privileged Identity Management

You answered this question correctly. ×

**Explanation:**

Privileged Identity Management allows you to make roles eligible for assignment and then, when they are activated, the roles are only assigned for a configurable amount of time.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/6-design-strategy-for-role-assignment-delegation>

## 22. The mean time to remediate (MTTR)

The **mean time to remediate** is the time between a security analyst beginning their investigation and when the incident is remediated.

Possible answers : **mean time to remediate,MTTR,time to remediate,time to resolution,mean time to resolution**

You answered this question correctly. ×

**Explanation:**

The mean time to remediate (MTTR) is the time period between when an analyst begins their investigation into an incident and when that incident has been remediated.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/2-understand-frameworks-processes-procedures>

## 23. Access Packages

A(n) **Access Package** is a feature of entitlement management that allows you to bundle group membership and application assignments together.

Possible answers :

You answered this question correctly. ×

**Explanation:**

Access packages are a feature of entitlement management that allow you to bundle group membership and application assignments together with policies and workflow approvals.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/7-define-identity-governance-for-access-reviews-entitlement-management>

## 24. Foundational design principles included in a Zero Trust architecture

Which two **foundational design principles** are included in a Zero Trust architecture?

Assume breach

Defense in depth

Multifactor authentication

Verify explicitly

Select 2 answers

You answered this question correctly. ×

**Explanation:**

The three foundational principles of a Zero Trust architecture include are verify explicitly, use least-privilege access, and assume breach. Defense in depth and MFA might be components of the security architecture, but they are not specifically part of Zero Trust.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/2-zero-trust-overview>

## 25. Azure Logic Apps is a resource type that allows you to create and run workflows

You are planning to automate the notification workflow for new Azure resource events, and you need to identify a platform for creating and running workflows. What should you use?

Defender for Cloud

Graph API

Logic Apps

Sentinel

You answered this question correctly. ×

**Explanation:**

Azure Logic Apps is a resource type that allows you to create and run workflows that you design and create.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/6-evaluate-security-workflows>

## 26. The Defender for Cloud Secure Score

A(n)  provides a numerical value of the current configuration of resources in a subscription compared against the Center for Internet Security controls and external benchmarks.

**Possible answers :**

You answered this question correctly. ×

**Explanation:**

The Defender for Cloud Secure Score measures the existing configuration of resources against the Microsoft Cloud Security Benchmark and the Center for Internet Security controls to provide a point-in-time reference for how these resources are configured, with security in mind.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/5-design-strategy-security-information-event-management>

## 27. Azure AD DS requires the use of Azure AD password hash synchronization with Azure AD Connect.

You are planning a hybrid on-premises/Azure authentication strategy. The company plans to use Azure Active Directory Domain Services (Azure AD DS) and synchronize it with Azure Active Directory. Which cloud authentication method should you use?

Azure AD cloud-only users

Azure AD password hash synchronization

Azure AD Pass-through Authentication

Federated authentication

You answered this question correctly. ×

**Explanation:**

Azure AD DS requires the use of Azure AD password hash synchronization with Azure AD Connect. This allows the Azure AD DS service to synchronize with Azure AD.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

## 28. The company security policy states that authentication for cloud services must occur in the cloud.

You are planning a hybrid on-premises/Azure authentication strategy. The company security policy states that authentication for cloud services must occur in the cloud. Which cloud authentication method should you use?

Azure AD cloud-only users

Azure AD password hash synchronization

Azure AD Pass-through Authentication

Federated authentication

You answered this question correctly. ×

**Explanation:**

To allow the authentication to stay in the cloud and not be transferred elsewhere, the password of the user account must be synchronized using Azure AD password hash synchronization.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

## 29. Azure AD Pass-through Authentication

It requires an agent in the on-premises environment to perform the authentication with the local Active Directory domain controllers.

You are planning a hybrid on-premises/Azure authentication strategy. The company's security policy states that authentication must be performed in the on-premises Active Directory environment. Which cloud authentication method should you use?

- Azure AD cloud-only users
- Azure AD password hash synchronization
- Azure AD Pass-through Authentication
- Federated authentication

You answered this question correctly. ×

**Explanation:**

Azure AD Pass-through Authentication requires an agent in the on-premises environment to perform the authentication with the local Active Directory domain controllers.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

### 30. You are designing a hub and spoke network architecture for an Azure environment.

You are designing a hub and spoke network architecture for an Azure environment. You need to identify an available address space to use with the virtual networks. Which two address spaces can you assign to an Azure virtual network?

- 10.10.0.0/16
- 169.254.0.0/16
- 172.16.0.0/16
- 172.50.0.0/16

Select 2 answers

You answered this question correctly. ×

**Explanation:**

The address spaces 10.10.0.0/16 and 172.16.0.0/16 fall into the RFC 1918 address ranges for private IP addresses and can be used with Azure virtual networks.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/8-design-technical-governance-strategies-for-traffic-filtering-segmentation>

### 31. Access reviews enable administrators and group owners to review membership and privileged role activation



A(n)  provides a way to ensure that only accounts that need access to a resource are members of a privileged group.

Possible answers :

You answered this question correctly. ×

**Explanation:**

An access review enables administrators and group owners to review membership and privileged role activation to ensure that users do not have excessive permissions over time.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/7-define-identity-governance-for-access-reviews-entitlement-management>

### 32. A firewall can act as a Layer 7 IDS

You are designing a hybrid Azure/on-premises network. You need to ensure that all traffic traverses an intrusion detection system (IDS). What should you include in the design?

- Application gateway
- ExpressRoute
- Firewall
- Virtual network gateway

You answered this question correctly. ×

**Explanation:**

A firewall can act as a Layer 7 IDS. An application gateway only has a web application firewall and does not provide full IDS services. ExpressRoute and virtual network gateways do not provide any IDS capabilities.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/7-design-for-hybrid-multi-tenant-environmentsrr>

### 33. Zero Trust principles

You are designing an architecture that follows the principles of Zero Trust. Drag the Zero Trust principle on the left to the correct definition on the right.

#### Correct Answers

Verify explicitly

Use least-privilege access

Assume breach

#### Matching items here:

Authenticate and authorize based on all available data points.

Verify explicitly ✓

Restrict access using just-in-time access.

Use least-privilege access ✓

Minimize segment access and blast radius.

Assume breach ✓

You answered this question correctly. ×

#### Explanation:

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/2-zero-trust-overview>

### 34. Report Reader

You need to ensure that a security analyst can read the audit activity report in Azure AD. The analyst must not have more permissions than necessary to read the Azure AD audit logs. Which role should you assign to the analyst?

Report Reader

Global Reader

Security Administrator

Global Administrator

You answered this question correctly. ×

#### Explanation:

All four roles listed provide the ability to read the Azure AD audit log. However, the role that provides least privilege from those available is the Report Reader. All other roles would also allow read and/or change access to other audit logs and security configurations.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/3-design-log-audit-security-strategy>

### 35. Azure Policy

Which Azure service provides methods to implement and manage governance, compliance reporting, security, and cost management?

- Azure Arc
- Azure Active Directory
- Azure Lighthouse
- Azure Policy

You answered this question correctly. ×

**Explanation:**  
Azure Policy provides a way to implement and require resources to meet governance guidelines, enforce consistent deployments, and help organizations achieve regulatory compliance.  
Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/7-design-for-hybrid-multi-tenant-environments>

### 36. Federated Authentication

You are planning a hybrid authentication strategy using a third-party service for multifactor authentication. Which cloud authentication method should you use?

- Azure AD cloud-only users
- Azure AD password hash synchronization
- Azure AD Pass-through Authentication
- Federated authentication

You answered this question correctly. ×

**Explanation:**  
Using a third-party service would require AD FS to transfer the authentication to the other identity provider.  
Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

## Objetivo 2: Evaluate Governance Risk Compliance (GRC) technical strategies

## 1. Azure Policy

You are implementing security for resources in an Azure subscription. You need to ensure that all virtual machines have a specific extension installed. What should you use?

Azure Advisor

Azure Policy

Defender for Cloud

Microsoft Sentinel

You answered this question correctly. ×

**Explanation:**

Azure Policy enables you to create guardrails for your environment, including using the DeployIfNotExist effect type to deploy additional components.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

## 2. Secure Score

Which component of Defender for Cloud provides insights into a key performance indicator related to how many security recommendations have been implemented for a subscription?

Alerts

Secure Score

Security Posture

Workload protection

You answered this question correctly. ×

**Explanation:**

Secure Score in Defender for Cloud provides you with a key performance indicator (KPI) related to how many recommendations have been implemented on a subscription.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/7-postures-use-secure-scores>

### 3. Risk Response

When planning to mitigate risks associated with known threats, in which phase of the risk management process would you tolerate or accept a known risk?

Identification

Assessment

Response

Monitoring

You answered this question correctly. ×

**Explanation:**

The risk management process has four phases: identification, assessment, response, and monitoring. Taking an action, even if the action is to accept the risk, is considered responding to the threat.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/6-interpret-technical-threat-intelligence-recommend-risk-mitigations>

### 4. Threat intelligence in Sentinel

Which tool in Microsoft Sentinel provides context, relevance, and priority to alerts?

Analytics rules

Hunting

Threat intelligence

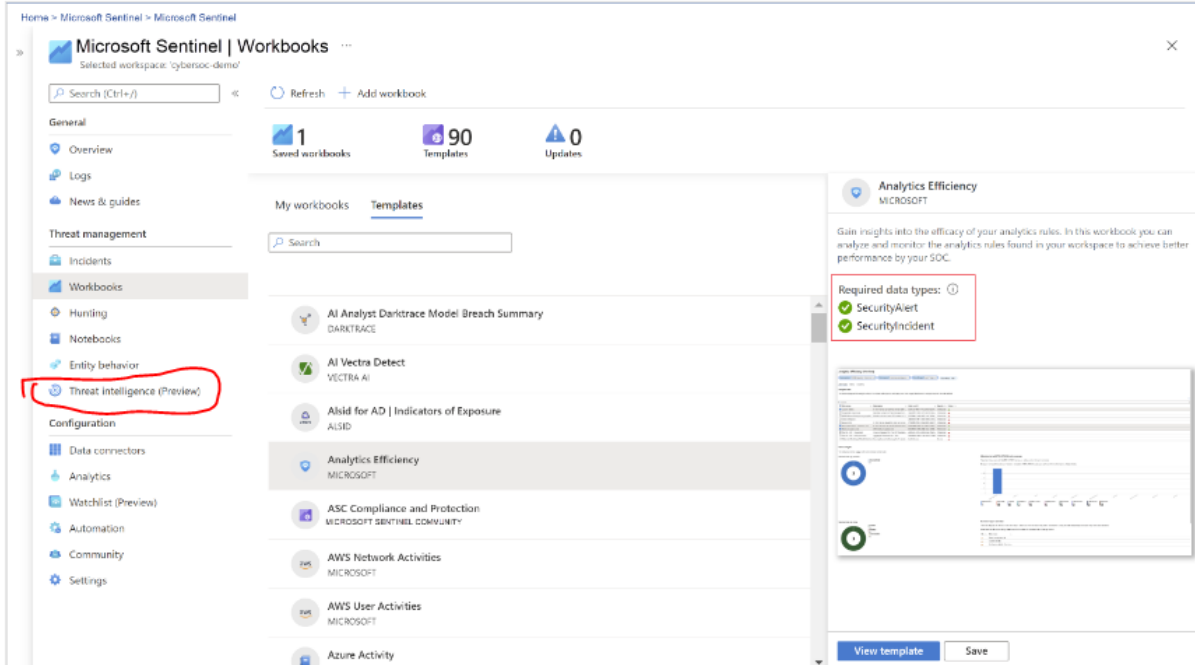
Workbooks

You answered this question correctly. ×

**Explanation:**

Threat intelligence in Microsoft Sentinel provides additional information around an alert so that security advisors can come to a solution faster.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/6-interpret-technical-threat-intelligence-recommend-risk-mitigations>



[What is Microsoft Sentinel? | Microsoft Learn](#)

5. Azure Policy Effects

Question 5 of 17

Question Id : SC-100-CP-1-043

You are implementing security for resources in an Azure subscription. You need to ensure that each resource has a default cost center tag applied if the resource was deployed without a cost center tag. Which two Azure Policy effects should you use?

- Append
- Audit
- AuditIfNotExist
- DeployIfNotExist

Select 2 answers

You answered this question correctly.

**Explanation:**  
 Azure Policy enables you to create guardrails for your environment, including being able alter or add to a deployment when the request is submitted with the Modify, Append, or DeployIfNotExist policy effects.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

Azure Policy enables you to create guardrails for your environment, including being able alter or add to a deployment when the request is submitted with the Modify, Append, or DeployIfNotExist policy effects.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

## 6. Azure Policy

You are implementing security for resources in an Azure subscription. You need to ensure that storage accounts cannot be deployed with HTTPS disabled. What should you use?

Azure Advisor

Azure Policy

Defender for Cloud

Microsoft Sentinel

Azure Policy enables you to create guardrails for your environment, including blocking deployments that do not meet requirements.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

## 7. Defender for Cloud

You are implementing security for resources in an Azure subscription that are subject to SOC TSP regulatory compliance. You need to identify recommendations and reports for the compliance of these resources. What should you use?

Azure Advisor

Azure Policy

Defender for Cloud

Microsoft Sentinel

Defender for Cloud provides a unified view of security, including reporting, recommendations, and compliance for an Azure subscription.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/3-evaluate-infrastructure-compliance-use-microsoft-defender-for-cloud>

## 8. Rapid Modernization Plan (RaMP)

Question Id : SC-100-CP-1-046

helps you define how to establish a cloud security posture and provides guidance for deployment paths.

Rapid Modernization Plan (RaMP) can help you define your cloud security posture and provides deployment paths for various layers of cloud security.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/2-postures-use-benchmarks>

## 9. Azure Policy Effects

You are implementing security for resources in an Azure subscription. You need to ensure that Azure resource deployments using an Azure region that has not been approved are not deployed. Which Azure Policy component should you configure?

- Array
- Assignment
- Effect
- Location

Azure Policy enables you to create guardrails for your environment, including being able to deny a deployment based on an Azure region using the Deny effect in the policy definition.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

## 10. Defender for Cloud uses MITRE ATTACK framework

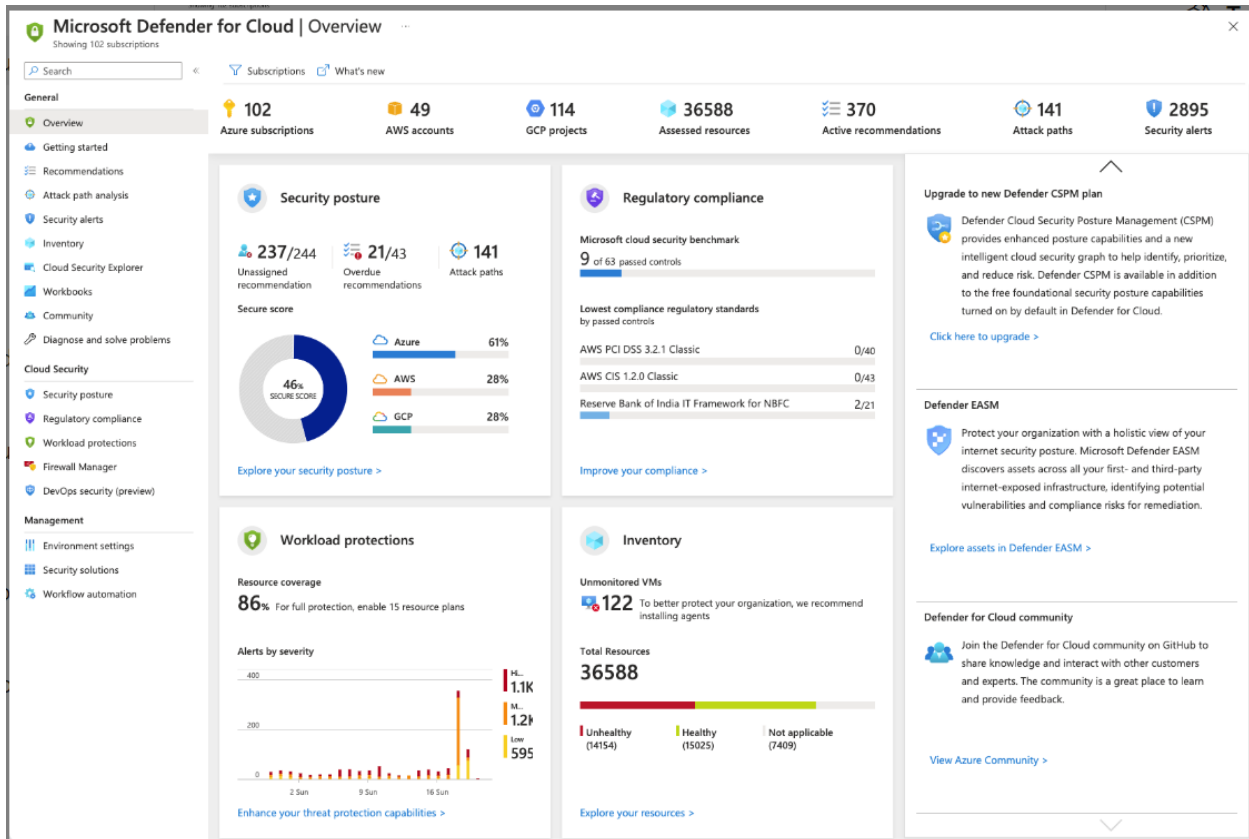
Which framework does Defender for Cloud use to allow you to identify security recommendations based on specific tactics?

- Cloud Adoption Framework
- MITRE ATTACK
- MITRE DEFEND
- Well-Architected Framework

Defender for Cloud correlates recommendations to increase your security posture and provides a reference to the MITRE Attack framework for these recommendations.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/3-postures-use-microsoft-defender-for-cloud>





[Review cloud security posture in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn](#)

## 11. Workflow Automation is built into Defender for Cloud

You need to configure an email notification when a new recommendation appears in Defender for Cloud. What should you configure?

- Azure Functions
- Azure Monitor
- Workbooks
- Workflow Automation

Workflow Automation is built into Defender for Cloud and allows you to create remediation logic, including email notifications.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/4-hygiene-of-cloud-workloads>

## 12. Data sovereignty

**Data sovereignty** mandates that data is stored in and under the legal jurisdiction of the country or region where the data is located.

Data sovereignty is part of a design solution involving where data will be stored and how the storage place affects the laws for that data.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/6-design-for-data-residency-requirements>

## 13. Azure Automation

You are planning operational compliance for an organization. You need to ensure that security updates are scheduled and applied to virtual machines. Which tool should you use?

- Azure Advisor
- Azure Automation
- Azure Blueprints
- Azure Policy

Azure Automation accounts allow you to schedule and implement patch management for virtual machines.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/2-interpret-compliance-requirements-their-technical-capabilities>

## 14. Azure Blueprints

**Azure Blueprints** bundle Azure Resource Manager templates, Azure Policy, and role assignments into a single container.

Azure Blueprints bundle together ARM templates, Azure policy definitions and assignments, and RBAC roles into a single solution.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/6-design-for-data-residency-requirements>

## 15. Azure Landing Zone

An Azure **landing zone** is a multi-subscription diagram of an Azure environment that plans for security and other aspects of the Well-Architected Framework at enterprise scale.

An Azure landing zone (LZ) defines the subscription layout for resources according to the Well-Architected Framework.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-security-for-azure-landing-zone>

## 16. Defender for Cloud provides continual assessment

Which tool should you use to continually assess the resources in a subscription for security configuration and vulnerability issues?

- Azure Advisor
- Azure Policy
- Defender for Cloud
- Microsoft Sentinel

Defender for Cloud provides continual assessment of the resources and configuration of those resources in a subscription.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/3-postures-use-microsoft-defender-for-cloud>

## 17. Operational compliance processes and the appropriate tools

Drag each operational compliance process to the appropriate tool to use to configure that process.

**Correct Answers**

- Patch management
- Policy enforcement
- Environment configuration
- Resource configuration

**Matching items here:**

- Azure Automation
- Patch management ✓**
- Azure Policy
- Policy enforcement ✓**
- Azure Blueprints
- Environment configuration ✓**
- Desired State Configuration
- Resource configuration ✓**

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/2-interpret-compliance-requirements-their-technical-capabilities>

## References

[SC-100: Microsoft Cybersecurity Architect \(Pearson Practice Test\) - O'Reilly Online Learning \(oreilly.com\)](#)