



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



SC-100 Dumps
SC-100 Braindumps
SC-100 Real Questions
SC-100 Practice Test
SC-100 Actual Questions



killexams.com

Microsoft

SC-100

Microsoft Cybersecurity Architect

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/SC-100>



Question: 546

You are designing a detection and response solution for an Azure environment. The solution must use Microsoft Sentinel to detect anomalous network traffic to an Azure VM and trigger a Defender XDR response to isolate the VM. Which configuration should you implement?

- A. Deploy Defender for Endpoint on the VM, integrate with Sentinel, and use a playbook for isolation
- B. Use Defender for Cloud to detect network anomalies, export to Sentinel, and automate VM isolation via Logic Apps
- C. Configure Azure Monitor to collect network logs, use Sentinel's analytics rules, and trigger Defender XDR via Azure Functions
- D. Enable Azure Network Watcher, ingest logs into Sentinel, create a KQL query for anomalies, and trigger a Defender XDR playbook

Answer: D

Explanation: Azure Network Watcher captures network traffic, and Microsoft Sentinel can ingest these logs for KQL-based anomaly detection. A Sentinel playbook triggers Defender XDR for VM isolation. Defender for Cloud is less specific for network traffic, Azure Monitor is not optimized, and Defender for Endpoint focuses on endpoint threats, not network anomalies.

Question: 547

An organization is deploying containerized workloads on AKS with a CI/CD pipeline using Azure DevOps. To comply with regulatory standards, you must specify security requirements for container orchestration to prevent privilege escalation. Which configuration should you recommend?

- A. Deploy Azure Defender for Containers and enable Azure Monitor for container health monitoring
- B. Configure AKS with Azure Active Directory pod-managed identities and enforce least privilege using Kubernetes RBAC
- C. Enable Azure Policy for AKS to restrict container capabilities and configure network policies for pod isolation
- D. Use Azure Container Registry with content trust and integrate it with Azure Key Vault for secret management

Answer: B

Explanation: Preventing privilege escalation in AKS requires fine-grained access controls. Configuring AKS with Azure Active Directory pod-managed identities allows pods to authenticate securely, while Kubernetes RBAC enforces least privilege, restricting pod permissions to minimize escalation risks.

Question: 548

An organization operates a multicloud environment with Azure PaaS, AWS IaaS, and Google Cloud SaaS. You need to design a solution for secure access, enforcing network segmentation and application controls. Which configuration aligns with Zero Trust?

- A. Deploy Azure Firewall with application rules, AWS Network Firewall with stateful rules, and Google Cloud Armor for SaaS
- B. Configure Azure Application Gateway with WAF, AWS Transit Gateway, and Google Cloud VPC firewall rules
- C. Use Microsoft Entra ID Conditional Access for app access, AWS VPC Security Groups, and Google Cloud IAM for SaaS
- D. Implement Azure NSGs with port-based rules, AWS NACLs, and Google Cloud default IAM policies

Answer: C

Explanation: Zero Trust emphasizes identity-based access and application controls. Microsoft Entra ID Conditional Access enforces app-specific policies across multicloud environments. AWS VPC Security Groups provide fine-grained network segmentation, and Google Cloud IAM ensures role-based access for SaaS. Firewall-based or port-based solutions (NSGs, NACLs) are less aligned with Zero Trust's focus on identity and application-layer security.

Question: 549

An organization needs a centralized logging solution with Microsoft Purview Audit to track Microsoft 365 user activities. The logs must be retained for 3 years and integrated with Microsoft Sentinel for real-time monitoring. Which configuration should you use?

- A. Enable Purview Audit (Premium), set 3-year retention in a Log Analytics workspace, and connect to Sentinel
- B. Configure Purview Audit (Standard), store logs in Azure Blob Storage for 3 years, and use Sentinel's connector
- C. Use Azure Monitor to collect Purview logs, set 3-year retention, and export to Sentinel
- D. Deploy Purview Audit (Premium), store logs in Azure Data Lake, and integrate with Sentinel

Answer: A

Explanation: Microsoft Purview Audit (Premium) supports up to 10-year retention in a Log Analytics workspace, ideal for 3-year requirements, and integrates with Microsoft Sentinel for real-time monitoring. Standard tier has shorter retention, Azure Monitor is not optimized, and Azure Data Lake lacks direct Sentinel integration.

Question: 550

Your organization requires mapping technologies to application security requirements for a new Azure-based application handling PCI DSS data. The application must encrypt data at rest and in transit. Which technology stack should you recommend?

- A. Azure MySQL with default encryption, Azure Kubernetes Service with HTTP ingress, and Azure Key Vault for certificates
- B. Azure Cosmos DB with client-side encryption, Azure Functions with HTTP triggers, and Azure Key Vault for secrets
- C. Azure Blob Storage with server-side encryption, Azure App Service with HTTP, and Azure AD for authentication
- D. Azure SQL Database with Transparent Data Encryption (TDE), Azure App Service with HTTPS, and Azure Key Vault for key management

Answer: D

Explanation: PCI DSS requires encryption of data at rest and in transit. Azure SQL Database with TDE ensures data at rest is encrypted, Azure App Service with HTTPS secures data in transit, and Azure Key Vault manages encryption keys securely. Option B's client-side encryption is complex and unnecessary, and HTTP triggers are insecure.

Question: 551

An organization is implementing a DevSecOps process aligned with the Microsoft Cloud Adoption Framework (CAF). The process must secure microservices on Azure Container Instances. Which solution should you recommend?

- A. Deploy Azure Arc for container management, implement Azure Policy for compliance, and use Azure Firewall for egress control
- B. Use Azure DevOps with GitHub Actions for scanning, enable Azure Monitor for container telemetry, and configure Azure Key Vault for secrets
- C. Integrate Azure Pipelines with Snyk for vulnerability scanning, configure Microsoft Defender for Cloud for runtime protection, and use Azure AD workload identity for secure access
- D. Configure Azure Security Center with container policies, deploy Azure AD Conditional Access for access, and use Microsoft Sentinel for threat detection

Answer: C

Explanation: CAF's DevSecOps guidance emphasizes securing microservices. Snyk, integrated with Azure Pipelines, scans for vulnerabilities in container images. Microsoft Defender for Cloud provides runtime protection, detecting threats. Azure AD workload identity secures access to Azure resources, aligning with Zero Trust. Other options lack specific focus on microservices security or CI/CD

integration.

Question: 552

An organization needs a monitoring solution for a hybrid environment to detect unauthorized changes to Azure Key Vault secrets. The solution must alert via Microsoft Sentinel. Which configuration should you use?

- A. Use Defender for Cloud to monitor Key Vault, export alerts to Sentinel, and set up analytics rules
- B. Enable Azure Key Vault diagnostics, ingest logs into Sentinel, and create a KQL query for secret changes
- C. Configure Azure Monitor to collect Key Vault logs, integrate with Sentinel, and use automation rules
- D. Deploy Defender for Endpoint on Key Vault servers, integrate with Sentinel, and monitor secret changes

Answer: B

Explanation: Azure Key Vault diagnostics logs capture secret changes, and Microsoft Sentinel can ingest these for KQL-based detection. Defender for Cloud is less granular, Azure Monitor is not optimized, and Defender for Endpoint is not applicable to Key Vault.

Question: 553

You are tasked with designing access controls for a hybrid environment with Azure IaaS VMs, AWS EC2 instances, and Salesforce SaaS. The solution must enforce Zero Trust principles, including application-level segmentation and identity-based access. Which configuration meets these requirements?

- A. Use Microsoft Entra ID Conditional Access with app-specific policies, AWS IAM roles with temporary credentials, and Salesforce Identity Connect for SSO
- B. Deploy Azure Firewall with application rules, configure AWS Security Groups with IP-based rules, and use Salesforce Shield for data encryption
- C. Implement Azure Application Gateway with Web Application Firewall (WAF), AWS Network ACLs, and Salesforce default access policies
- D. Configure Azure Network Security Groups (NSGs) with port-based rules, AWS VPC peering, and Salesforce MFA with default settings

Answer: A

Explanation: Zero Trust requires identity-based access and application-level controls. Microsoft Entra ID Conditional Access enables app-specific policies, enforcing MFA and device compliance for Azure and Salesforce. AWS IAM roles with temporary credentials align with least privilege and Zero Trust by

limiting access scope. Salesforce Identity Connect integrates with Entra ID for SSO, ensuring seamless identity management. Other options rely on network-based controls (NSGs, Security Groups) or lack application segmentation (Salesforce default policies), which don't fully align with Zero Trust principles.

Question: 554

A law firm uses macOS 14 and Windows 11 devices. You need to specify a configuration to enforce secure file sharing. Which setting leverages Microsoft Endpoint Manager?

- A. Disable DLP policies and use OneDrive with no folder protection
- B. Configure Data Loss Prevention (DLP) policies and enable OneDrive with Known Folder Move
- C. Enable DLP policies for unmanaged devices only and disable OneDrive
- D. Set DLP policies to warn-only and configure OneDrive with public sharing

Answer: B

Explanation: Secure file sharing requires data protection. DLP policies in Endpoint Manager prevent sensitive data leaks, while OneDrive with Known Folder Move ensures files are backed up and protected.

Question: 555

You are evaluating security update solutions for a hybrid environment with diverse OS platforms. Which solution ensures compliance with Microsoft's security baselines and minimizes administrative overhead?

- A. Use Azure Automation Update Management with scheduled updates and Azure Monitor for compliance
- B. Deploy WSUS with group policies and use Microsoft Purview for auditing
- C. Configure Azure Arc with automated patching and validate with Azure Policy
- D. Implement Microsoft Defender for Servers with automated updates and Microsoft Sentinel for monitoring

Answer: A

Explanation: Azure Automation Update Management centralizes update scheduling for diverse OS platforms, reducing administrative overhead. Azure Monitor tracks compliance with Microsoft security baselines. Other options either require more manual effort (WSUS) or lack centralized management (Azure Arc, Microsoft Defender).

Question: 556

You are specifying security requirements for an AKS cluster running containerized workloads with sensitive data. The orchestration must ensure secure communication between services. Which configuration should you recommend?

- A. Configure Kubernetes network policies with mutual TLS (mTLS) and enable Azure Defender for Containers for runtime protection
- B. Deploy Azure Container Registry with content trust and integrate it with Azure Key Vault for secret management
- C. Enable AKS with Azure Active Directory integration and configure role-based access control (RBAC)
- D. Use Azure Policy to enforce container resource limits and enable Azure Monitor for logging

Answer: A

Explanation: Secure communication in AKS requires encrypted, authenticated service interactions. Kubernetes network policies with mTLS enforce encrypted communication between services, while Azure Defender for Containers provides runtime protection against threats.

Question: 557

You are designing an external identity solution for a university with 100,000 students and 2,000 faculty. The solution must support B2C self-service and B2B collaboration with decentralized identity. Which configuration is optimal?

- A. Deploy Azure AD B2C with OAuth 2.0, Entra B2B with SAML federation, and a custom decentralized identity solution
- B. Configure Microsoft Entra External ID for B2C with self-service sign-up, Entra B2B with email one-time passcodes, and Entra Verified ID for decentralized identity
- C. Use Microsoft Entra External ID for B2C with social logins, Entra B2B with guest invitations, and a third-party blockchain for decentralized identity
- D. Implement Microsoft Entra External ID for B2C with MFA, Entra B2B with direct federation, and a third-party identity provider

Answer: B

Explanation: Microsoft Entra External ID for B2C with self-service sign-up supports scalable student access. Entra B2B with email one-time passcodes simplifies faculty collaboration. Entra Verified ID provides a native decentralized identity solution, reducing complexity. Third-party or custom solutions increase integration challenges, and social logins or MFA alone don't address decentralized identity.

Question: 558

An organization is implementing a DevSecOps process aligned with the Microsoft Cloud Adoption Framework (CAF). The process must secure APIs hosted on Azure API Management. Which solution should you recommend?

- A. Deploy Azure Arc for API management, implement Azure Policy for compliance, and use Azure Firewall for egress control
- B. Use Azure DevOps with GitHub Actions for API testing, enable Azure Monitor for API telemetry, and configure Azure Key Vault for secrets
- C. Integrate Azure Pipelines with Postman for API testing, configure Microsoft Defender for Cloud for runtime protection, and use Azure AD workload identity for secure access
- D. Configure Azure Security Center with API policies, deploy Azure AD Conditional Access for access, and use Microsoft Sentinel for threat detection

Answer: C

Explanation: CAF's DevSecOps guidance emphasizes securing APIs. Postman, integrated with Azure Pipelines, tests API security during CI/CD. Microsoft Defender for Cloud provides runtime protection, detecting threats. Azure AD workload identity secures API access to Azure resources, aligning with Zero Trust. Other options lack specific focus on API security or CI/CD integration.

Question: 559

You are designing a security strategy for an Azure environment using the Microsoft Azure Well-Architected Framework. Which solution ensures workload protection for Azure App Services?

- A. Implement Azure AD Privileged Identity Management (PIM) for App Service admins and enable Azure Monitor
- B. Configure Azure Firewall with application rules for App Services and implement Azure Key Vault for secrets
- C. Enable Azure Policy to enforce HTTPS for App Services and configure Network Security Groups (NSGs)
- D. Deploy Microsoft Defender for Cloud with App Service plan protection and enable Azure AD authentication

Answer: D

Explanation: The Azure Well-Architected Framework emphasizes workload protection and identity security. Deploying Microsoft Defender for Cloud with App Service plan protection provides threat detection and vulnerability management, while Azure AD authentication ensures secure access, aligning with the framework. Azure Firewall and Key Vault focus on network and secrets, not App Service

protection. Azure Policy and NSGs address protocol and filtering but lack threat detection. PIM and Azure Monitor focus on access and monitoring, not workload protection.

Question: 560

You need to design a security solution for Azure Storage accounts using Microsoft Defender for Storage. The solution must detect data exfiltration attempts and integrate with SIEM. Which configuration is optimal?

- A. Enable Defender for Storage with activity monitoring and connect to Azure Monitor
- B. Enable Defender for Storage with basic scanning and use Azure Policy for SIEM integration
- C. Enable Defender for Storage with anomaly detection and integrate with Azure Sentinel
- D. Enable Defender for Storage with malware scanning and sync with Microsoft Purview

Answer: C

Explanation: Microsoft Defender for Storage with anomaly detection identifies data exfiltration attempts. Integration with Azure Sentinel provides SIEM capabilities for advanced threat analysis. Azure Monitor lacks SIEM features, basic scanning is insufficient, and Purview is for governance, not real-time SIEM.

Question: 561

An energy company uses Microsoft Defender for IoT to secure SCADA systems. You need to evaluate a solution to enforce compliance with NIST 800-82. Which configuration ensures secure protocol usage and threat detection?

- A. Use Defender for IoT with default protocol settings and manual threat detection
- B. Configure Defender for IoT to block all non-SCADA protocols and disable behavioral analytics
- C. Deploy Defender for IoT with protocol validation for DNP3 and enable behavioral analytics for threat detection
- D. Set up Defender for IoT to allow all protocols and rely on external SIEM for analytics

Answer: C

Explanation: NIST 800-82 emphasizes secure protocol usage and proactive threat detection in SCADA environments. Defender for IoT's protocol validation for DNP3 ensures only authorized communications occur, while behavioral analytics detect deviations indicative of threats.

Question: 562

Your organization needs to design a solution to manage secrets, keys, and certificates for a hybrid application hosted on Azure and on-premises servers. The solution must ensure that secrets are rotated every 30 days, access is audited, and certificates are issued from a trusted internal Certificate Authority (CA). Which Azure service configuration meets these requirements?

- A. Use Azure Key Vault with manual key rotation; configure Role-Based Access Control (RBAC) with least privilege; use Azure Certificate Authority for certificate issuance
- B. Use Azure Key Vault with automatic key rotation every 30 days; configure Microsoft Entra ID Privileged Identity Management (PIM) for access control; integrate with an on-premises CA for certificate issuance
- C. Use Azure App Service to store secrets; configure Microsoft Entra ID Conditional Access for access; use a third-party CA for certificate issuance
- D. Use Azure Blob Storage to store secrets; configure Shared Access Signatures (SAS) for access; integrate with an external CA for certificate issuance

Answer: B

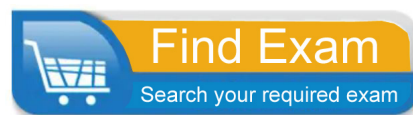
Explanation: Azure Key Vault is the appropriate service for managing secrets, keys, and certificates securely. Automatic key rotation every 30 days meets the rotation requirement, and access auditing is built into Key Vault. Integrating with an on-premises CA ensures certificates are issued from a trusted internal source. Microsoft Entra ID Privileged Identity Management (PIM) provides just-in-time access control, aligning with least privilege principles for managing sensitive resources.





KILLEXAMS.COM

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:



Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.