Azure Security - Detailed Reference

Azure Security — Detailed Reference (Topics 49-52)

Topic 49: Microsoft Defender for Cloud

CSPM and CWP. Secure Score, recommendations, regulatory compliance, threat detection, JIT VM access.

Plans: Free (CSPM), Servers (~$15/VM/mo), App Service (~$7/app/mo), SQL (~$15/server/mo), Storage, Key Vault, DNS, Containers.

JIT VM Access: Management ports closed by default. Request access, NSG temporarily opens, auto-closes. Eliminates persistent open management ports.

Regulatory Compliance: Assess against HIPAA, ISO 27001, SOC 2, PCI DSS, NIST, CIS. Continuous evaluation. Compliance score per framework. Remediate failed controls.

Topic 50: Azure Key Vault

Store secrets, keys, certificates.

Access: Vault access policy (legacy) or Azure RBAC (preferred). RBAC Roles: Administrator, Secrets User, Secrets Officer, Crypto User, Crypto Officer, Certificate User, Certificate Officer. Security: Soft delete (90 days, on by default), Purge protection, Firewall, Private Endpoint, Diagnostic logging. Managed HSM: FIPS 140-2 Level 3. ~$2,160/month. Dedicated single-tenant. Key Rotation: Auto-rotate on schedule. Applications use latest version. Old versions remain accessible for decryption.

Topic 51: Microsoft Sentinel

Cloud SIEM/SOAR.

Components: Data connectors, Analytics rules (Scheduled, NRT, MS Security, Fusion), Incidents, Workbooks, Playbooks (Logic Apps), Hunting queries, Watchlists, Threat intelligence.

Playbooks: Auto-block IPs, create tickets, notify teams. Logic Apps triggered by incidents.

Cost: ~$2.46/GB ingested. First 5GB/day free with Defender plan.

Topic 52: Zero Trust Architecture

“Never trust, always verify.”

Principles: Verify explicitly, Use least privilege, Assume breach.

By Pillar: - Identity: Entra ID, Conditional Access, PIM, MFA - Endpoints: Intune, Compliance policies - Applications: Entra auth, API Management - Data: Purview, encryption, RBAC - Infrastructure: Policy, Defender, NSGs, Firewall, Private Endpoints - Network: Micro-segmentation, Private Link - Visibility: Sentinel, Monitor