SC-100 STUDY CRAM

https://onboardtoazure.com

Identity

- Azure Active Directory Partnets
- Azure Active Directory
- Azure Active Directory Customers
- B2B
- B2C
- Conector de AD
- Hashes
- Active Directory Domain Service
- **Defender for Identity**

P2:
- PMI
- Identity protection

P1:
- Conditional access
- MFA

Free:
- Security defaults

Risk

Endpoint

- MS Endpoint Manager (MEM)
  - Intune
  - Config Mgr
- Policy
  - Compliance
  - Config
- Inventory
- **Defender for Endpoint**
  - Protect
  - Detect
  - Respond
- **Defender for Servers**
  - Adaptative App Hardering
  - FIM
  - JIT

Adaptative Network Hardening

Network

+ DDoS Protection Std

- Global
- Azure Front Door L7
- WAF (L7)
- Azure Firewall
- UDR
- Region
- APP GW
- WAF (L7)
- App Service Env. v3
- SQL Managed Instance
- Service Endpoint
- App Endpoint
- Private Endpoint
- Service
- App Svc
- Private Link
- SQL
- Public Endpoint
- S2S VPN / Express Route PP

Virtual Network

Network Security Group Rules – L4

Infrastructure

Defender for Cloud
- Cloud Posture / Compliance
- Recomendations
- Secure score

Using

- AWS
- GCP
- Azure

Auto agent provision Policy

Other cloud providers

Azure Arc
- Servers
- K8S
- Data
- App
- AI

Onprem Infra

Check

Azure Policy
- Compliance
- Guardrails
- Guess Config

Blueprints
- Policy
- Resource Groups
- RBAC
- Templates

Azure Resource Manager

Subscription

- Portal
- Native

Defender for Servers JIT
- IP
- Duration

Modify

Azure Bastion

RDP
SSH
NSG

Virtual Machine (VM2)
- UEFI + vTPM
- Trusted launch
- Confidential compute
  - Memory and CPU enc.
  - OS Level
  - Enclave (Intel SGX)

Managed Idenity
- System
- User

Encryption at rest
- Platform Managed Key (PMK)
- Customer Managed Key (CMK)

Azure Key Vault
- Keys [HSM]
- Secrets
- Certificates

Signals

Context Conditional Access Control

Azure Active Directory P1/P2

Session Control

APPS

Custom APP

DevOps
- Azure DevOps
- Github

Advance Security
- Code analysis
- Miss configuration

Reverse Proxy

Defender for App Service

SaaS

API

DATA

MS Purview
- Discover
- Classify
- Lineage

Labels

Information Protection

Protection

MSQL
- Discover
- Classify
- Lineage
- Masking

Azure Backup
- PIN
- Multi-user Authorization (Resource Guard)

1 - Collect

Connectors
- AAD
- O365
- Syslog
- FW
- ...

SIEM / SOAR Azure Sentinel

Log Analytics Workspace

KQL

2 - Detect

- Analytics
- Hunting
- Intelligence

Incidents

3 - Investigate

4 – Respond
- Automation Rules
- Playbook

Logic Apps

Zero Trust
1 – Verify explicitly
2 – Use least privilege
3 – Assume breach

Least Privileges

Azure Active Directory
- RBAC
- JIT
  - AAD PIM (P2)
  - AAD Rules
  - ARM Rules

Active Directory Domain Service Onpremise
- PAM