Challenge ①

Challenge ②

Challenge ③

Challenge ④

Challenge ⑥

Goals

Azure Sub

- Shared Dashboard

Foundation – Resource Strategy / Structure

- Sub Mgmt Group, RG / Tenant

- Elevation of Privilege
- Static Creds
- Audit Access
- PIM / Security

Identity Baseline

- Who can manage
- Sub owners / Sec admins
- AD & AAD Setup
- Groups → PIM
- (JIT) → PIM
- Global admin
- Sec admin / admin
- Sec admin
- n PA
- Integration
- Workload – users / dev / sec
- Provide Sec Admin Rights
- Assess Identity Baseline Questionnaire Score?

Sec Baseline

- What do you have to prove & how often
- What IC change needs to happen
- What do you have to prove to auditors or what can you monitor

- min policy audit or enforcement
- Key List
- Priority – Sprint 1H
- Backlog – future sprints
- Charge Ax coverage
- Answer Sec Baseline Qs Score?

Resource Consistency

- SHALL Force Allow SQL Azure to be deployed w/o TDE in my tenant
- SUC steps
- Automation stg
- Key Vault
- SQL Azure
- TDE
- Naming & tagging
- Compliance & Policy

Cost Mng

- Azure cost mng → Reporting By BU / LOB
- Quotas

Challenge ⑤

Deployment Acceleration

- Environment RG
- Sandbox, Non-Prod, Prod ← SOC, RG
- Isolation → Tenant, Sub, RG (Foundation)
- → Network / Sec Security (VDC)
- → RPE (Logic Apps) / ISE
- Integration
- Automation ← Build Move
- Self-Suc (CATALOGS?)
- Code repository
- PRM, Terraform

Challenge ⑦

- Full Dashboard w/ Alerts
- Sign off to Compliance Manager
- Diagnostics + Event Hub → 3rd Party Siem

Open Hack → Business Goal → Agile Deployment of Workload Bot! AKS in Azure → Sign off by CISO Monthly

- About CISO what Angle
- Include Nuclear / Physical Attack
- Include DATA Tamper / Release

BIZ → CAF Baseline

Tenant definition & Understanding

Azure Sub ← Best Practices Doc

- On-Prem
- Resources
- IAAS
- PAAS

Tech

- RBAC
- Blueprint
- Policy
- Resource Graph
- Mgmt Groups
- Hybrid
  - Az monitor / Alerting
  - Az Security Center
  - Sentinel
- Diagnostics & Event Hub
- Az Dashboard
- Automation? Az DevOps / Jenkins / Zenkins / Ansible

→ 3rd Party Siem

(Policies) → CIS Benchmarks ISO 27001

Doc Map

Ops | Sec | Compliance Bot

- Compliance Mgmt
- Security CTR
- Provision
- Sentinel → Reporting
- 3rd party
- Inventory Timeline

Trust but Verify Dashboards/Alerts

CAF Categories

- Identity Baseline
- Security Baseline
- Resource Consistency
- Cost Mng

Deployment Consistency

- Environments
- Suc Catalog

Alerts 2 CISO

Open Tasks

① In Each Section

- Scrapbook Items on
- Doc Link to Best Practices
- Doc Link to Compliance
- Link to Baseline tool!
- Scenario / MVP
- Backlog

② Environment?

③ Workflow?

- Which tool in Each Change

④ Task List to create Openhack

- Azure DevOps

⑤ Break Down Challenges to Channels