Microsoft Azure Enterprise Cloud Security Assessment

CYBERINFINITI LTD.

FEBRUARY 2026

A Comprehensive Cloud security evaluation across 9 Practice labs

Executive Summary

This Enterprise Cloud Security Assessment evaluated Cyberinfiniti Ltd’s Microsoft Azure environment across identity governance, access control, monitoring, threat detection, and incident response through nine structured labs. The assessment measured the effectiveness of preventive, detective, and responsive controls against modern cloud threats, aligning findings with Zero Trust, least-privilege, and defense-in-depth principles.

Key Results indicate that Azure’s integrated security ecosystem significantly strengthens attack surface reduction, visibility, and incident response when properly governed. Key improvement areas include configuration complexity, governance consistency, and skills dependency—informing strategic recommendations for enhancing overall cloud security maturity.

Objectives

The primary objectives of the assessment were to:

- Evaluate identity and access controls to ensure enforcement of least privilege and role separation.
- Assess centralized visibility and monitoring across cloud workloads.
- Validate the ability to detect misconfigurations, vulnerabilities, and active threats.
- Measure the effectiveness of attack surface reduction controls.
- Demonstrate incident detection and automated response aligned with modern SOC operations.
- Translate technical findings into executive-level risk, impact, and maturity insights.

Azure Environment Architecture

Region

East US deployment

Subscription

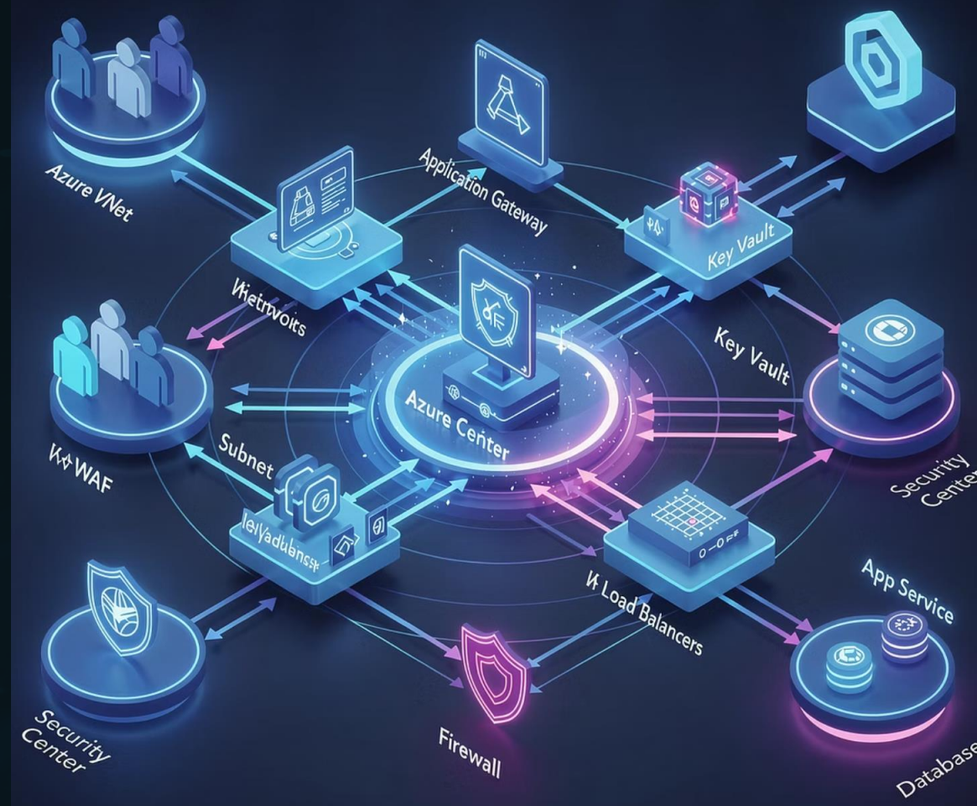
Pay-As-You-Go model

Access Model

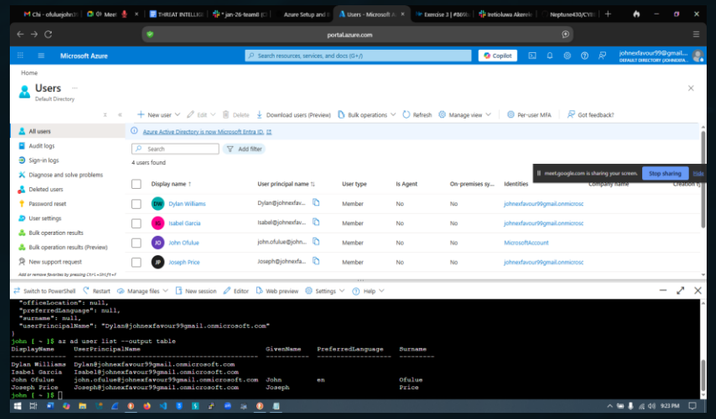
Contributor & Owner roles

Identity

Dedicated Entra ID tenant in (TEAM8) Resource Group

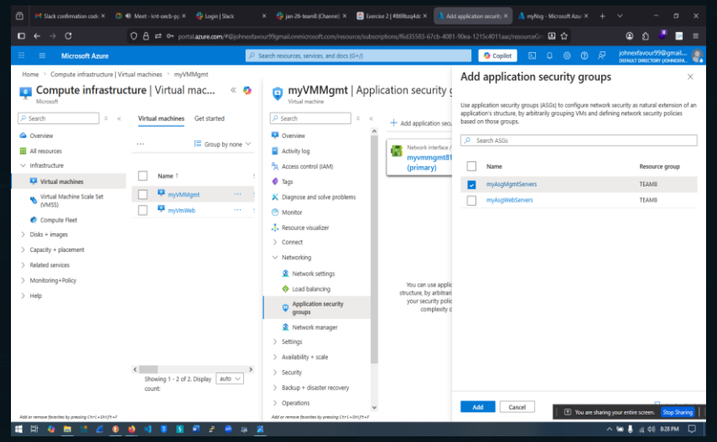


Labs 1-3: Identity, Network & Firewall Security



Lab 01: RBAC

Group-based access control with Senior Admins, Junior Admins, and Service Desk groups. VM Contributor role assigned for delegated management.



Lab 02: NSG & ASG

Network segmentation with Web Servers and Management Servers. RDP restricted to management, HTTP allowed to web tier.

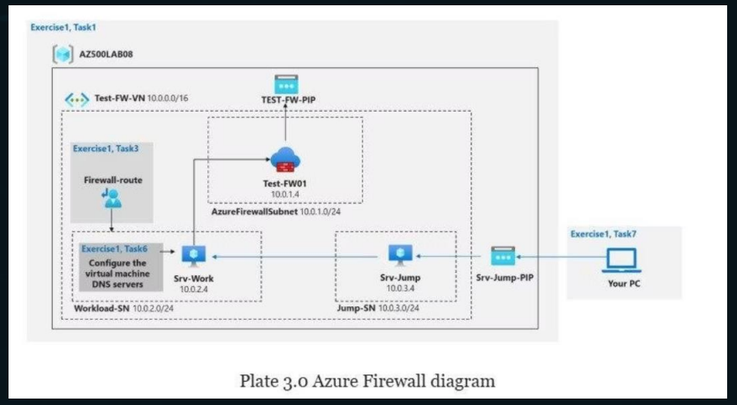


Plate 3.0 Azure Firewall diagram

Lab 03: Azure Firewall

Centralized traffic control with custom routes. Outbound access limited to bing.com, external DNS queries allowed.

Labs 4-6: Container, Storage & Monitoring Security

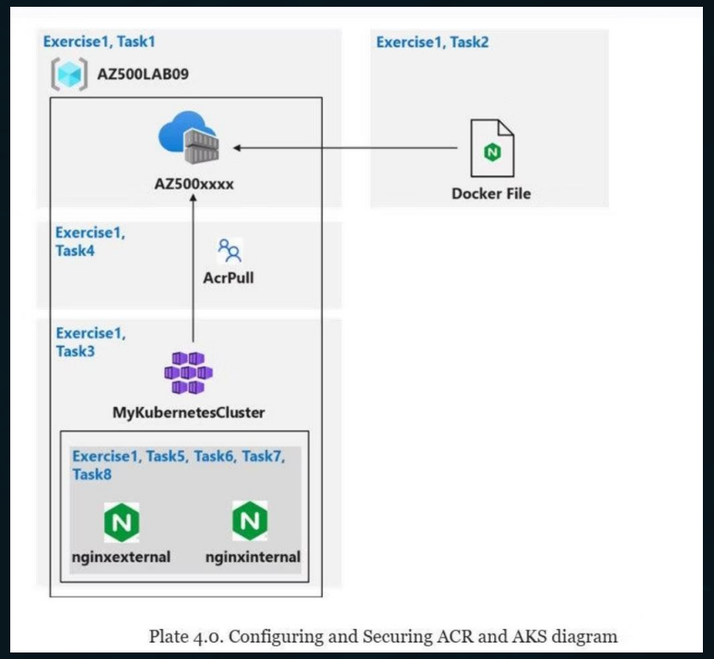


Plate 4.0. Configuring and Securing ACR and AKS diagram

Lab 04: ACR & AKS

Secure container deployment with private registry access. AcrPull permissions configured for AKS cluster.

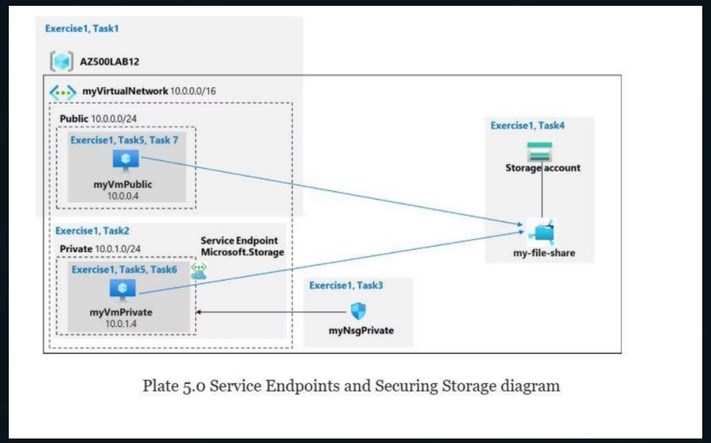


Plate 5.0 Service Endpoints and Securing Storage diagram

Lab 05: Service Endpoints

Storage restricted to specific subnet. Traffic remains on Azure backbone, unauthorized access blocked.

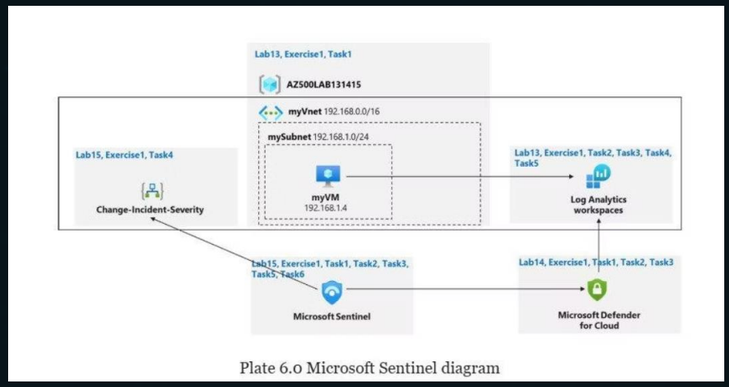
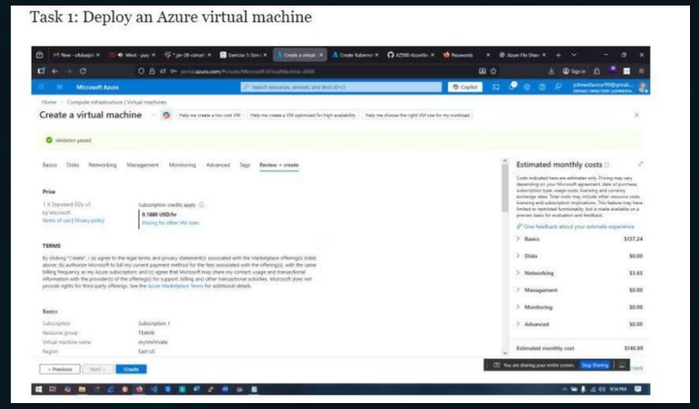


Plate 6.0 Microsoft Sentinel diagram

Lab 06: Log Analytics & DCR

Centralized logging with Data Collection Rules. Security events, system logs, and performance metrics captured.

Labs 7-9: Advanced Threat Protection



Lab 07: Defender for Cloud

Plan 2 enabled for advanced threat protection and vulnerability management

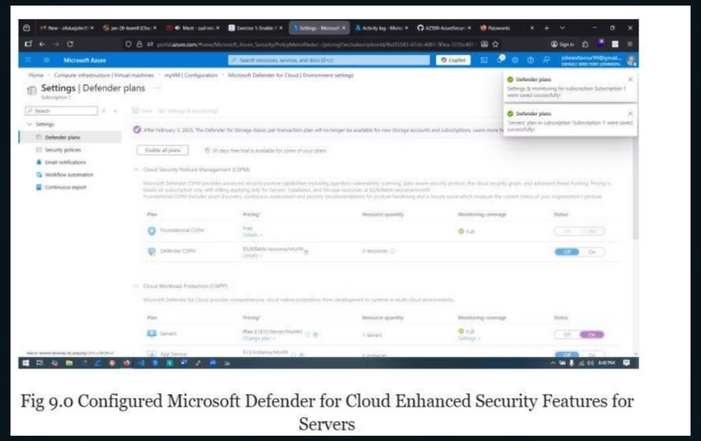
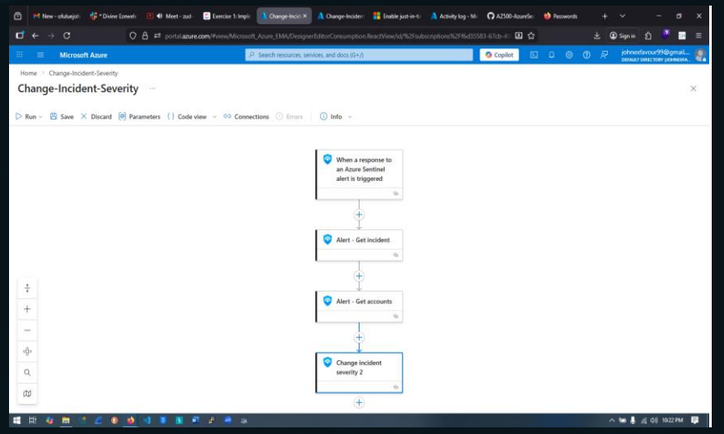


Fig 9.0 Configured Microsoft Defender for Cloud Enhanced Security Features for Servers

Lab 08: Just-in-Time Access

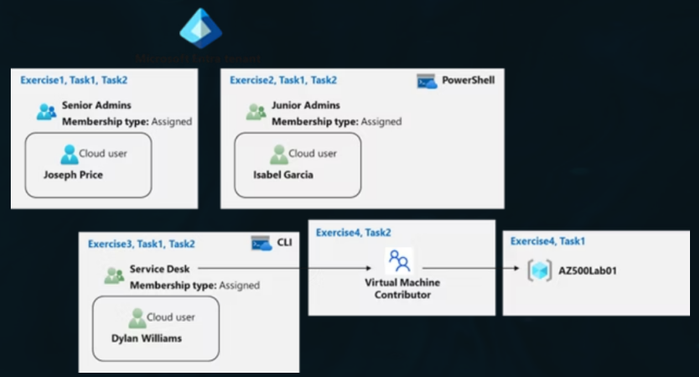
Time-limited VM access reduces brute-force attack exposure



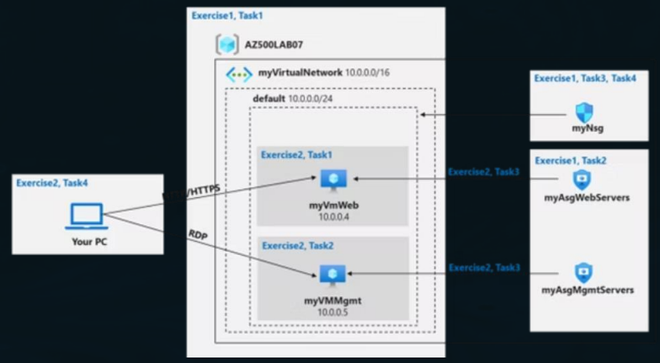
Lab 09: Microsoft Sentinel

SIEM/SOAR with automated playbooks for incident response

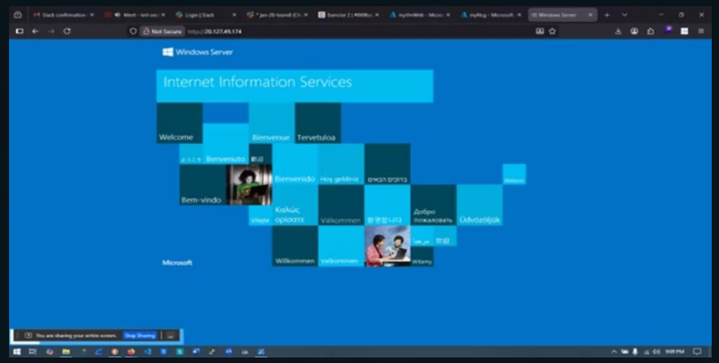
Lab Implementation Details: Identity & Network Security



Lab 01: RBAC - Group-based access control with role assignments

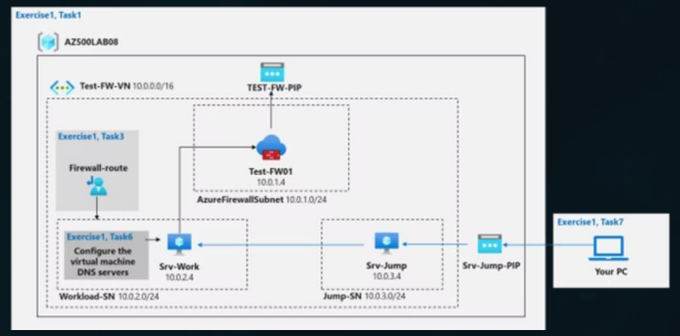


Lab 02: NSG & ASG - Network segmentation architecture

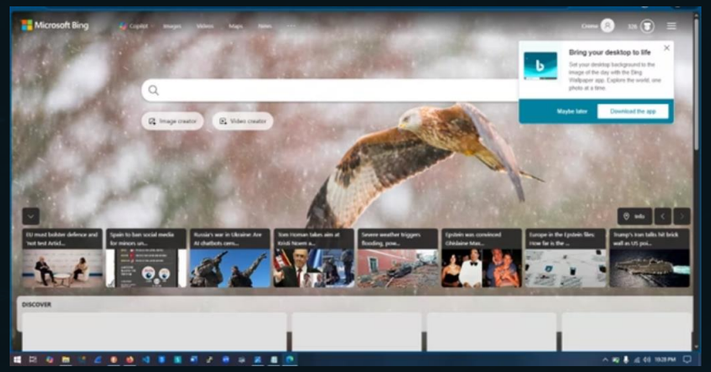


Lab 03: IIS Server Configuration

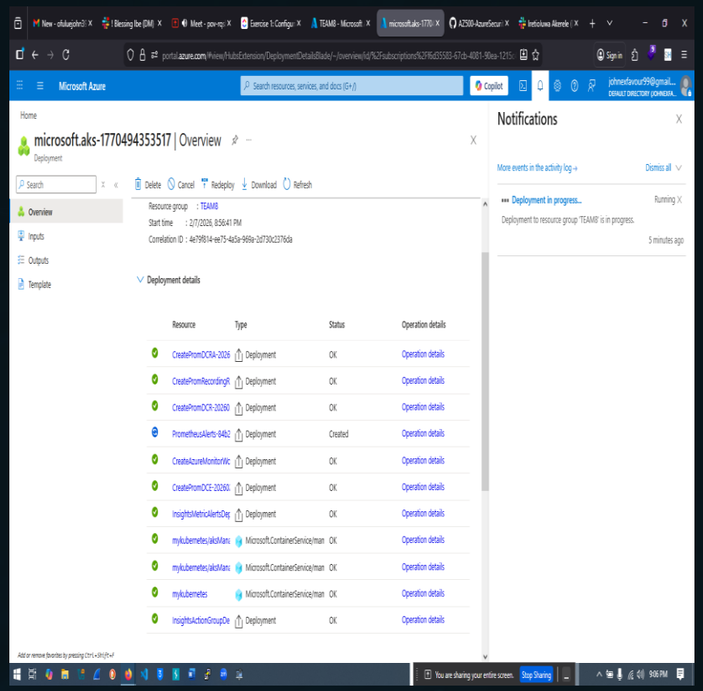
Lab Implementation Details: Firewall & Container Security



Lab 04: Azure Firewall topology with routing

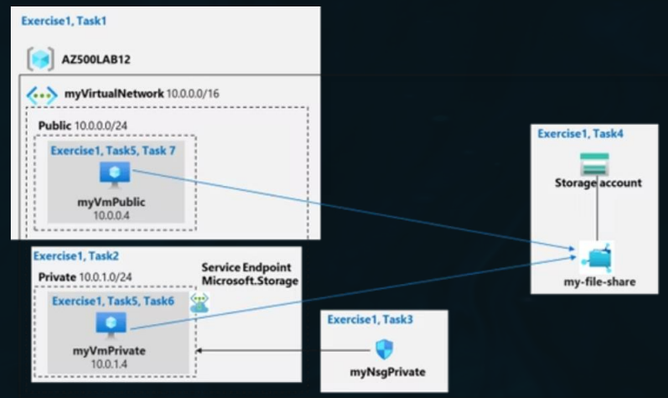


Lab 05: Firewall testing - Bing.com access validation

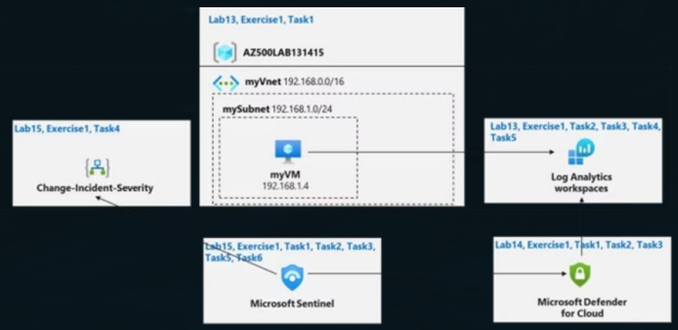


Lab 06: ACR & AKS container deployment

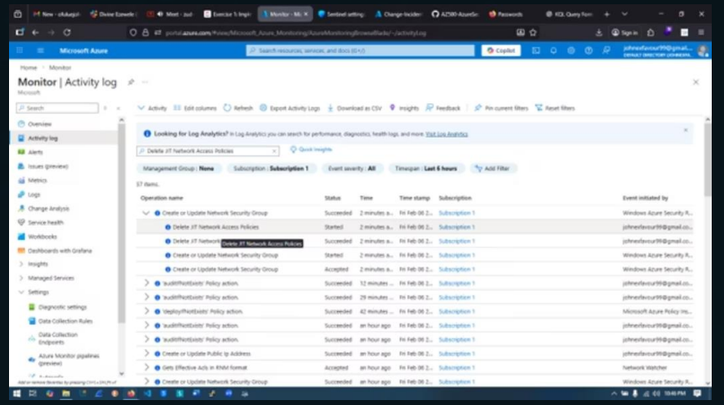
Lab Implementation Details: Storage & Monitoring



Lab 07: Service Endpoints - Storage access control

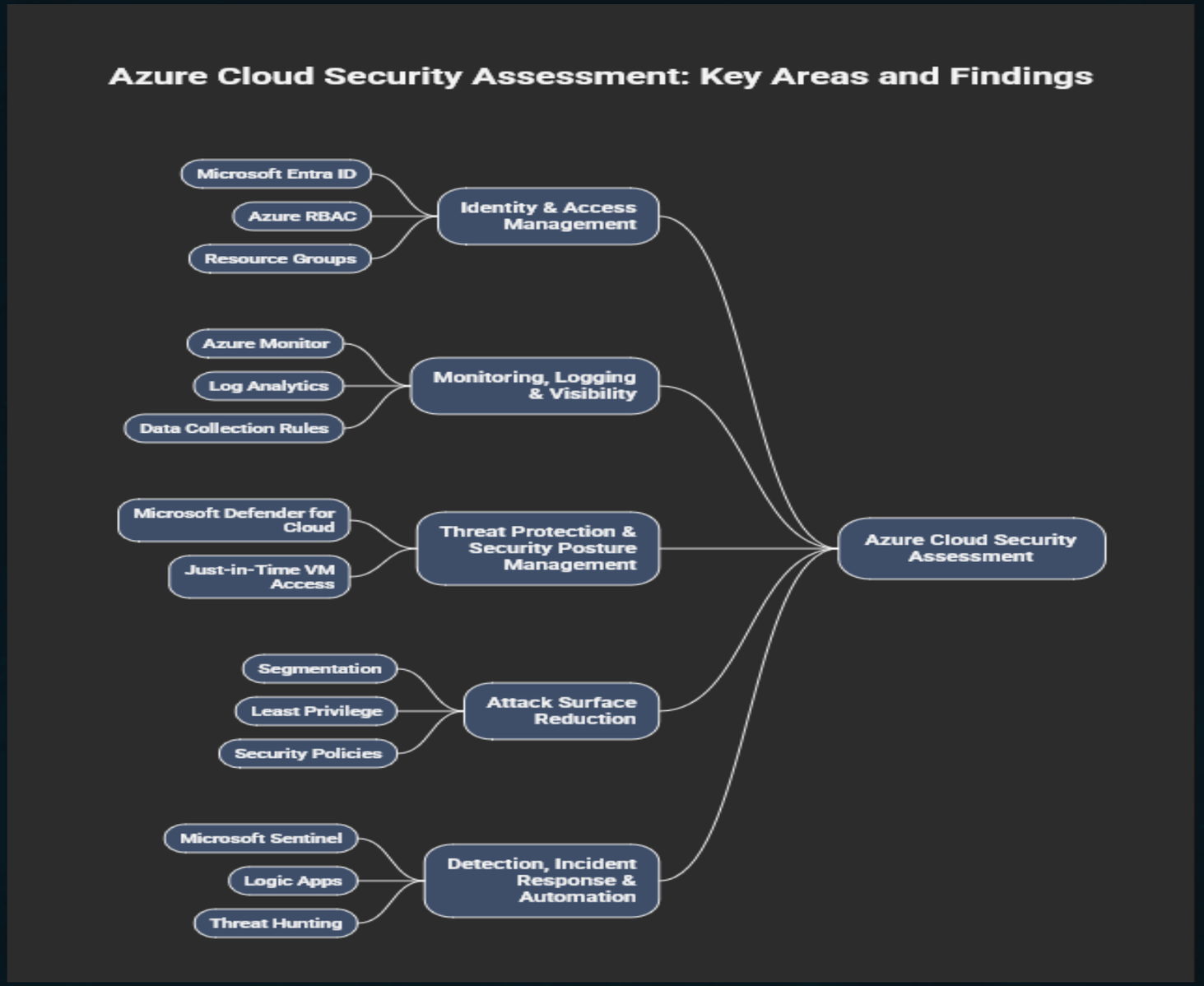


Lab 08: Log Analytics & DCR integration

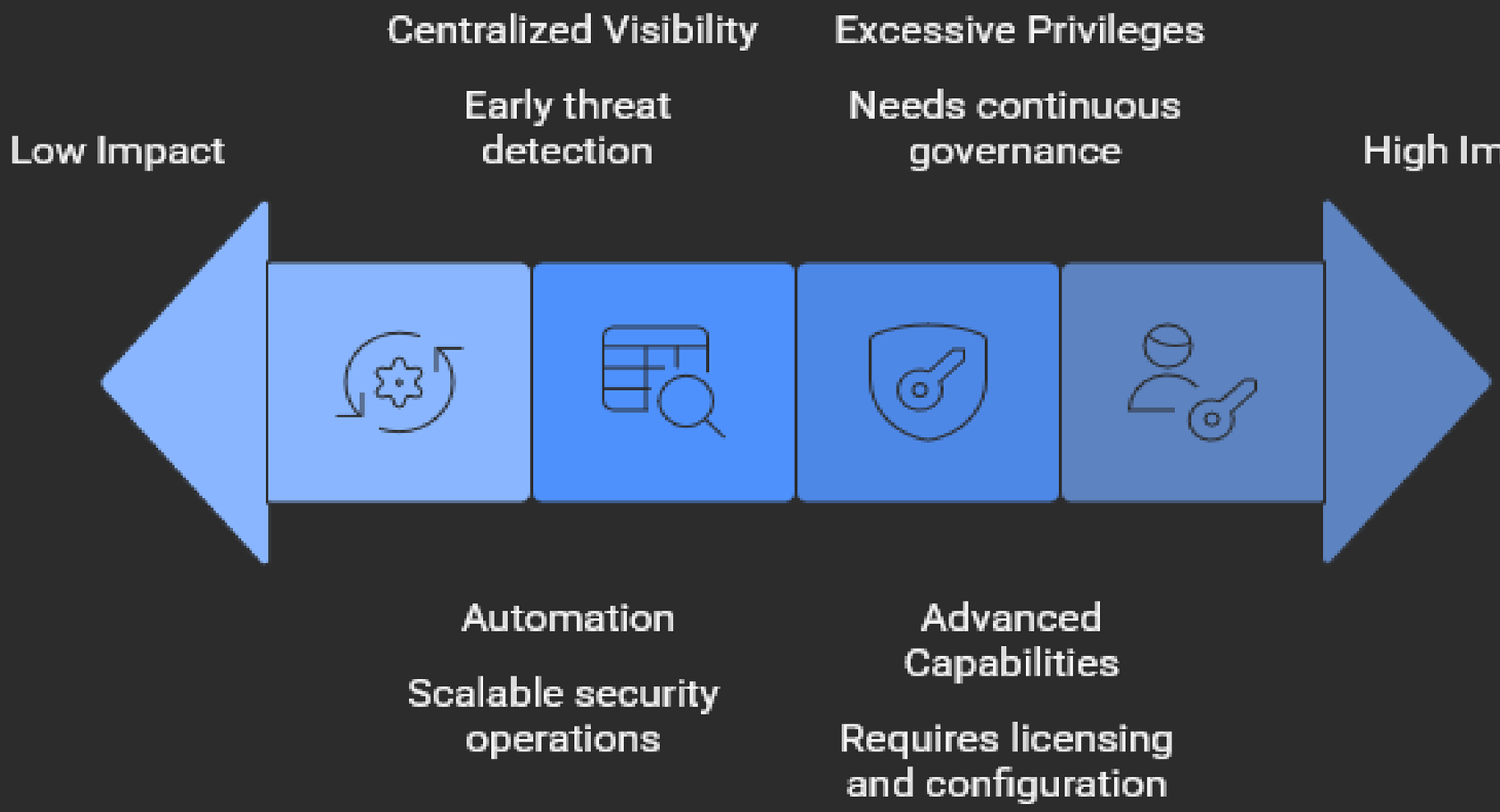


Lab 09: Activity Log monitoring dashboard

Key Findings & Risk Insights

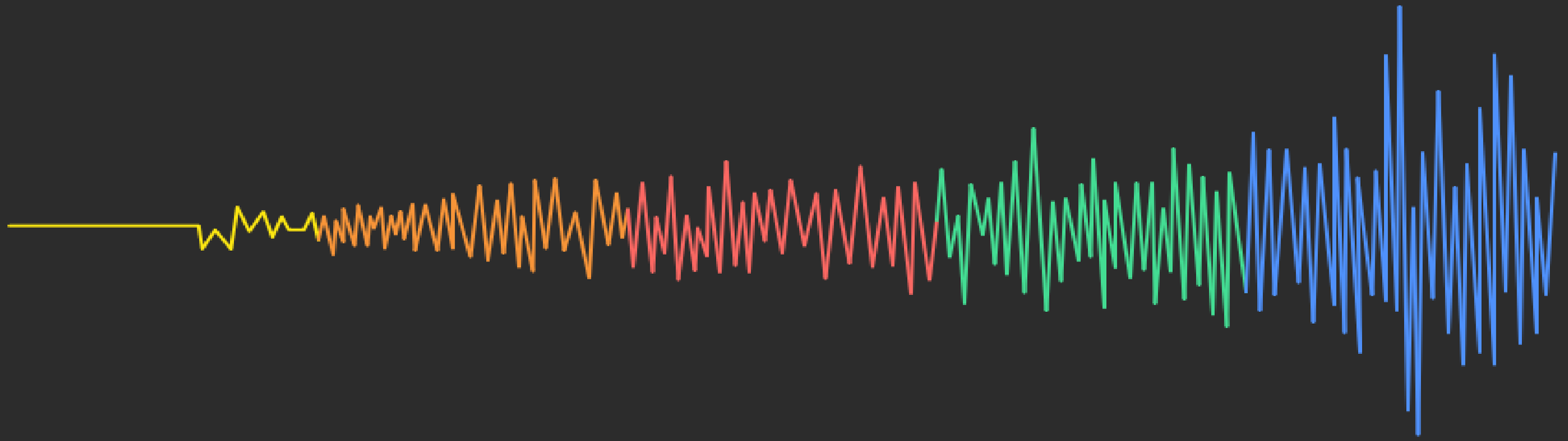


Cloud security risks insights ranked by impact and mitigation effort.



Security recommendations range from reactive to proactive measures.

Reactive ← → Proactive



Strengthen Visibility

Detect suspicious activity before escalation

Regularly Review

Identify misconfigurations and remediate promptly

Enforce Least-Privilege

Remove unnecessary permissions and enforce group access

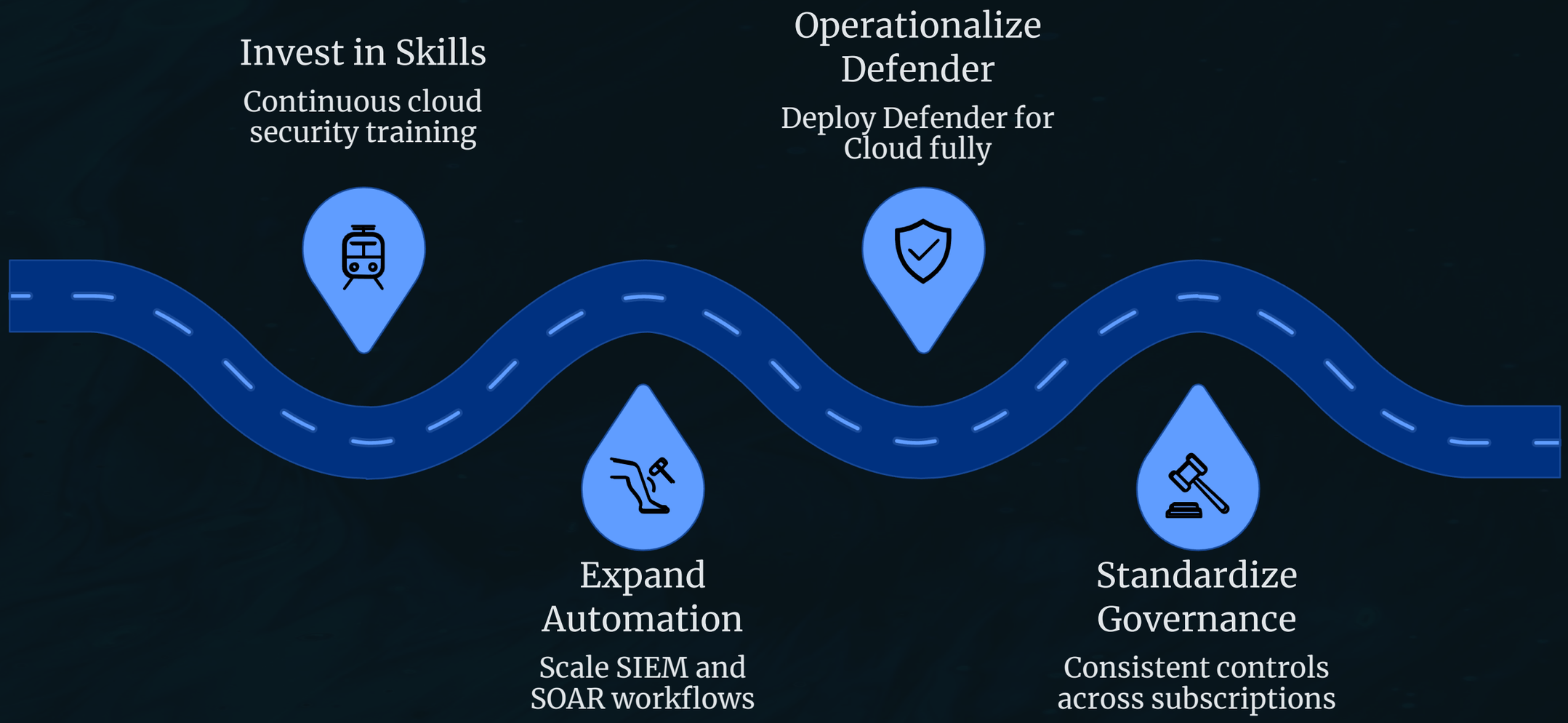
Automate Operations

Deploy playbooks to automate repetitive tasks

Leverage Advanced Features

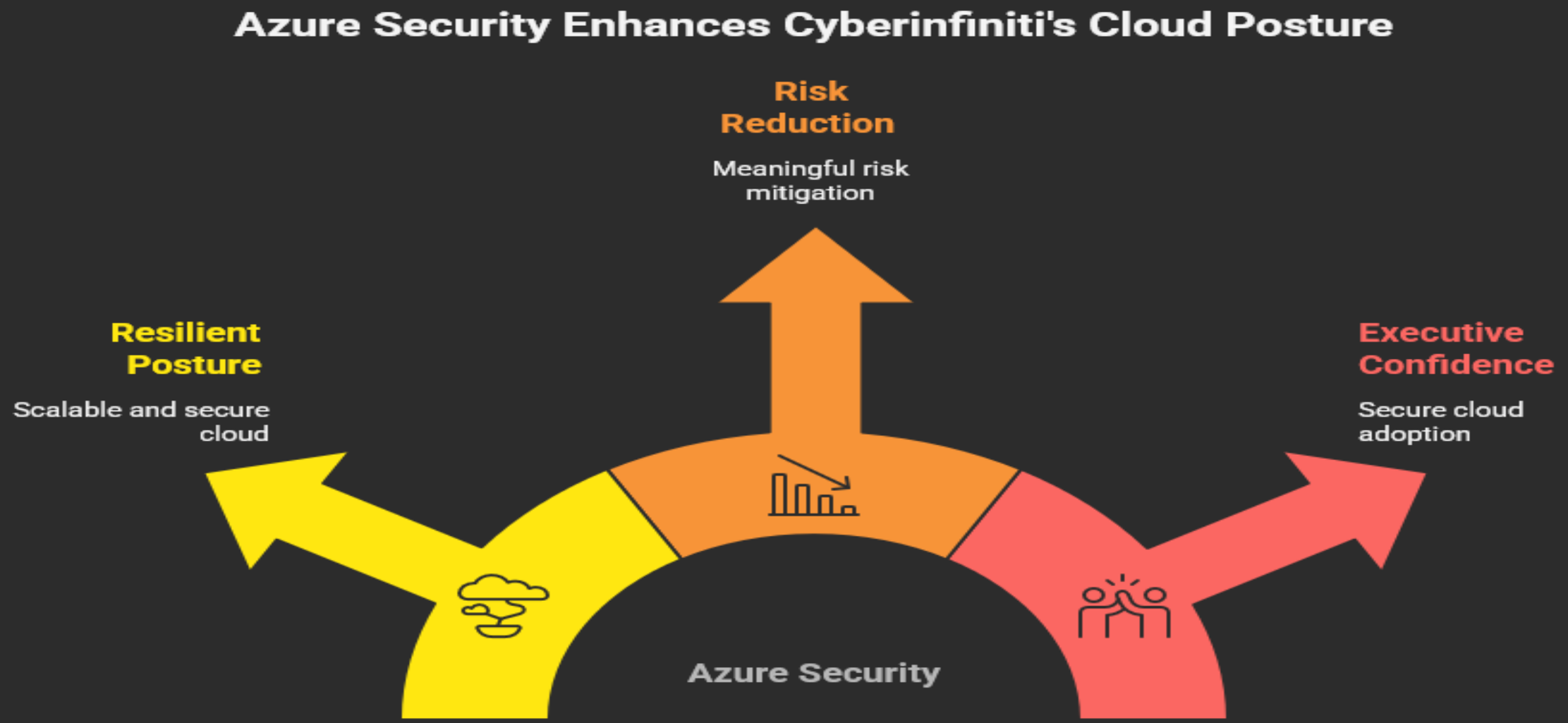
Use threat detection and vulnerability assessments

Security Recommendations cont’d



This strategic roadmap outlines the essential steps for enhancing our cloud security posture.

CONCLUSION


Azure Security Enhances Cyberinfiniti's Cloud Posture
Risk Reduction
Meaningful risk mitigation
Resilient Posture
Scalable and secure cloud
Executive Confidence
Secure cloud adoption
Azure Security

THANK YOU !