Microsoft

SC-100 Microsoft Cybersecurity Architecture

Case study scenario summary: Modernizing Identity and Data Security at Woodgrove Bank

About the organization

Woodgrove Bank

- A US-based financial institution serving over 10 million customers.
- Offers services including consumer banking, investment advisory, and commercial lending.
- Employs thousands of staff and contractors.

IT Infrastructure

Hybrid Model

- Core banking systems are maintained on-premises.
- Customer-facing portals and productivity workloads are hosted in Microsoft Azure and Microsoft 365.

Identity Management

- Utilizes a hybrid identity model.
- On-premises Active Directory is synchronized with Microsoft Entra ID.

Challenges

Identity Management

- Provisioning: Managed independently by business units through automated scripts and manual requests.
- Risk: Role changes and terminations can lead to prolonged elevated privileges.

Guest Access

- Microsoft Entra Guest Accounts: Used for partnerships with external entities.
- Risk: Permissions for guests are similar to internal users, increasing potential security vulnerabilities.

Multi-Factor Authentication (MFA)

- Implementation: Consistently applied for all user and guest access.
- User Feedback: Frequent authentication prompts and account lockouts have led to increased IT helpdesk calls.

Risks

Data Security Risks

- Sensitive Document Management: Customer documents and regulatory reports are sometimes stored improperly.
- Risk: Past incidents of unintentional data sharing due to misplaced files in open-access team sites or guest-enabled collaboration spaces.

Security Incidents

- Telemetry Findings: Unusual sign-in patterns detected, including unexpected locations and failed MFA attempts.
- Risk: Investigations revealed dormant accounts executing elevated PowerShell commands and anomalous access to sensitive SharePoint files.

Architectural Responsibility

Zero Trust Solution

- As the security architect, your responsibility is to design a Zero Trust-aligned solution that mitigates risks and enhances the overall security posture of Woodgrove Bank's hybrid environment.