Microsoft

Zero Trust Assessment and Implementation Plan

A Use Case for a Multinational Multi-Cloud Company

Presented By:

Alaa Eddine AYEDI

“Cloud Security Intern”

Supervised By:

Mr. Karim ABED

Consultim-IT

The Best of Consulting and IT

2024-2025

Agenda

1. **Company Profile & Current State**
2. **Gap Assessment Findings**
3. **Action Plan for Each Pillar**
4. **Implementation Timeline**
5. **Expected Outcomes**
6. **Next Steps & Discussion**

Company Profile

Cyberone Solutions

Technology Services & Consulting

5,000+ employees globally

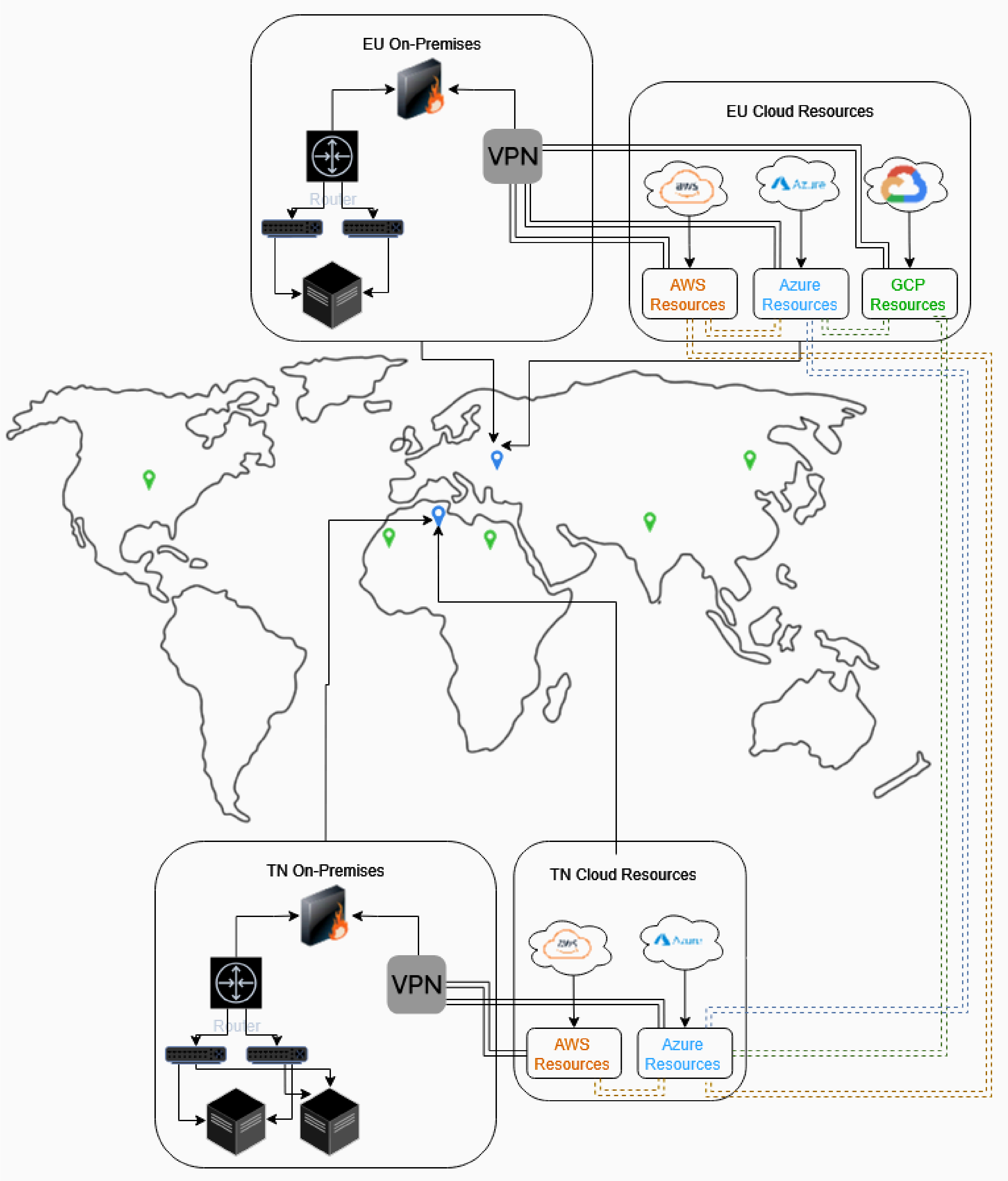
$1.2 billion annually

Headquarters in Europe,
major operations in Tunisia

On-premises data centers
Multicloud strategy (AWS, Azure, GCP)

Traditional perimeter security
Globally distributed remote workforce

Current Architecture



Current Security Challenges

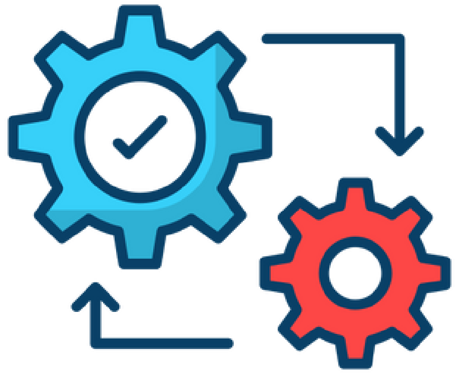
Current Business & Security Challenges

Rising Security Incidents

Remote Workforce Issues

Regulatory Complexity

Cloud Security Inconsistency



M&A Integration

Digital Transformation

Assessment Approach

Microsoft Zero Trust Assessment Methodology

- **Comprehensive Discovery:** Current state analysis across all environments
- **Security Control Mapping:** Inventory of existing controls mapped to Zero Trust pillars
- **Gap Analysis:** Identification of control deficiencies against Microsoft's framework
- **Risk Prioritization:** Ranking of gaps based on business impact and remediation complexity
- **Stakeholder Validation:** Collaborative review of findings with business and technology leaders
- **Roadmap Development:** Creation of phased implementation plan addressing prioritized gaps

Identity

Current State & Gaps

Current State:

- Legacy Active Directory with limited cloud integration
- Basic password-based authentication predominant
- MFA limited to select privileged accounts
- Fragmented identity systems across regions

Key Gaps:

- Lack of unified identity platform across environments
- Absence of risk-based authentication
- Insufficient conditional access policies
- Inadequate privileged access governance
- Limited visibility into identity-based threats

Endpoints

Current State & Gaps

Current State:

- Fragmented endpoint management across regions
- Basic endpoint protection focused on antivirus
- Manual patching processes with compliance gaps
- Limited device inventory and visibility

Key Gaps:

- Inadequate visibility into endpoint security posture
- Inconsistent compliance enforcement
- Limited threat detection and response capabilities
- Absence of secure application controls
- Insufficient endpoint risk assessment

Applications

Current State & Gaps

Current State:

- Legacy applications with network-level access controls
- Limited API security measures
- Minimal application-level monitoring
- Early-stage DevSecOps practices

Key Gaps:

- Lack of centralized application access management
- Insufficient application-level monitoring
- Inadequate API security governance
- Limited implementation of least privilege
- Absence of cloud application security controls

Network

Current State & Gaps

Current State:

- Traditional perimeter-based security model
- VPN-based remote access
- Basic network segmentation
- Inconsistent cloud network controls

Key Gaps:

- Overreliance on perimeter security
- Insufficient micro-segmentation
- Lack of Zero Trust Network Access approach
- Limited visibility into east-west traffic
- Inadequate cloud network security controls

Infrastructure

Current State & Gaps

Current State:

- Traditional data center alongside cloud resources
- Limited infrastructure visibility across environments
- Basic security controls for on-premises infrastructure
- Inconsistent cloud security configurations

Key Gaps:

- Inadequate hybrid infrastructure security governance
- Inconsistent cloud security posture management
- Limited infrastructure monitoring
- Absence of unified infrastructure security policies
- Insufficient automation for security configurations

Data

Current State & Gaps

Current State:

- Basic data classification
- Limited data loss prevention
- Inconsistent encryption practices
- Minimal data access governance

Key Gaps:

- Lack of comprehensive data classification
- Insufficient data protection controls
- Inconsistent encryption implementation
- Limited data access governance
- Absence of unified data security strategy

Current vs. Future State Overview

Security Domain	Current State	Future State with Microsoft Technologies
Identity	Legacy AD, basic auth, limited MFA	Microsoft Entra ID, passwordless, risk-based Conditional Access
Endpoints	Basic protection, manual patching	Intune + Defender for Endpoint, automated compliance
Applications	Network-level access, minimal API security	Entra app proxy, MCAS, API Management, WAF
Network	Perimeter VPN, limited segmentation	Virtual WAN, ZTNA, micro-segmentation
Infrastructure	Traditional DC + cloud, limited visibility	Azure Arc, Defender for Cloud, unified security policies
Data	Limited classification, basic controls	Purview, sensitivity labels, DLP, Information Protection

Microsoft Entra ID

Identity

Action Plan

Priority Actions:

1. Deploy Microsoft Entra ID as central identity provider
2. Establish hybrid identity with Entra ID Connect
3. Implement passwordless authentication with Microsoft Authenticator
4. Configure risk-based Conditional Access policies
5. Deploy Entra Privileged Identity Management (PIM)
6. Establish Just-In-Time (JIT) administrative access
7. Configure Privileged Access Workstations (PAWs)
8. Implement continuous access evaluation

Microsoft Technologies:

- Entra ID, Authenticator, Conditional Access, PIM, Identity Protection

Endpoints

Action Plan

Priority Actions:

1. Deploy Microsoft Intune for unified endpoint management
2. Implement comprehensive device compliance policies
3. Deploy Microsoft Defender for Endpoint across all devices
4. Establish vulnerability management program
5. Implement application control with Microsoft Defender Application Control
6. Configure attack surface reduction rules
7. Deploy automated remediation workflows
8. Implement secure remote access with device health attestation

Microsoft Technologies:

- Intune, Defender for Endpoint, Defender Application Control

Applications

Action Plan

Priority Actions:

1. Implement Entra ID Application Proxy for legacy applications
2. Deploy Microsoft Defender for Cloud Apps (CASB)
3. Establish API security with Azure API Management
4. Implement Web Application Firewall (WAF)
5. Integrate security into DevOps with Defender for DevOps
6. Deploy Azure Key Vault for secrets management
7. Implement application-level conditional access
8. Establish continuous application security monitoring

Azure Keyvault

Microsoft Technologies:

- Application Proxy, Defender for Cloud Apps, API Management, WAF, Key Vault

Network

Action Plan

Priority Actions:

1. Implement Azure Virtual WAN to replace traditional VPN
2. Deploy Azure Firewall for cloud-native network security
3. Establish micro-segmentation with Network Security Groups
4. Implement Zero Trust Network Access (ZTNA)
5. Deploy Defender for Cloud Apps for CASB functionality
6. Configure Azure Front Door for secure application delivery
7. Implement Azure Network Watcher for traffic analysis
8. Deploy Azure DDoS Protection

Microsoft Technologies:

- Virtual Network, Azure Firewall, NSGs, Front Door, Network Watcher, DDoS Protection

Infrastructure

Action Plan

Priority Actions:

1. Deploy Azure Arc for hybrid infrastructure management
2. Implement Microsoft Defender for Cloud across all environments
3. Establish unified security policies
4. Deploy infrastructure-level threat protection
5. Implement automated compliance monitoring
6. Establish infrastructure-level identity controls
7. Deploy security posture management
8. Implement automated remediation for infrastructure

Microsoft Technologies:

- Azure Arc, Defender for Cloud, Azure Policy, Defender for Servers

Data

Action Plan

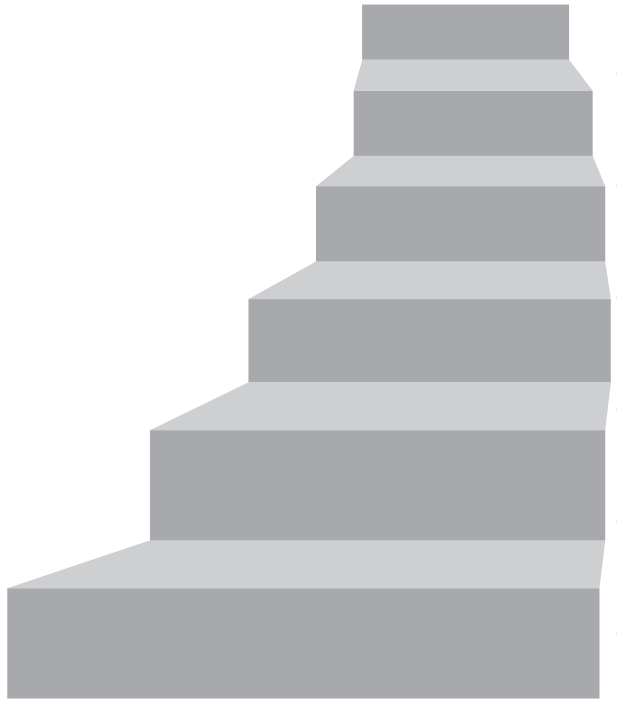
Priority Actions:

1. Deploy Microsoft Purview for data classification and governance
2. Implement sensitivity labels across Microsoft 365
3. Establish Data Loss Prevention (DLP) policies
4. Configure Azure Information Protection
5. Implement data access governance with Entra ID Entitlement Management
6. Deploy Defender for Cloud Apps for data security
7. Establish automated data discovery and classification
8. Implement comprehensive encryption strategy

Microsoft Technologies:

- Purview, DLP, Information Protection, Entitlement Management

Implementation Timeline Overview



- **Phase 1 :** Identity Foundation
- **Phase 2 :** Endpoint Security
- **Phase 3 :** Application Security
- **Phase 4 :** Network Security Transformation
- **Phase 5 :** Cross-Pillar Integration and Optimization
- **Phase 6 :** Data Security

Identity Foundation

Key Activities:

- Detailed identity assessment
- Microsoft Entra ID deployment
- Hybrid identity configuration
- Initial Conditional Access policies
- MFA rollout starting with privileged accounts
- Basic privileged access management
- Initial monitoring and alerting
- User awareness training

Key Milestones:

- Complete Entra ID deployment
- 100% MFA coverage for privileged accounts
- Baseline Conditional Access policies

Endpoint Security

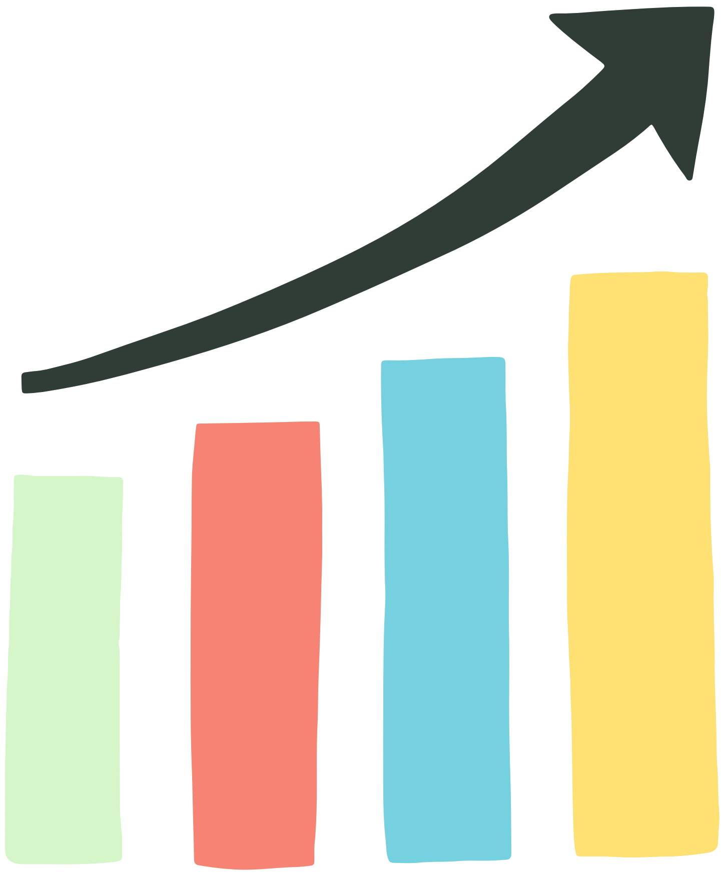
Key Activities:

- Comprehensive endpoint inventory
- Microsoft Intune deployment
- Device compliance policy development
- Microsoft Defender for Endpoint deployment
- Vulnerability management configuration
- Initial application control policies
- Automated remediation workflows
- Security operations training

Key Milestones:

- Complete Intune deployment
- 90% endpoint coverage with Defender
- Baseline compliance policies

Application Security



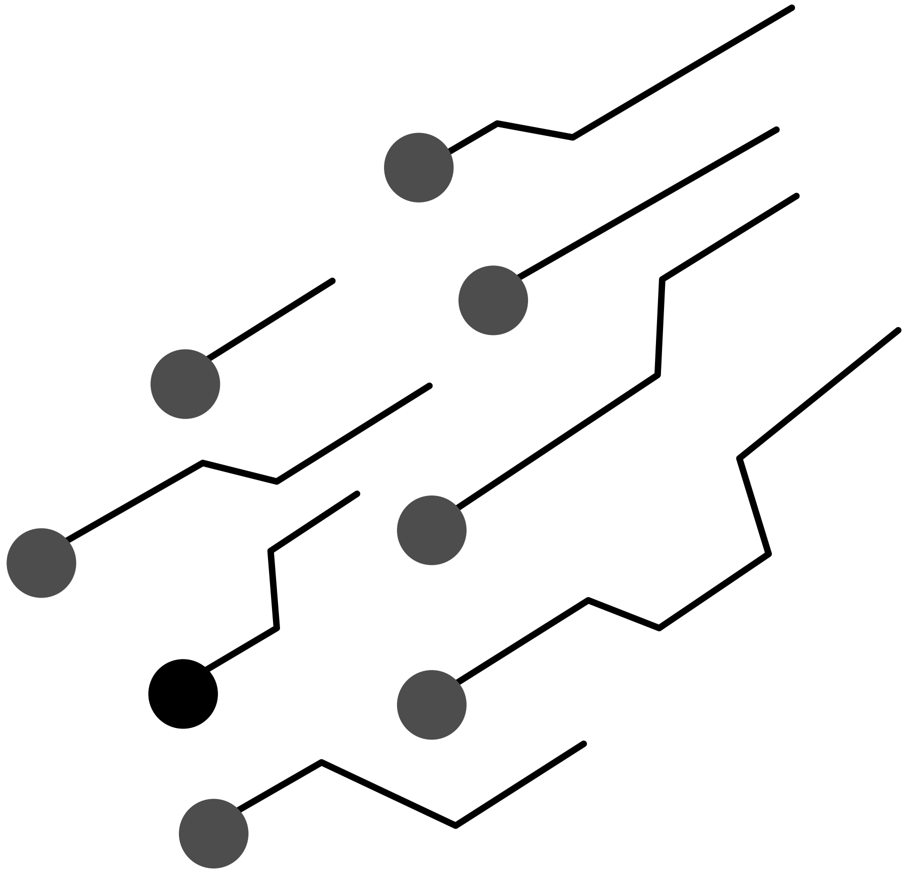
Key Activities:

- Application inventory and risk assessment
- Application proxy implementation for legacy apps
- Microsoft Defender for Cloud Apps deployment
- API security control implementation
- Web Application Firewall deployment
- Application-level monitoring configuration
- DevSecOps pipeline integration
- Secrets management deployment

Key Milestones:

- Complete application inventory
- Implement CASB controls
- Establish DevSecOps foundation

Network Security Transformation



Key Activities:

- Detailed network assessment
- Azure Virtual WAN implementation
- Initial microsegmentation policies
- Zero Trust Network Access for critical applications
- Azure Firewall configuration
- Network monitoring implementation
- Begin phasing out traditional VPN
- DDoS protection implementation

Key Milestones:

- Complete Virtual WAN deployment
- Microsegmentation for critical systems
- Begin legacy VPN decommissioning

Cross-Pillar Integration

Key Activities:

- Microsoft Sentinel deployment
- Cross-pillar automation implementation
- Comprehensive dashboard development
- Advanced analytics configuration
- Automated response workflow deployment
- Integrated security testing
- Continuous improvement process establishment
- Comprehensive metrics and reporting development

Key Milestones:

- Deploy Sentinel
- Implement automation workflows
- Establish Zero Trust dashboard

Data Security

Key Activities:

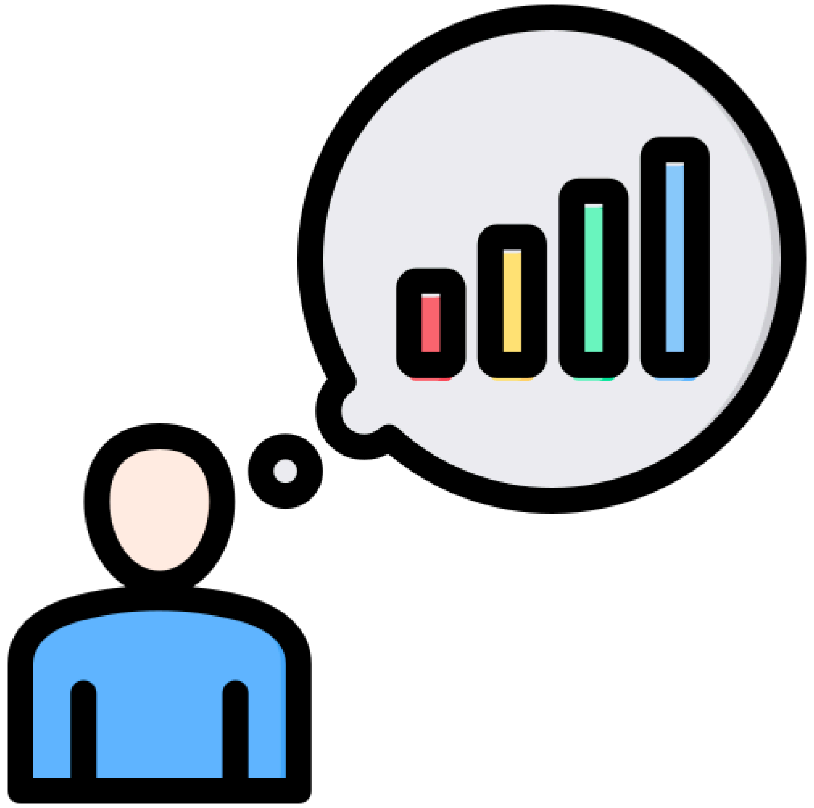
- Data discovery and classification
- Microsoft Purview deployment
- Sensitivity label implementation
- Data Loss Prevention configuration
- Data access governance establishment
- Encryption control deployment
- Data security monitoring implementation
- Data handling training

Key Milestones:

- Complete initial data classification
- Implement DLP controls
- Establish data governance framework

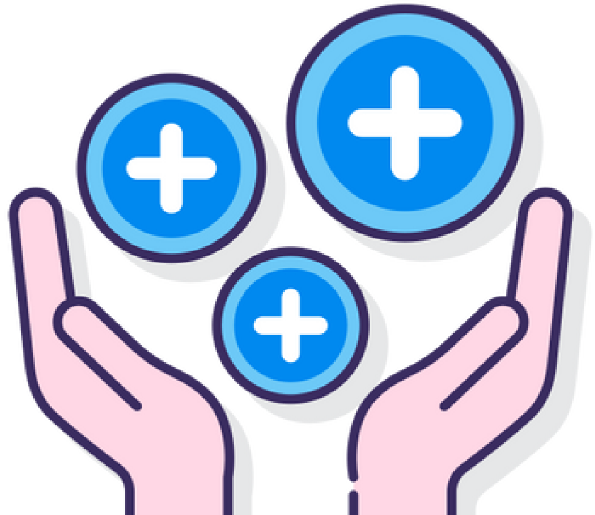
Security Improvement Expectations

- reduction in identity-based compromises
- reduction in privileged access misuse
- improvement in authentication security posture
- reduction in endpoint-based security incidents
- improvement in endpoint compliance rates
- reduction in malware incidents
- decrease in lateral movement during security testing
- reduction in network-based attack surface
- improvement in network visibility
- improvement in mean time to detect (MTTD)
- improvement in mean time to remediate (MTTR)
- reduction in overall security incidents



Operational Benefits

- reduction in VPN-related help desk tickets
- improvement in remote worker experience
- reduction in authentication-related issues
- reduction in manual security operations
- improvement in cross-environment visibility
- reduction in security alert noise
- faster onboarding time for new acquisitions
- reduction in security-related project delays
- improvement in time-to-market for new initiatives



Compliance Outcomes

- Unified compliance reporting across all regions
- Automated evidence collection for regulatory audits
- reduction in compliance gaps
- reduction in time required for compliance audits
- improvement in audit preparation efficiency
- reduction in audit findings
- Comprehensive risk visibility across all environments
- Proactive risk mitigation capabilities
- Improved ability to demonstrate compliance to regulators

Technology Investments

Microsoft Security Suite

- Microsoft Entra ID (Identity & Access Management)
- Microsoft Intune (Endpoint Management)
- Microsoft Defender (XDR Platform)
- Microsoft Purview (Data Security & Compliance)
- Microsoft Sentinel (SIEM & SOAR)

Azure Security Services

- Azure Virtual WAN & Azure Firewall
- Azure Key Vault
- Azure API Management
- Azure Front Door & WAF
- Azure DDoS Protection

Thank You!

Contact Information:

- Cloud Security Intern: *Alaa Eddine Ayedi*
- Email: *alaa.ayedi.personal@gmail.com*
- Phone: *(+216) 20468880*

Reference Materials:

- *Microsoft Zero Trust Framework documentation*