**Project: Module 5**

**Objective:**

This project focuses on identifying, analyzing, and mitigating critical cybersecurity risks within XYZ Corp’s hybrid IT environment. The goal is to evaluate the organization’s current infrastructure using established threat analysis frameworks and design a secure, modernized network architecture aligned with industry best practices.

**Scope of Work:**

The assessment targets both on-premise and cloud-based systems across all major departments, including Finance, IT, Sales, HR, Marketing, and Operations. The organization’s infrastructure includes 500 endpoints, 10 servers, and a range of Azure cloud services. The project addresses key areas such as endpoint protection, network segmentation, identity and access management, logging and monitoring, and cloud security configurations.

**Methodology:**

MITRE ATT&CK Framework is applied to map real-world adversarial techniques to existing vulnerabilities.

A current-state network diagram is created to visualize existing weaknesses, followed by a redesigned infrastructure diagram to illustrate proposed improvements.

A gap analysis is conducted to highlight missing or insufficient controls.

Cryptographic principles such as AES encryption, RSA key exchange, hashing, and digital signatures are demonstrated in securing data communication.

**Deliverables:**

A network diagram of the current infrastructure.

A detailed gap analysis using MITRE ATT&CK and/or STRIDE.

A redesigned infrastructure diagram with enhanced security features.

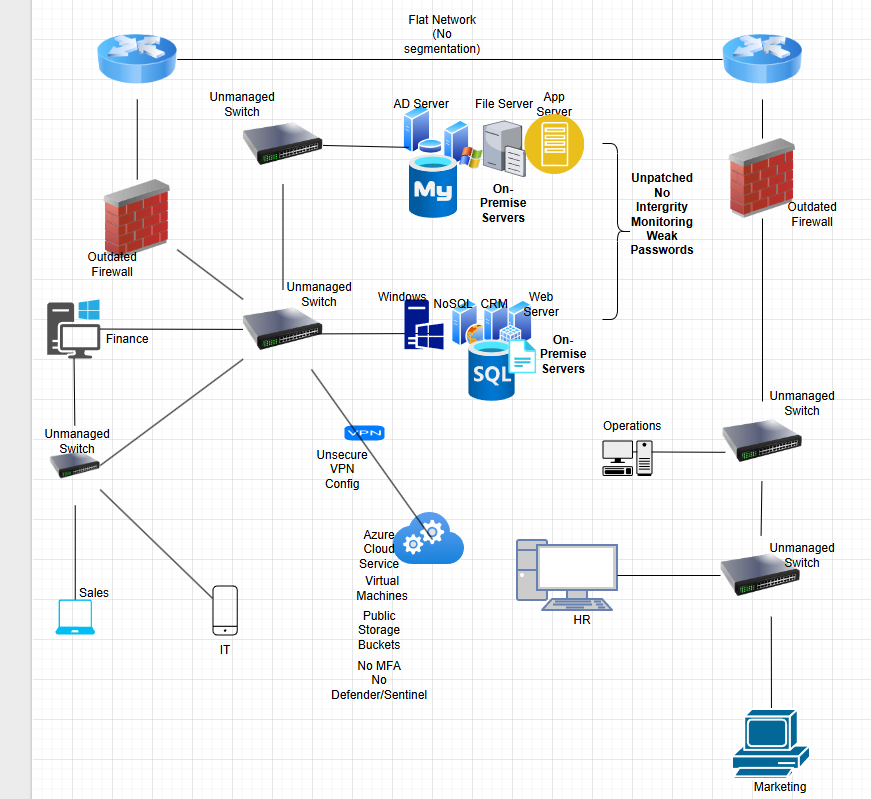
A justification document outlining selected cybersecurity tools and design choices.

**Outcome:**

The final deliverables provide XYZ Corp with a roadmap to transition from a vulnerable flat network environment to a segmented, secure, and monitored infrastructure. This approach improves visibility, reduces risk exposure, and aligns with compliance standards such as ISO 27001, GDPR, and PCI-DSS.

**Deliverable One**: **Current Network Diagram**

This deliverable involves creating a visual representation of XYZ Corp’s existing network infrastructure. The diagram highlights all key components—endpoints, servers, cloud services, and networking devices—along with major security weaknesses such as flat architecture, outdated firewalls, and misconfigured cloud settings. It serves as a baseline for identifying vulnerabilities and planning improvements in later phases of the project.

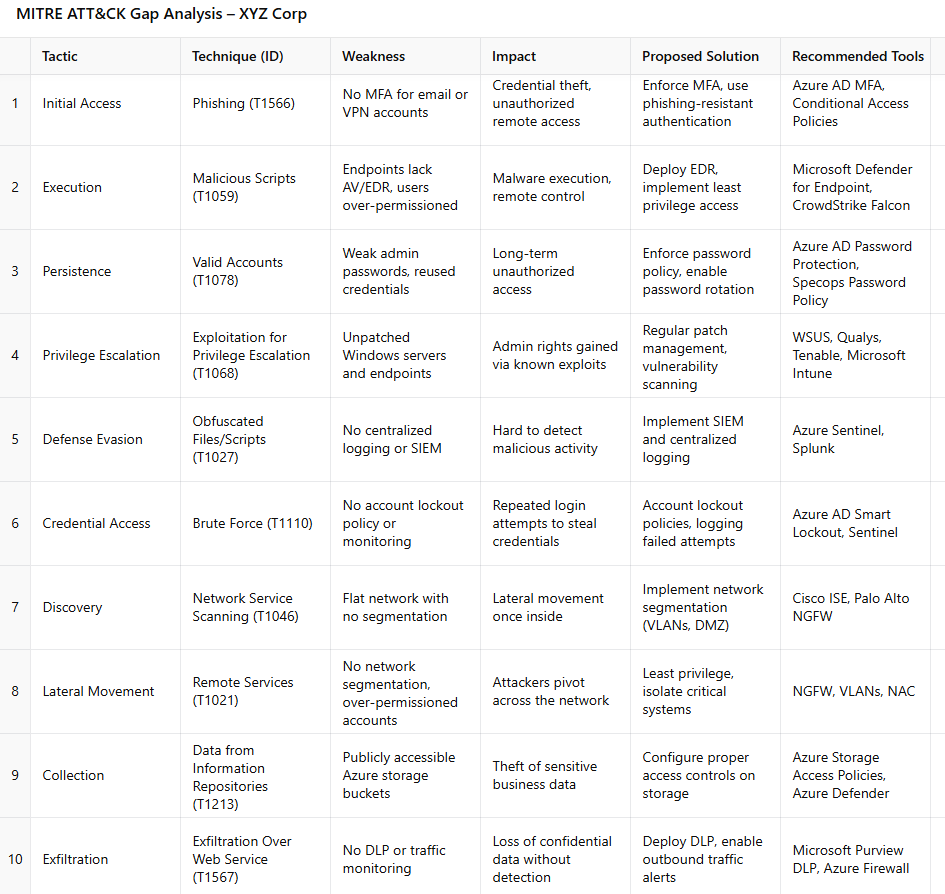


**Deliverable Two:** **Gap Analysis Using MITRE ATT&CK**

This part of the project focuses on identifying real security weaknesses in XYZ Corp’s current IT setup by using the MITRE ATT&CK Framework. This framework helps map out how real-world attackers typically operate—step by step—so it’s easier to see where the organization is most at risk.

At least ten key vulnerabilities were identified across different areas of the network, such as unpatched servers, weak endpoint protection, lack of multi-factor authentication, and publicly accessible cloud storage. Each of these issues was matched to a specific attacker tactic and technique from MITRE’s database.

For every gap found, a clear solution is suggested—along with the right tools to fix it. This analysis doesn’t just point out what’s wrong; it also lays the foundation for improving the organization’s overall security and guides the changes made in the redesigned network.



**Deliverable 3: Redesigned Infrastructure Diagram**

Securing servers is a vital part of protecting the organization’s infrastructure. In this project, a layered security approach was applied to safeguard both on-premise and cloud-based servers. Critical public-facing systems, like the web server, are placed in a DMZ (Demilitarized Zone) to isolate them from internal resources and reduce exposure to internet-based threats. Behind the internal firewall, core servers such as Active Directory, file servers, and databases are protected with endpoint detection and response (EDR) tools, strict patch management, and access controls. Encryption is used to secure data at rest and in transit, while all server activity is logged and monitored through a centralized SIEM platform. These combined measures help prevent unauthorized access, data breaches, and system compromise while maintaining strong visibility and control.

Below is a screenshot that mirrors all the applied security measures:

