Security Enhancement Plan for SecureTech Inc.

SecureTech Inc. is actively addressing key cybersecurity challenges, including unauthorized access to file systems, outdated infrastructure, and a rising number of phishing incidents. To mitigate these threats, the company will implement least privilege access policies, strengthen multi-factor authentication (MFA), modernize its patch management strategy, and initiate phishing simulations alongside targeted employee training.

Over the next 30 days, critical objectives include tightening access control mechanisms, auditing and optimizing firewall configurations, completing a thorough asset inventory, and launching comprehensive security awareness programs. Each initiative has clearly assigned ownership to ensure cross-departmental accountability and timely execution.

Primary Threats Include:

- Phishing Attacks
- Social Engineering
- Man-in-the-Middle (MitM) Attacks
- Distributed Denial of Service (DDoS)
- Brute Force Login Attempts

Threat Prioritization

Threat	Vulnerability	Priority	Justification
Phishing Attacks	Employee emails workstations	High	Due to multiple employee reports of receiving phishing emails
Social engineering	Employee	Medium	Employees should know how to be aware of social engineering while being on the system
Brute Force Log In	MFA	High	The IT department reports a surge in failed login attempts to the email server, traced back to IP addresses in regions where SecureTech Inc. has no business operations.
Man in the Middle Attack	Encryption	High	A critical file server shows signs of unauthorized access, with some files unexpectedly modified or deleted.
DDOS Attack	Network Tools MFA	High	Network monitoring tools detected abnormal traffic patterns, including spikes in outbound data transfers occurring late at night.

Threats, Vulnerabilities, and Recommended Mitigations

Threat/Vulnerability	Recommendation	Justification
Phishing	Employee training Email Filtering	As employees are trained more regarding phishing they wont be subject to click into links from fraudulent companies.
Man in the Middle	Implement MFA Implement Encryption Implement Strong Password	MFA and strong password creates a more secure log in process for a user. With Encryption, this creates the need to have a key.
DDOS	Robust infrastructure Patch and Update systems Using Firewalls	Put a stop to the unwanted network interference

Data Types, Solutions, and Applications

Data Type	Solution	Application	Benefit
Healthcare, HPPA	Data Protection Services	Data Backup and Recovery	Protecting health care data from being breched.
Financial	Data Protection Services	Access Control	Ensures only authorized individuals have access to this information
Phishing Emails	Employee Training to understand how to spot it.	Employee Training Email Filtering	Teach employee's how to spot phishing attacks before they can fall subject to them.
Network Intrusion	Patch & Update systems	System Updates	Prevent unwanted network interference
Employee and Client Data	Data Protection Services	Access Control	Ensures only authorized individuals have access to the information necessary.

Conclusion

This Security Enhancement Plan aims to reinforce the safety and integrity of SecureTech Inc.'s infrastructure. Based on identified threats and vulnerabilities, we have outlined targeted solutions, their applications, and the rationale behind each recommendation.

From completing this project, I gained valuable hands-on experience and recognized how crucial reading comprehension is in identifying threats hidden in documentation. Understanding how attacks are described is just as important as defending against them.

Of all the recommendations provided, I believe employee training stands out as the most impactful. Phishing remains one of the most common and preventable threats—proper education can empower staff to spot and avoid suspicious emails, significantly reducing organizational risk.