Executive Summary

Our red team engagement targeted your organization's defenses with the goal of identifying realistic attack vectors and strengthening your security posture. The most significant finding was a successful phishing attack (T1566), which provided initial access to your environment. From there, the attacker conducted lateral movement, privilege escalation, and ultimately exfiltrated sensitive data. These findings indicate areas for immediate improvement in authentication controls, network segmentation, and threat monitoring.

Findings

- Phishing (TID1566): Attackers gained initial access by exploiting the trust of end users through a convincing phishing email, resulting in credential compromise.
- Internal Network Access: After initial compromise, attackers interacted with internal systems, exposing network segmentation weaknesses.
- Lateral Movement: Using compromised credentials, the attacker moved between systems, increasing their access footprint.
- Privilege Escalation: The attacker escalated privileges to obtain greater control over critical systems.
- Data Exfiltration: Sensitive data were exfiltrated from the environment, highlighting deficiencies in data loss prevention and monitoring.

Findings Table

Finding ID	TTP	CVSS Score	Remediation
FID001	Phishing (T1566)	7.5	MFA enforcement

Recommendations

- Enforce Multi-Factor Authentication (MFA): Require MFA for all user accounts to prevent unauthorized access even if credentials are compromised.
- Improve Network Segmentation: Restrict lateral movement by segmenting networks and enforcing the principle of least privilege.
- Enhance Phishing Awareness: Provide regular training to help employees recognize and report phishing attempts.
- Monitor for Lateral Movement: Deploy detection mechanisms to identify suspicious internal activity, such as unusual logins and data transfers.
- Data Loss Prevention: Implement controls to monitor and prevent unauthorized exfiltration of sensitive information.

During this assessment, our team simulated common cyberattack techniques, starting with a phishing campaign that successfully tricked employees into enabling access to your network. Once inside, the attacker was able to move between systems, escalate privileges, and ultimately remove sensitive data—demonstrating how quickly a single breach can escalate into serious business risk. The findings underscore the need for stronger access controls, ongoing employee awareness, and advanced monitoring. By prioritizing multi-factor authentication, network segmentation, and timely detection, your organization can significantly reduce exposure to similar real-world threats. We are prepared to work with your team to implement these improvements and enhance your cyber resilience.