🔮 Preventive Mitigations:

🔮 Preventive Solution #1

Solution #1 M1017: User Training	**Difficulty:** 1 (Easy)	**Priority:** 3 (High)
Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.		
Addresses attack vector(s):	T1566: Phishing, T1036: Masquerading, T1078: Valid Accounts, T1020: Automated Exfiltration, T1528: Steal Application Access Token	

STAKEHOLDERS		
Executives	**IT Team**	**Legal**
Resolve the lack of security training by scheduling & enforcing basic cybersecurity training to increase awareness of different common threats used to attack business online. This will save the company time & ultimately money.	Security training reduces risk of incidents.	Reduces risk of breaches which helps to meet regulatory compliance.

GOALS		
Name	**Description**	**Deadline**
User Training	Our goal would be to implement quarterly cybersecurity awareness training.	The IT department should conduct demonstrations quarterly.

🔮 Preventive Solution #2

Solution #2 M1018: User Account Management	**Difficulty:** 2 (Medium)	**Priority:** 3 (High)
Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.		

Consider defining and enforcing a naming convention for user accounts to more easily spot generic account names that do not fit the typical schema.

Enforce the principle of least privilege by limiting privileges of user accounts so only authorized accounts can modify and/or add server software components.

Regularly audit user accounts for activity and deactivate or remove any that are no longer needed.

Enforce role-based access control to limit accounts to the least privileges they require. A Cloud Access Security Broker (CASB) can be used to set usage policies and manage user permissions on cloud applications to prevent access to application access tokens. In Kubernetes applications, set "automountServiceAccountToken: false" in the YAML specification of pods that do not require access to service account tokens.

Addresses attack vector(s):	T1110: Brute Force, T1036: Masquerading, T1505: Server Software Component: SQL Stored Procedures, T1078: Valid Accounts, T1020: Automated Exfiltration, T1528: Steal Application Access Token

STAKEHOLDERS		
Executives	**IT Team**	**Legal**
By strengthening User Account Management, it will lower cost, increase efficiency while increasing security.	By following PoLP it will minimize potential damage from breaches. It will also help prevent human error & will prevent the spread of malware.	The company should follow PoLP guidelines & enforce things like MFA. By being PCI-DSS compliant, the company will save money & avoid fines.

GOALS		
Name	**Description**	**Deadline**
M1018: User Account Management	Manage the creation, modification, use, and permissions associated to user accounts.	2 Months

🔮 Preventive Solution #3

Solution #3 M1016: Vulnerability Scanning	**Difficulty:** 1 (Easy)	**Priority:** 3 (High)

Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.

Addresses attack vector(s):	T1566: Phishing, T1036: Masquerading, T1078: Valid Accounts, T1020: Automated Exfiltration, T1528: Steal Application Access Token	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
By improving vulnerability management the organization can reduce risk, minimize downtime & ensure operations of IT infrastructure.	By improving vulnerability management the organization can reduce risk, minimize downtime & ensure operations of IT infrastructure.	Lack of compliance can lead to fines. As a result, our suggestion would be to continuously scan the network & to employ a proper patch management policy. This will increase compliance & decrease the likelihood of fines.
GOALS		
Name	**Description**	**Deadline**
M1016: Vulnerability Scanning	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.	6 months to 1 year