Catfish

Compromised Administrator Account Response Plan

The Facts Were These: Someone used the credentials of a domain admin to perform unauthorized actions, such as creating new accounts and changing group policies.

Below is a breakdown of each phase of the plan and a rough estimate of the timeline starting from the detection of the threat to the recovery stage.

Immediate Actions (0-15 minutes)

Detection

Unusual administrative activities detected.
New user accounts created unexpectedly.
Group policy changes without authorization.
Privileged access monitoring alerts.

Initial Response

Disable compromised administrator account immediately.
Reset all administrative account passwords.
Revoke active sessions for administrative accounts.
Enable enhanced logging for administrative activities.

Containment (15 minutes - 1 hour)

Access Control

Review and audit all administrative accounts.
Disable unnecessary administrative privileges.
Implement emergency access controls.
Monitor for continued suspicious activities.

System Security

Review recent system changes and configurations.
Audit Active Directory for unauthorized changes.
Check for new user accounts and group memberships.
Verify system integrity and security settings.

Investigation (1-8 hours)

Activity Analysis

Review Active Directory logs for unauthorized changes.
Analyze administrative access logs and activities.
Check for lateral movement and privilege escalation.
Identify scope of unauthorized access.

Impact Assessment

Assess data and system compromise.
Review configuration changes and their impact.
Identify affected systems and users.
Document timeline of malicious activities.

Recovery (8-24 hours)

System Restoration

Restore unauthorized system changes.
Remove unauthorized user accounts and access.
Implement additional security controls.
Verify system integrity and functionality.

Access Management

Implement least privilege principles.
Review and update administrative procedures.
Implement multi-factor authentication.
Update password policies and procedures.

Communication	
Internal	**External**
Notify executive leadership immediately.	Consider law enforcement notification.
Inform legal and compliance teams.	Report to regulatory authorities if required.
Update IT operations and security teams.	Coordinate with security vendors.
Coordinate with human resources if needed.	Update customers if services are affected.

Post-Incident

Implement privileged access management (PAM).

Conduct regular access reviews.

Implement continuous monitoring.

Update administrative procedures and training.