Account Access Removal via Multi-Platform Audit Correlation, Detection Strategy DET0120

Archived: 2026-04-02 12:37:44 UTC

AN0334

Correlated user account modification (reset, disable, deletion) events with anomalous process lineage (e.g., PowerShell or net.exe from an interactive session), especially outside of IT admin change windows or by non-admin users.

Log Sources

Mutable Elements

Field	Description
UserContext	Account performing the operation (e.g., Domain Admins vs. local users)
TimeWindow	Alert only on actions outside of maintenance windows
ParentProcessName	Detect suspicious process lineage (e.g., powershell.exe launching net.exe)

AN0335

Password changes or account deletions via 'passwd', 'userdel', or 'chage' preceded by interactive shell or remote command execution from non-privileged accounts.

Log Sources

Mutable Elements

Field	Description
ExecPath	Binary path for passwd or userdel, which may vary by distro
NonRootUIDThreshold	Alert only if auid != root or expected service account

AN0336

Execution of dscl or sysadminctl commands to disable, delete, or modify users combined with anomalous process ancestry or terminal session launch.

Log Sources

Mutable Elements

Field	Description
CommandLinePattern	Allow variation in dscl/sysadminctl command structure
AnomalousUserFlag	Detect new or rarely seen users performing user removal

AN0337

Invocation of esxcli 'system account remove' from vCLI, SSH, or vSphere API with anomalous user access or outside maintenance windows.

Log Sources

Mutable Elements

Field	Description
RemoteUserRole	ESXi role triggering the change (e.g., Administrator vs. Viewer)
ExpectedIPs	IP ranges authorized to conduct admin-level actions

AN0338

O365 UnifiedAuditLog entries for Remove-Mailbox or Set-Mailbox with account disable or delete actions correlated with suspicious login locations or MFA bypass.

Log Sources

Mutable Elements

Field	Description
RoleAssignment	Determine if operation was delegated to expected admin group
GeoThreshold	Trigger on unusual geographic login sources

AN0339

Deletion or disablement of user accounts in platforms like Okta, Salesforce, or Zoom with anomalies in admin session attributes or mass actions within short duration.

Log Sources

Mutable Elements

Field	Description
BulkActionThreshold	Trigger if multiple deletions occur within a short period
SessionDeviceType	Alert on deletions initiated from unfamiliar device contexts

---