Password Policy Discovery – cross-platform behavior-chain analytics, Detection Strategy DET0161

Archived: 2026-04-05 13:53:45 UTC

AN0455

Cause→effect chain: (1) a user or service spawns a shell/PowerShell that queries local/domain password policy via commands/cmdlets (e.g., `net accounts`, `Get-ADDefaultDomainPasswordPolicy`, `secedit /export`); (2) optional directory/LDAP reads from DCs; (3) same principal performs adjacent Discovery or credential-related actions within a short window. Correlate sysmon process creation with PowerShell ScriptBlock and Security logs.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window between policy query and adjacent suspicious activity (e.g., 15–30 minutes).
PrivilegedUserAllowList	Accounts (e.g., Helpdesk) allowed to run policy queries routinely.
HostRoleScope	Limit alerts on DCs/management servers; raise on user workstations/VDI.
PS_ScriptBlockPatterns	Cmdlet/function names to treat as high-signal in your environment.

AN0456

Chain: (1) interactive/non-interactive `chage -l`, `grep` / `cat` of PAM config (e.g., `/etc/pam.d/common-password`, `/etc/security/pwquality.conf`); (2) optional reads of `/etc/login.defs`; (3) same user performs account enumeration or password change attempts shortly after. Use auditd `execve` and file read events plus shell history collection.

Log Sources

Mutable Elements

Field	Description
MonitoredPaths	Exact PAM/QoP config files used by your distro (Debian vs. RHEL paths differ).
ServiceAccountsExclude	System daemons that legitimately parse policies on boot.

Field	Description
TerminalType	TTY vs. non-interactive—raise risk for non-interactive remote execution.

AN0457

Chain: (1) execution of `pwpolicy` or MDM/DirectoryService reads of account policies; (2) optional read of `/Library/Preferences/com.apple.loginwindow` or config profiles; (3) follow-on credential probing or lateral movement by same user/session. Use unified logs and process telemetry.

Log Sources

Mutable Elements

Field	Description
MDMProfileIDs	Approved profiles reading/updating auth policies.
AdminConsoleHosts	Jamf or management hosts where queries are expected.

AN0458

Chain: (1) cloud API calls that fetch tenant/organization password policy (e.g., AWS `GetAccountPasswordPolicy`, GCP/OCI equivalents or IAM settings reads); (2) within a short window, the same principal creates users, rotates creds, or changes auth settings. Use cloud audit logs.

Log Sources

Mutable Elements

Field	Description
CloudReadOnlyApps	Approved security tooling principals that routinely read policy.
ApiClientIPAllowList	Corporate egress IPs for administrative API access.

AN0459

Chain: (1) IdP policy/read operations by a principal (e.g., Microsoft Entra/Graph requests to read password or authentication policies); (2) adjacent risky changes (role assignment, app consent) by same principal. Use IdP audit logs.

Log Sources

Data Component	Name	Channel
User Account Metadata (DC0013)	azure:audit	operation contains 'Get*Password*Policy' OR 'List*Authentication*Policy' OR 'Get-ADDefaultDomainPasswordPolicy'

Mutable Elements

Field	Description
TrustedPartnerAppIds	Legitimate partner apps that enumerate policies.
GeoRiskTolerance	Raise risk for unusual geo or TOR/VPN egress.

AN0460

Chain: (1) SaaS admin API or PowerShell remote session reads tenant password/authentication settings (e.g., M365 Unified Audit Log ‘Cmdlet’ with `Get-MsolPasswordPolicy` / `Get-OrganizationConfig` parameters that expose password settings); (2) same session proceeds to mailbox or tenant changes.

Log Sources

Data Component	Name	Channel
User Account Metadata (DC0013)	m365:unified	Workload=AzureActiveDirectory OR Exchange AND (Operation=Cmdlet AND Parameters contains 'Password' AND (CmdletName='Get-*' OR CmdletName='Get-OrganizationConfig'))

Mutable Elements

Field	Description
SaaSAdminGroup	Known admin groups or break-glass accounts.
SessionAnomalyThreshold	Rate/volume of read operations per session considered anomalous.

AN0461

Chain: (1) privileged CLI sessions run read-only commands that dump AAA/password policies (e.g., `show aaa`, `show password-policy`); (2) same account changes AAA or user DB shortly after. Use network device AAA/command accounting or syslog.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	networkdevice:syslog	cmd='show aaa*' OR 'show running-config | include password|aaa' OR 'show aaa common-criteria policy all'

Mutable Elements

Field	Description
ApprovedNOCSources	Jump hosts permitted to run show commands.
DeviceTier	Higher risk weight on edge/critical devices.
