Detect MFA Modification or Disabling Across Platforms, Detection Strategy DET0190

Archived: 2026-04-05 13:59:17 UTC

AN0543

Detects registry and Group Policy modifications that disable or weaken MFA, suspicious PowerShell usage modifying MFA-related attributes, and anomalous login sessions succeeding without expected MFA challenge.

Log Sources

Mutable Elements

Field	Description
WatchedAttributes	List of AD attributes or policy fields tied to MFA enforcement that may vary by organization.
TimeWindow	Correlation window between MFA policy changes and anomalous login behavior.

AN0544

Detects conditional access policy changes, exclusion of accounts from MFA enforcement, or registration of new MFA factors by non-admin or anomalous users.

Log Sources

Mutable Elements

Field	Description
PrivilegedRoles	Roles permitted to modify MFA settings in IdP; helps tune detection of unauthorized changes.

AN0545

Detects API calls to cloud secrets/MFA configurations where MFA enforcement policies are disabled or bypassed.

Log Sources

Mutable Elements

Field	Description
MonitoredServices	Specific cloud services or IAM policies relevant to MFA enforcement.

AN0546

Detects PAM module modifications or removal of MFA hooks in /etc/pam.d/ configurations, correlated with successful authentications lacking MFA prompts.

Log Sources

Mutable Elements

Field	Description
MFAHooks	Paths to organization-specific PAM modules enforcing MFA.

AN0547

Detects modifications to authorization plugins responsible for MFA enforcement and correlates with suspicious login sessions missing MFA prompts.

Log Sources

Mutable Elements

Field	Description
WatchedPluginPaths	Paths to organization-deployed MFA authorization plugins.

AN0548

Detects suspicious MFA method changes, such as registration of weaker factors (e.g., SMS), or removal of MFA requirements for specific accounts or groups.

Log Sources

Mutable Elements

Field	Description
AcceptedFactors	Configured MFA factors allowed in SaaS environment; tuned to organizational policies.

AN0549

Detects MFA bypass attempts by modifying tenant-wide authentication policies or excluding high-value accounts from MFA enforcement.

Log Sources

Mutable Elements

Field	Description
MonitoredPolicies	Specific tenant or suite policies tied to MFA enforcement.

Source: https://attack.mitre.org/detectionstrategies/DET0190#AN0549