Detect Conditional Access Policy Modification in Identity and Cloud Platforms, Detection Strategy DET0030

Archived: 2026-04-05 18:41:25 UTC

AN0087

Detects modifications to IAM conditions or policies that alter authentication behavior, such as adding permissive trusted IPs, removing MFA requirements, or changing regional access restrictions. Behavioral detection focuses on anomalous policy updates tied to privileged accounts and subsequent suspicious logon activity from previously blocked regions or devices.

Log Sources

Mutable Elements

Field	Description
MonitoredIAMConditions	Specific condition keys (SourceIp, RequestedRegion, MFAAuthenticated) tuned per environment.
TimeWindow	Correlates policy modification with follow-on logins from newly permitted sources.
PrivilegedAccounts	List of administrative accounts to prioritize when monitoring for conditional access changes.

AN0088

Detects suspicious updates to conditional access or MFA enforcement policies in identity providers such as Entra ID, Okta, or JumpCloud. Focus is on removal of policy blocks, addition of broad exclusions, or registration of adversary-controlled MFA methods, followed by anomalous login activity that takes advantage of the modified policies.

Log Sources

Mutable Elements

Field	Description
TargetedApplications	Specific SaaS or cloud apps most sensitive to conditional access changes.
RiskThresholds	Risk scores or signals that may be tuned for anomaly detection in login behavior.

Field	Description
UserContext	Business roles or expected MFA patterns per user/group to reduce false positives.

Source: https://attack.mitre.org/detectionstrategies/DET0030