Detection Strategy for Multi-Factor Authentication Request Generation (T1621), Detection Strategy DET0160

Archived: 2026-04-05 16:16:19 UTC

AN0449

Monitor for excessive or anomalous MFA push notifications or token requests, especially when login attempts originate from unusual IPs or geolocations and do not correspond to legitimate user-initiated sessions.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Threshold of MFA prompts per user within a short time period
GeoIPAllowList	Expected login locations for workforce; deviations can be tuned

AN0450

Detect abnormal MFA activity within cloud service provider logs, such as repeated generation of MFA challenges for the same user session or mismatched MFA device and login origin.

Log Sources

Mutable Elements

Field	Description
FailedLoginThreshold	Number of failed logins before raising detection

AN0451

Detect repeated failed login events followed by MFA challenges triggered in rapid succession, especially if originating from service accounts or anomalous IP addresses.

Log Sources

Mutable Elements

Field	Description
ServiceAccountExclusion	Exclude specific accounts where automated MFA requests are legitimate

AN0452

Monitor PAM and syslog entries for unusual frequency of login attempts that trigger MFA prompts, particularly when MFA challenges do not match expected user behavior.

Log Sources

Mutable Elements

Field	Description
AuthRetryThreshold	Number of retries per user allowed before detection is triggered

AN0453

Detect anomalous OAuth or SSO logins that repeatedly generate MFA challenges, particularly where MFA approvals are denied or timed out by the user.

Log Sources

Mutable Elements

Field	Description
MFAProvider	Identify which MFA service provider logs are in use (Okta, Duo, Microsoft Authenticator)

AN0454

Detect user account logon attempts that trigger multiple MFA challenges through enterprise identity integrations, especially if MFA push requests are generated without successful interactive login.

Log Sources

Mutable Elements

Field	Description
DeviceEnrollmentStatus	Exclude unmanaged macOS devices that use different MFA providers

---

Source: https://attack.mitre.org/detectionstrategies/DET0160#AN0452