Detecting Unauthorized Collection from Messaging Applications in SaaS and Office Environments, Detection Strategy DET0567

Archived: 2026-04-05 16:11:27 UTC

AN1565

Atypical access to Slack or Teams conversations via APIs, automation tokens, or bulk message export functionality, particularly after an account takeover or rare sign-in pattern. Often includes mass retrieval of chat history, download of message content, or scraping of workspace/channel metadata.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time interval to observe post-login message scraping behavior
MessageExportThreshold	Number of messages or files accessed/downloaded to flag for review
UserContext	User privilege level, team membership, or role context to suppress false positives
AccessMethod	Direct user access vs API token, OAuth app, or bot interaction

AN1566

Suspicious access to Microsoft Teams chat messages via eDiscovery, Graph API, or export methods after rare or compromised sign-in. Often associated with excessive file access, sensitive content review, or anomaly from expected user behavior.

Log Sources

Mutable Elements

Field	Description
UserRole	Whether user is part of InfoSec, Legal, or expected to use Teams eDiscovery tools
GeoRiskScore	Unusual country/IP sign-in patterns prior to Teams data export
AccessVolume	Message or file threshold for triggering alert

Source: https://attack.mitre.org/detectionstrategies/DET0567#AN1565