Detect Unsecured Credentials Shared in Chat Messages, Detection Strategy DET0111

Archived: 2026-04-02 11:19:58 UTC

AN0309

Detection correlates message events in email and collaboration tools (e.g., Outlook, Teams) that contain regex-like patterns resembling credentials, API keys, or tokens. Anomalous forwarding or bulk copy activity of chat/email content containing secrets is flagged. Suspicious behavior includes users pasting secrets into direct messages or attaching config files with passwords.

Log Sources

Mutable Elements

Field	Description
RegexPatterns	Customizable credential-detection regex (e.g., API_KEY=, bearer token formats) depending on enterprise apps in use
AllowedDomains	Exclude known trusted domains or automated system-to-system messages
TimeWindow	Adjust correlation period for bulk credential sharing events

AN0310

Detection monitors SaaS collaboration tools (e.g., Slack, Zoom, Jira) for messages or files containing credential-like patterns, or for suspicious API calls retrieving bulk chat histories by non-admin users. Identifies adversary behavior chains where chat logs are queried via APIs or integration bots to systematically extract sensitive material.

Log Sources

Mutable Elements

Field	Description
IntegrationScope	Tune to ignore known enterprise bots with message-read access (e.g., DLP scanners)
RegexPatterns	Customizable regex for detecting secret formats (JWT, OAuth tokens, SSH keys)
UserContext	Correlate with user role to filter developers vs standard users

Source: https://attack.mitre.org/detectionstrategies/DET0111#AN0309