Slack Integrations

Introduction

Slack is used by numerous organizations as their primary chat and collaboration tool.

Please note the Audit Logs API is only available to Slack workspaces on an Enterprise Grid plan. These API methods will not work for workspaces on a Free, Standard, or Business+ plan.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Requirements

Configuration

Enabling the integration in Elastic

1. In Kibana go to **Management > Integrations**
2. In the "Search for integrations" search bar type **Slack.**
3. Click on "Slack" integration from the search results.
4. Click on **Add Slack** button to add Slack integration.

Configure Slack audit logs data stream

Enter values "OAuth API Token".

1. OAuth API Token will be generated when a Slack App is created.

CONFIGURE USING API TOKEN

For the Slack integration to be able to successfully get logs the following "User Token Scopes"" must be granted to the Slack App:

- **auditlogs:read**

Logs

Audit

Audit logs summarize the history of changes made within the Slack Enterprise.

SLACK Integration?Procedures

Please provide the following information to CyTech:

Collect Slack logs via API

1. API URL - The root URL for the API endpoints.

Slack Audit logs

1. OAuth API Token - The OAuth API Token used to authenticate with the Slack API

Revision #3
Created 23 April 2024 14:18:26
Updated 19 June 2024 06:54:01