Enable and Configure Automatic Remediation for SaaS API DLP in Slack and ServiceNow

Contents

Introduction

This document describes how to enable and configure automatic remediation for SaaS API DLP in Slack and ServiceNow tenants.

Overview

You can now discover and automatically remediate sensitive data exposure in your Slack and ServiceNow tenants. This helps you maintain compliance and prevent the exposure of sensitive data, such as intellectual property or credentials for other systems.

Authorize New Tenants for Supported Platforms

As an administrator, you can authenticate new tenants for Slack and ServiceNow using the SaaS API Data Loss Prevention (DLP) feature in the Umbrella dashboard.

1. Go to**ADMIN > AUTHENTICATION > PLATFORMS**in the Umbrella dashboard.
2. Authenticate the new tenant as prompted.

Automatic Remediation Supported by SaaS API DLP

- **ServiceNow:**
  SaaS API DLP supports automatic quarantine. The quarantined file is saved in the Cisco Quarantine table. Only the administrator who authenticated the tenant can access this table.

- **Slack:**
  SaaS API DLP supports automatic deletion of files and messages.

Configure Automatic Remediation for Infected Files

As an administrator, you can configure SaaS API DLP to automatically remediate sensitive data exposure.

Set the response action in the SaaS API DLP rule:

1. In the Umbrella dashboard, go to**POLICIES > MANAGEMENT > DATA LOSS PREVENTION POLICY**.
2. Click**ADD RULE**.
3. Select**SAAS API RULE**.
4. Set the desired**ACTION**in the Response Action section to enable automatic remediation.

Find More Information

Refer to the Umbrella documentation for detailed guidance.

- Enable SaaS API Data Loss Protection for Slack Tenants
- Enable SaaS API Data Loss Protection for ServiceNow Tenants