在Slack和ServiceNow中为SaaS API DLP启用和配置自动补救

目录

简介

本文档介绍如何为Slack和ServiceNow租户中的SaaS API DLP启用和配置自动补救。

概述

现在，您可以在Slack和ServiceNow租户中发现并自动修复敏感数据泄露。这有助于保持合规性并防止敏感数据（例如知识产权或其他系统的凭证）泄露。

为支持的平台授权新租户

作为管理员，您可以使用Umbrella控制面板中的SaaS API防数据丢失(DLP)功能对Slack和ServiceNow的新租户进行身份验证。

1. 在Umbrella控制面板中转到ADMIN > AUTHENTICATION > PLATFORMS。
2. 根据提示对新租户进行身份验证。

SaaS API DLP支持的自动补救

- ServiceNow:
  SaaS API DLP支持自动隔离。隔离的文件保存在思科隔离区表中。只有对租户进行身份验证的管理员可以访问此表。

- Slack:
  SaaS API DLP支持自动删除文件和消息。

配置受感染文件的自动补救

作为管理员，您可以配置SaaS API DLP以自动修复敏感数据泄露。

在SaaS API DLP规则中设置响应操作：

1. 在Umbrella控制面板中，转至POLICIES > MANAGEMENT > DATA LOSS PREVENTION POLICY。
2. 点击ADD RULE。
3. 选择SAAS API规则。

4. 在Response Action部分中设置desiredACTION以启用自动补救。

查找更多信息

请参阅Umbrella文档以获取详细指导。

- 为Slack租户启用SaaS API数据丢失保护
- 为ServiceNow租户启用SaaS API数据丢失保护

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。