为Slack和ServiceNow中的云恶意软件配置自动补救

目录

简介

本文档介绍如何为Slack和ServiceNow租户中的云恶意软件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恶意软件风险。这些功能通过删除或隔离感染病毒的文件帮助保护租户的安全。

为支持的平台授权新租户

作为管理员，您可以通过Umbrella控制面板对云恶意软件防护的新Slack或ServiceNow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。

云恶意软件支持的自动修复

- ServiceNow:
  云恶意软件支持自动隔离。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才能访问。

- Slack:
  云恶意软件支持自动删除受感染的文件。

配置受感染文件的自动补救

作为管理员，您可以配置云恶意软件以自动修复受感染的文件：

1. 在Umbrella控制面板中，转至ADMIN > AUTHENTICATION > PLATFORMS。
2. 使用租户的身份验证向导。在步骤3中设置响应操作。
3. 选择您的首选响应操作（隔离或监控）。
4. 您可以根据需求变化随时更新响应操作。

相关资源

- 为松弛的租户启用云恶意软件防护
- 为ServiceNow租户启用云恶意软件防护

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）。