Configure Automatic Remediation for Cloud Malware in Slack and ServiceNow

Contents

Introduction

This document describes how to enable and configure automatic remediation for Cloud Malware in Slack and ServiceNow tenants.

Overview

You can now discover and automatically remediate malware risks in your Slack and ServiceNow tenants. These features help keep your tenants secure by removing or quarantining infected files.

Authorize New Tenants for Supported Platforms

As an administrator, you can authenticate new Slack or ServiceNow tenants for Cloud Malware protection through the Umbrella dashboard.

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

Automatic Remediation Supported by Cloud Malware

- **ServiceNow:**
  Cloud Malware supports automatic quarantine. Quarantined files are saved in the Cisco Quarantine table, accessible only to the admin who authenticated the tenant.

- **Slack:**
  Cloud Malware supports automatic deletion of infected files.

Configure Automatic Remediation for Infected Files

As an administrator, you can configure Cloud Malware to remediate infected files automatically:

1. In the Umbrella dashboard, go to**ADMIN > AUTHENTICATION > PLATFORMS**.
2. Use the authentication wizard for your tenant. Set the response action during step 3.
3. Choose your preferred response action (quarantine or monitoring).
4. You can update the response action at any time as your needs change.

Related Resources

- Enable Cloud Malware Protection for Slack Tenants
- Enable Cloud Malware Protection for ServiceNow Tenants