Webhook通知

Data Infrastructure Insights

NetApp
February 03, 2026

目次

Webhook通知

Webhookを使用したワークロードセキュリティ通知

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用して、さまざまなアプリケーションに重大なアラート通知や警告アラート通知を送信できます。

多くの商用アプリケーションは、Slack、PagerDuty、Teams、Discord など、標準の入力インターフェースとして Webhook をサポートしています。汎用的でカスタマイズ可能な Webhook チャネルをサポートすることで、Workload Security はこれらの配信チャネルの多くをサポートできます。 Webhook の設定に関する情報は、それぞれのアプリケーションの Web サイトで確認できます。例えば、Slackは"この便利なガイド"。

複数の Webhook チャネルを作成し、各チャネルを異なる目的、個別のアプリケーション、異なる受信者などを対象にすることができます。

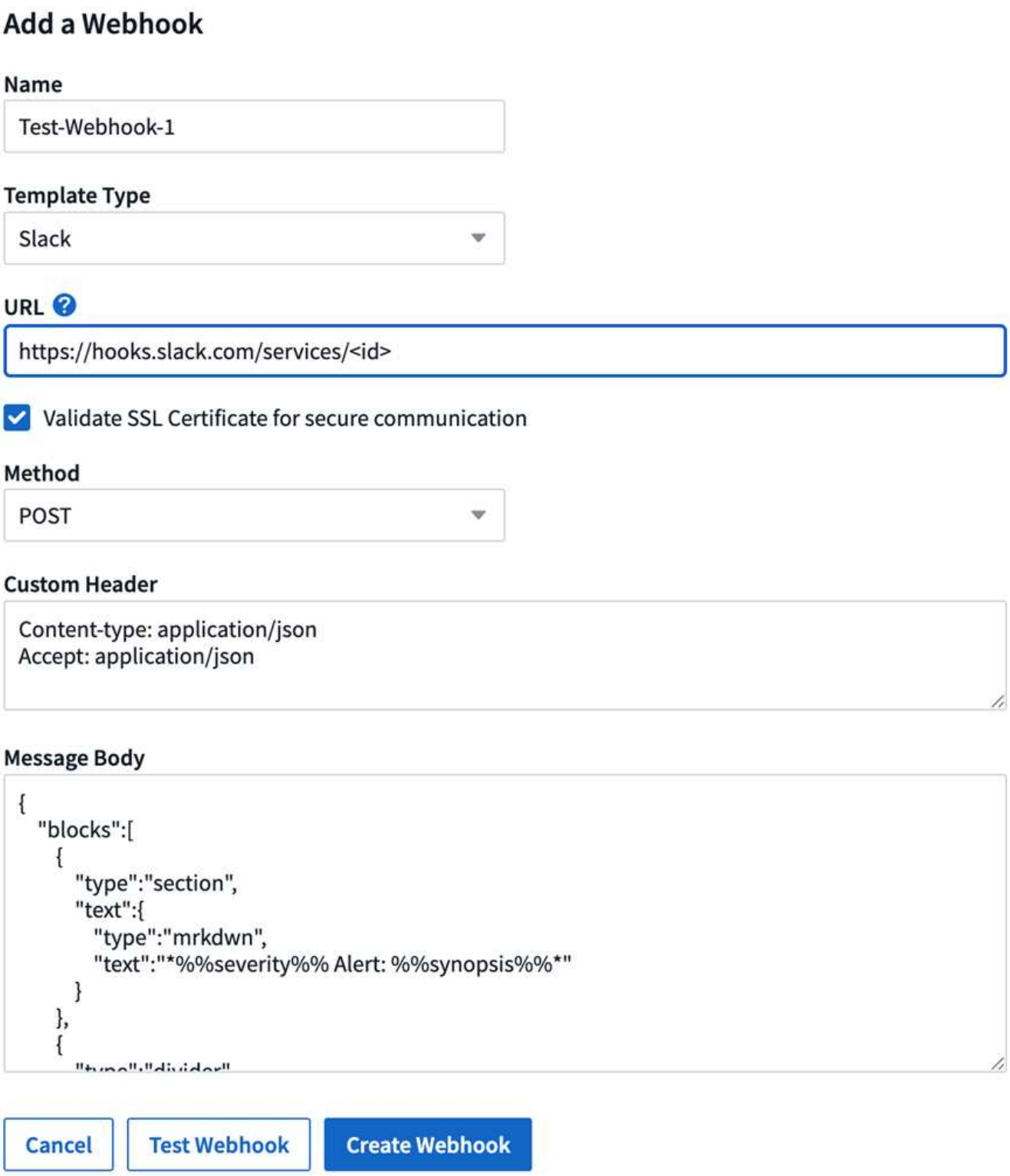
Webhookチャネルインスタンスは次の要素で構成されています

Name	説明
URL	Webhook ターゲット URL（URL パラメータとともに http:// または https:// プレフィックスを含む）
方法	GET/POST - デフォルトはPOST
カスタムヘッダー	ここでカスタムヘッダーを指定します
メッセージ本文	メッセージの本文をここに入力してください
デフォルトのアラートパラメータ	Webhookのデフォルトパラメータを一覧表示します
カスタムパラメータとシークレット	カスタムパラメータとシークレットを使用すると、固有のパラメータやパスワードなどの安全な要素を追加できます。

Webhookの作成

Workload Security Webhook を作成するには、「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。次の画像は、Slack Webhook 作成画面のサンプルを示しています。

注意: Workload Security Webhook を作成および管理するには、ユーザーは Workload Security *Admin* である必要があります。



- 各フィールドに適切な情報を入力し、「保存」をクリックします。
- 「Webhook のテスト」ボタンをクリックして接続をテストすることもできます。これにより、選択したメソッドに従って、定義された URL に「メッセージ本文」（置換なし）が送信されることに注意してください。
- SWS Webhook は、いくつかのデフォルト パラメータで構成されています。さらに、独自のカスタム パラメータまたはシークレットを作成することもできます。

パラメーター: パラメーターとは何か、どのように使用するのか?

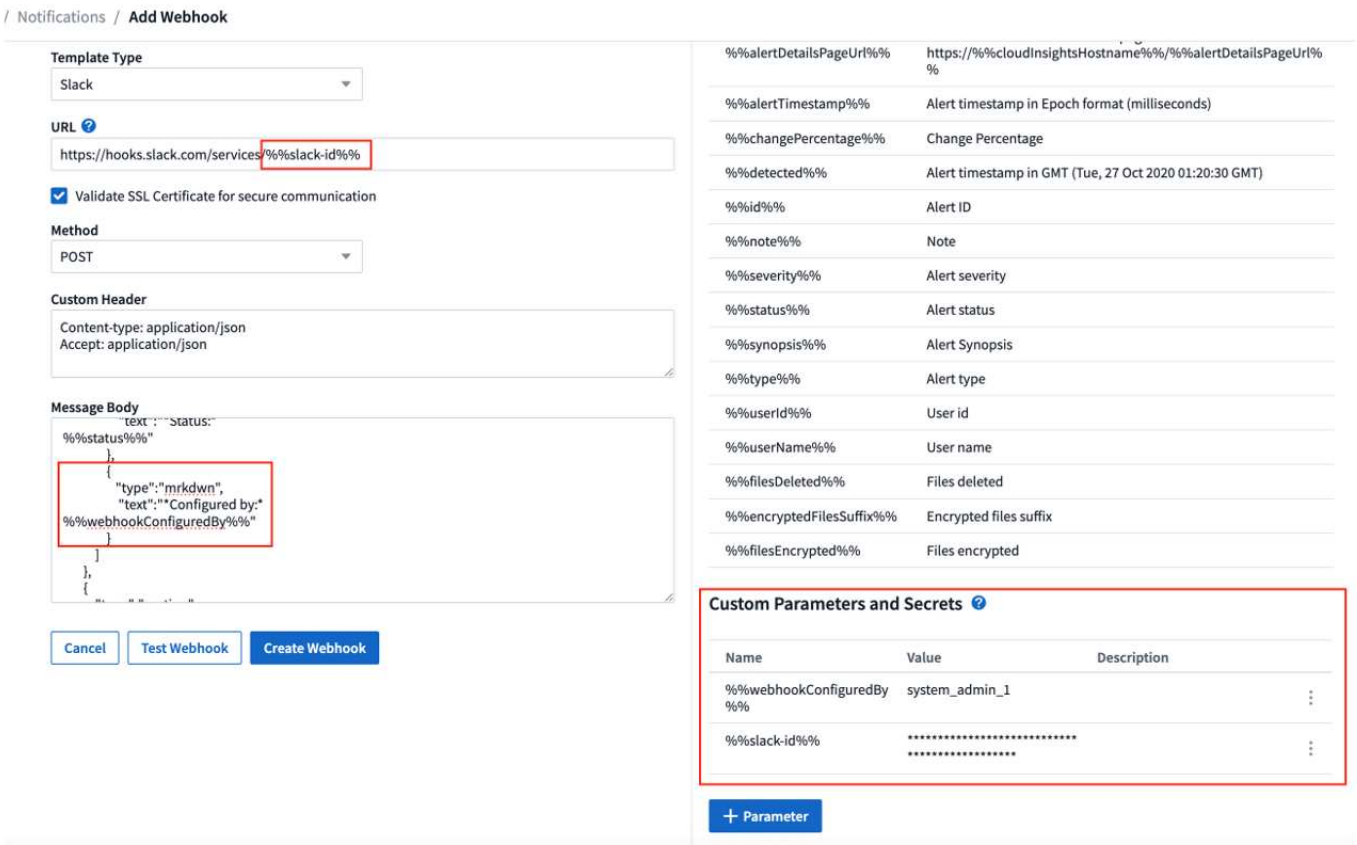
アラート パラメータは、アラートごとに設定される動的な値です。たとえば、*%%severity%%* パラメータは、アラートの重大度タイプに置き換えられます。

「Test Webhook」ボタンをクリックしたときには置換は実行されないことに注意してください。テストでは、パラメータのプレースホルダー (*%%<param-name>%%*) を表示するペイロードが送信されますが、データに置き換えられることはありません。

カスタムパラメータとシークレット

このセクションでは、必要なカスタム パラメータやシークレットを追加できます。カスタム パラメータまたはシークレットは、URL またはメッセージ本文に含めることができます。シークレットを使用すると、ユーザーはパスワード、apiKey などの安全なカスタム パラメータを設定できます。

次のサンプル画像は、Webhook の作成時にカスタム パラメータがどのように使用されるかを示しています。



ワークロード セキュリティ **Webhook** リスト ページ

Webhook リスト ページには、名前、作成者、作成日、ステータス、セキュリティ、最終報告のフィールドが表示されます。注: 「ステータス」列の値は、最後の Webhook トリガーの結果に基づいて変化し続けます。以下はステータス結果の例です。

ステータス	説明
OK	通知を正常に送信しました。
403	禁止されています。

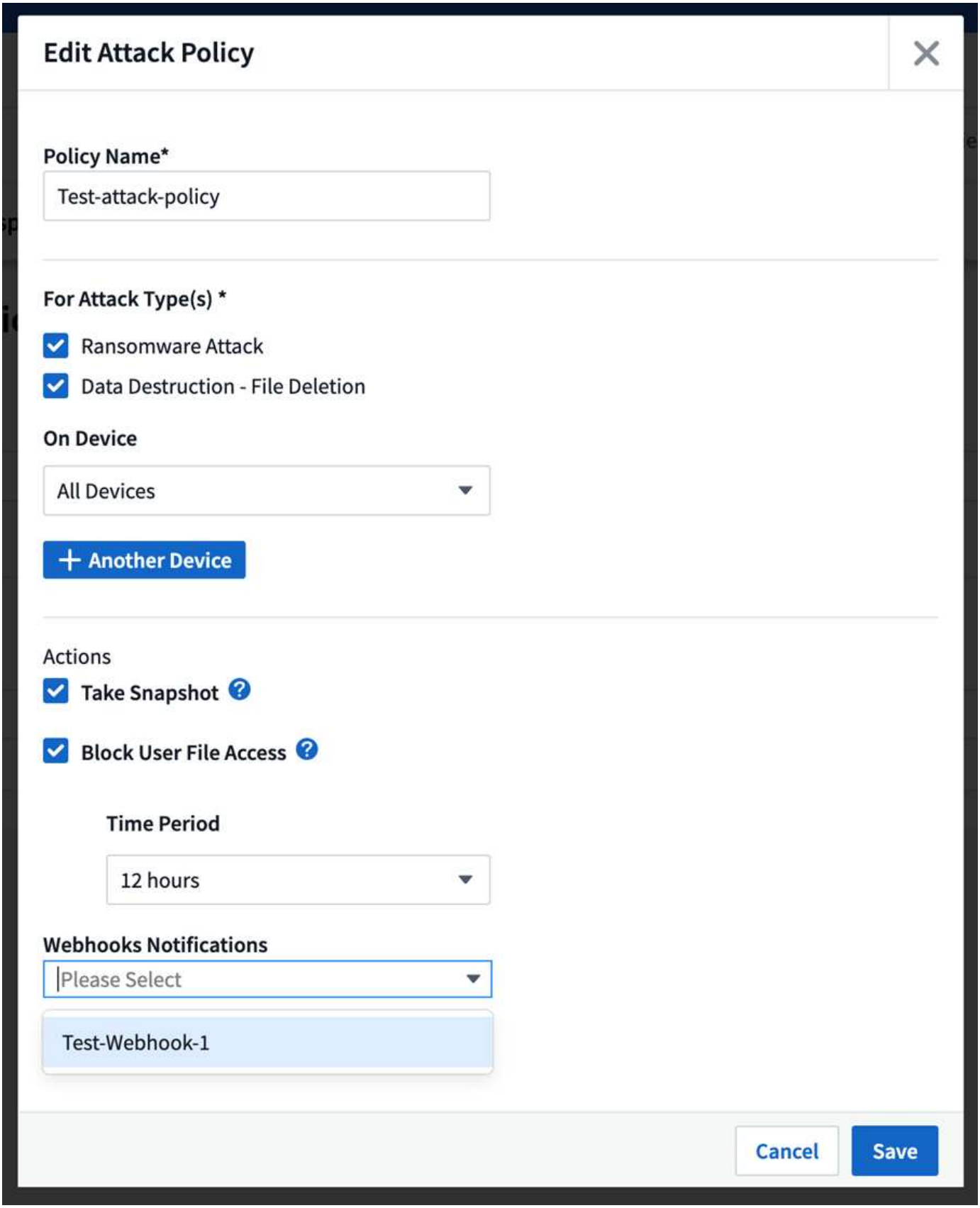
404	URLが見つかりません。
400	要求の形式が正しくありません。メッセージ本文にエラーがある場合、このステータスが表示されることがあります。例: • 形式が不適切な json。 • 予約済みのキーに無効な値を指定しています。たとえば、PagerDuty は「重大度」として、critical/warning/error/info のみを受け入れます。その他の結果の場合は、400 ステータスが返される可能性があります。 • アプリケーション固有の検証エラー。たとえば、Slack ではセクション内に最大 10 個のフィールドが許可されます。 10 個を超えると、400 ステータスになる可能性があります。
410	リソースは利用できなくなりました

「最終報告」列には、Webhook が最後にトリガーされた時刻が示されます。

ウェブフック一覧ページから、ユーザーはウェブフックを編集/複製/削除することもできます。

アラートポリシーで**Webhook**通知を構成する

アラート ポリシーに Webhook 通知を追加するには、「ワークロード セキュリティ」>「ポリシー」に移動し、既存のポリシーを選択するか、新しいポリシーを追加します。 アクション セクション > *Webhook* 通知ドロップダウンで、必要な Webhook を選択します。



Webhook 通知はポリシーに関連付けられています。攻撃 (RW/DD/WARN) が発生すると、設定されたアクション (スナップショットの取得/ユーザーのブロック) が実行され、関連する Webhook 通知がトリガーされます。

注: 電子メール通知はポリシーとは無関係であり、通常どおりトリガーされます。

- ポリシーが一時停止されている場合、Webhook 通知はトリガーされません。
- 複数の Webhook を 1 つのポリシーにアタッチできますが、ポリシーにアタッチする Webhook は 5 つ以下にすることをお勧めします。

ワークロードセキュリティ**Webhook**の例

Webhooksの"スラック"

Webhooksの"ページャーデューティ"Webhooksの"チーム"Webhooksの"不和"

Discord 向けワークロード セキュリティ Webhook の例

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、Discord 用の Webhook を設定する例を示します。

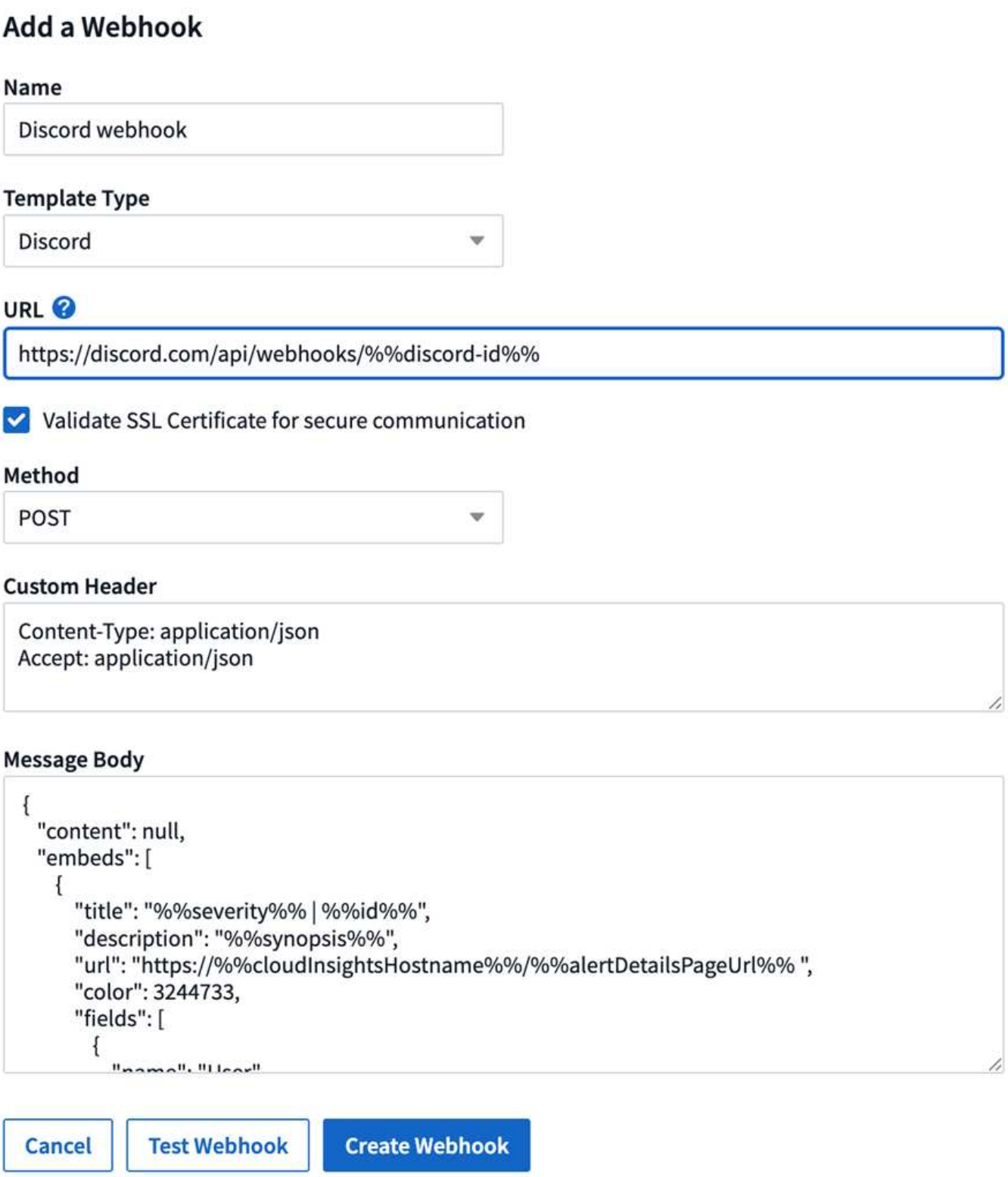
このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Discordドキュメント"最新情報についてはこちらをご覧ください。

Discordの設定:

- Discordでサーバーを選択し、テキストチャンネルの下にあるチャンネル編集（歯車アイコン）を選択します。
- *統合 > Webhookの表示*を選択し、*新しいWebhook*をクリックします。
- Webhook URL をコピーします。これを Workload Security Webhook 設定に貼り付ける必要があります。

ワークロード セキュリティ **Webhook** を作成します。

1. 「管理」>「通知」に移動し、「*Workload Security Webhooks*」タブを選択します。新しい Webhook を作成するには、「+ Webhook」をクリックします。
2. Webhook に意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、**Discord** を選択します。
4. 上記の Discord URL を *URL* フィールドに貼り付けます。



Webhook をテストするには、メッセージ本文の URL 値を有効な URL (*https://netapp.com* など) に一時的に置き換えて、[*Test Webhook*] ボタンをクリックします。 Discord では、テスト Webhook 機能が動作するために有効な URL を指定する必要があります。

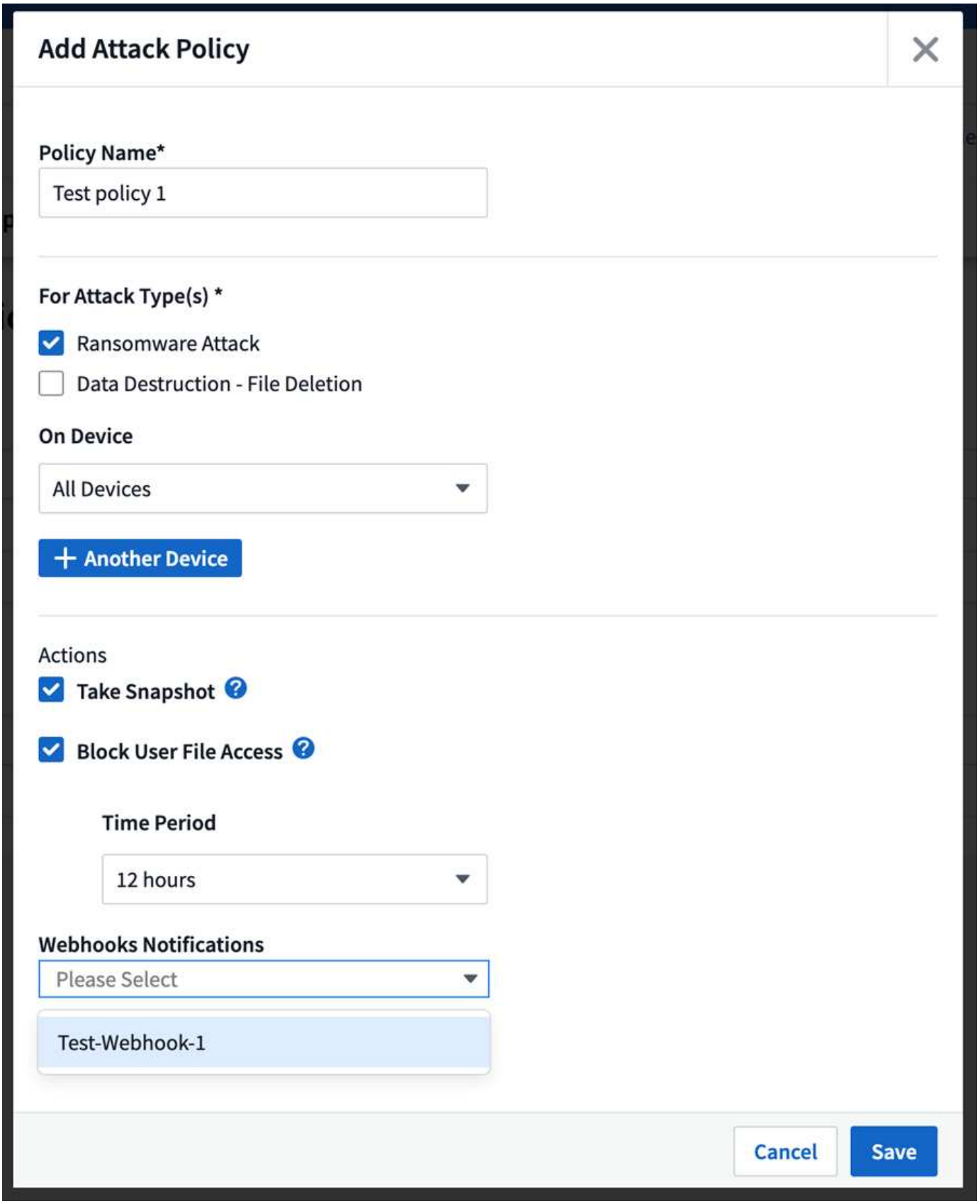
テストが完了したら、必ずメッセージ本文を元に戻してください。

Webhook経由の通知

Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_ または+警告ポリシー_をクリックします。

- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [*Webhooks Notifications*] ドロップダウンで、必要な Discord Webhook を選択して保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。



PagerDuty のワークロード セキュリティ Webhook の例

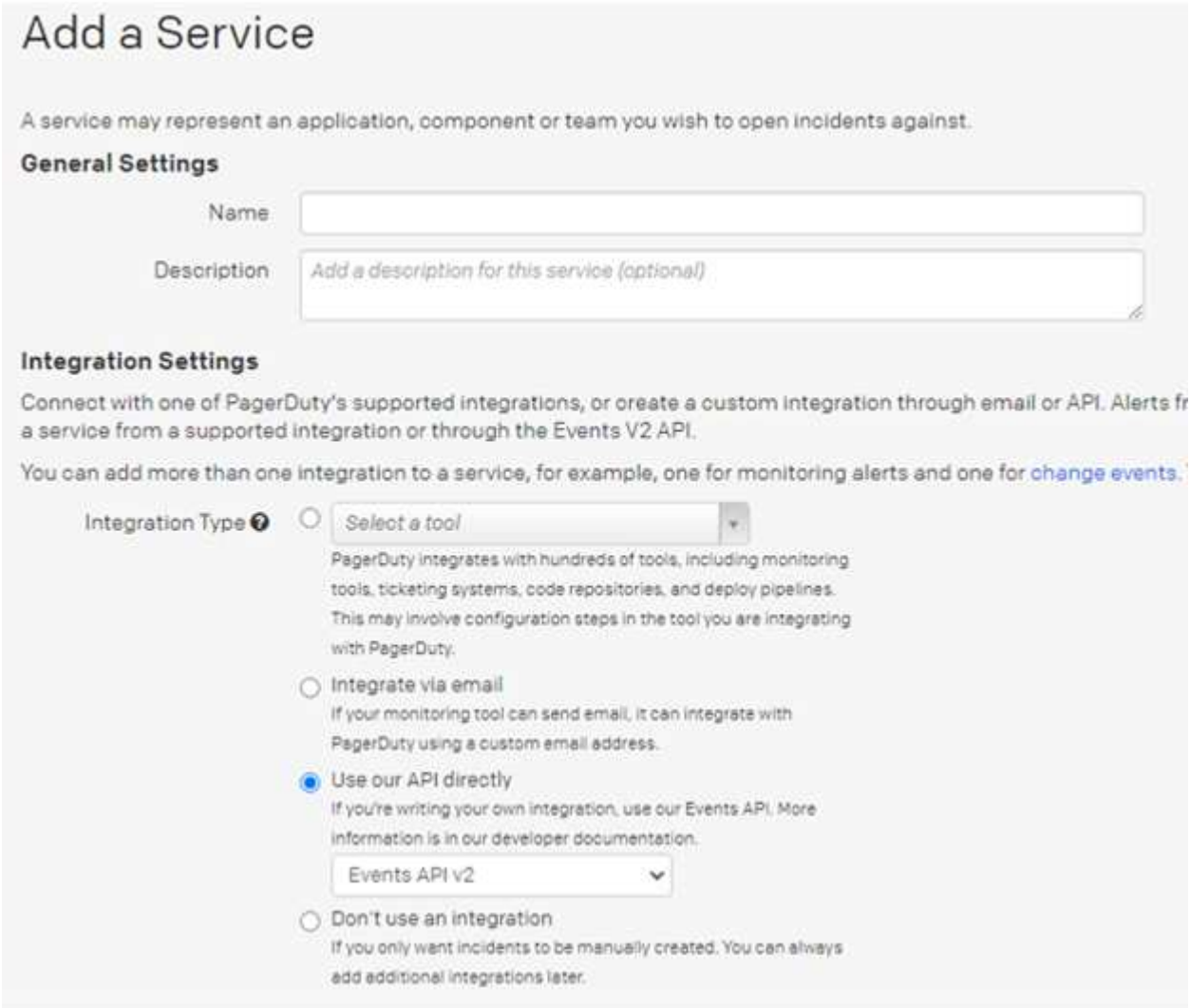
Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用して

さまざまなアプリケーションにアラート通知を送信できます。このページでは、PagerDuty の Webhook を設定する例を示します。

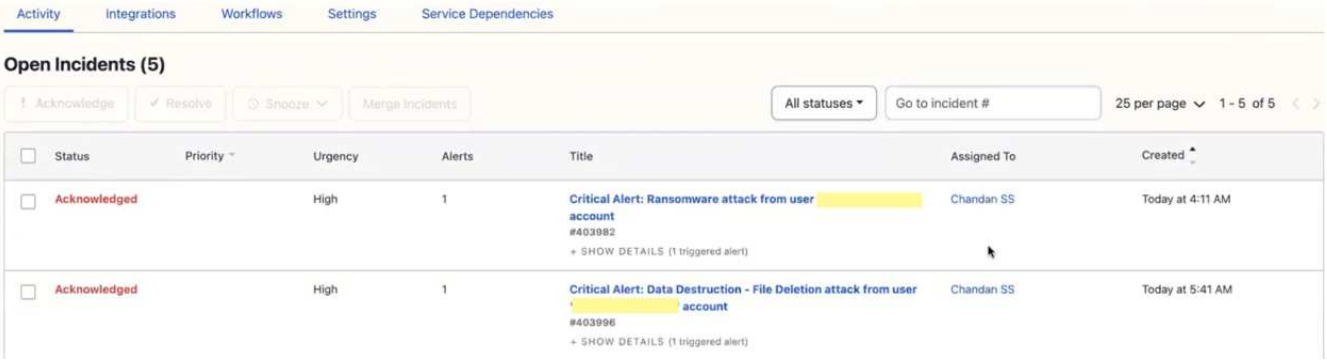
このページはサードパーティの指示を参照しており、変更される可能性があります。参照"PagerDutyのドキュメント"最新情報についてはこちらをご覧ください。

PagerDutyのセットアップ:

1. PagerDuty で、サービス > サービス ディレクトリ に移動し、+ 新しいサービス ボタンをクリックします。
2. _名前_を入力し、_API を直接使用_を選択します。 _サービスの追加_を選択します。

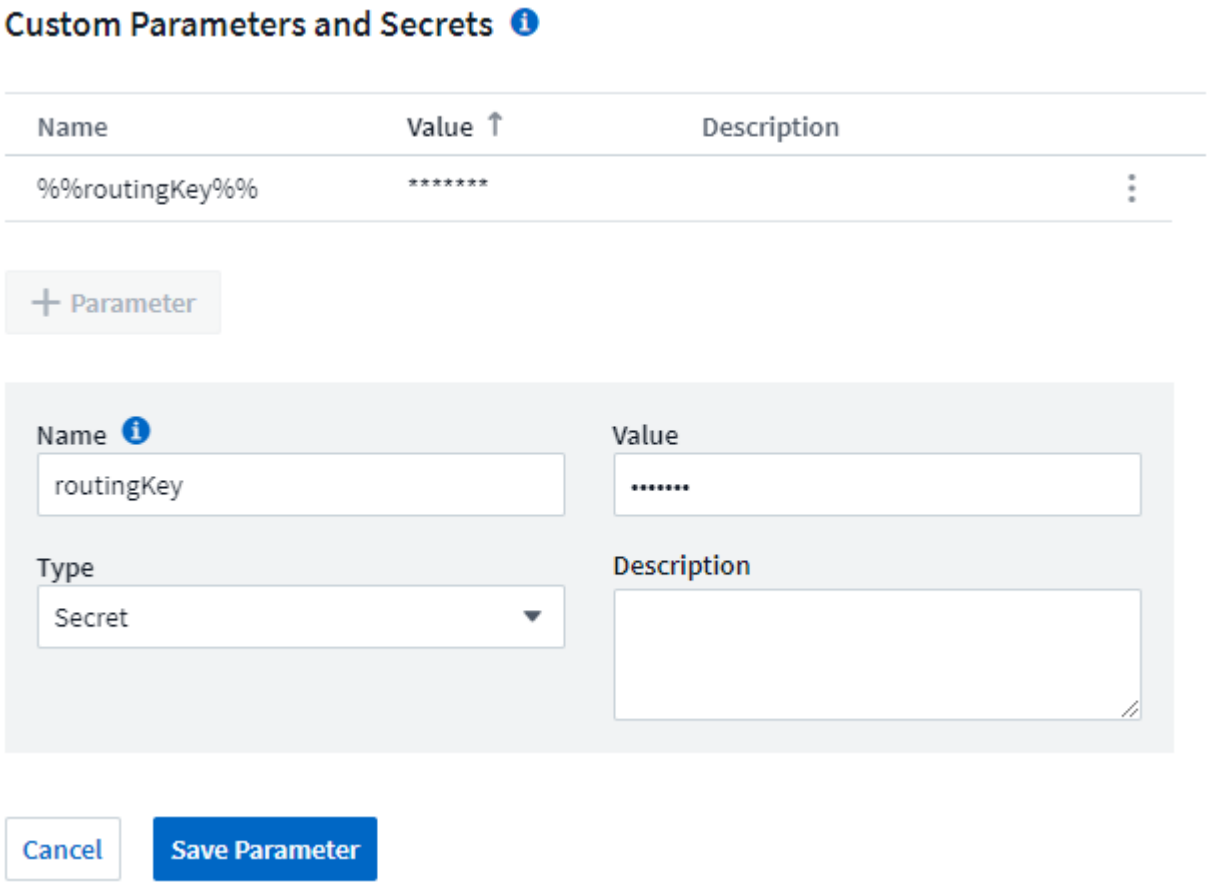


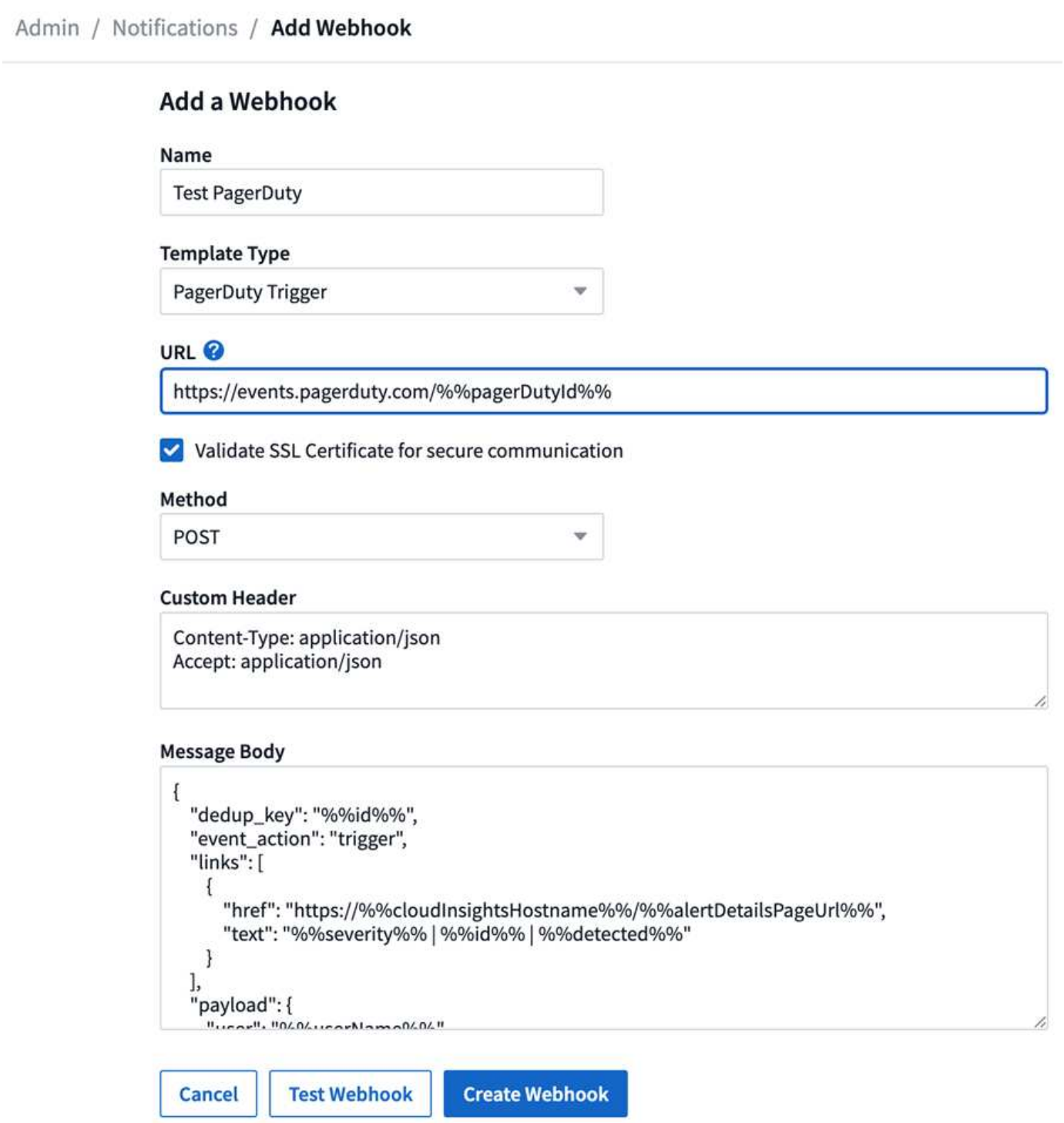
3. *統合キー*を表示するには、[統合] タブを選択します。以下の Workload Security Webhook を作成するときに、このキーが必要になります。
4. アラートを表示するには、「インシデント」または「サービス」に移動します。



Workload Security PagerDuty Webhook を作成します。

- 「管理」>「通知」に移動し、「*Workload Security Webhooks*」タブを選択します。新しい Webhook を作成するには、「+ Webhook」を選択します。
- Webhook に意味のある名前を付けます。
- テンプレート タイプ ドロップダウンで、*PagerDuty* トリガー を選択します。
- *routingKey* という名前のカスタム パラメータ シークレットを作成し、その値を上記で作成した PagerDuty *Integration Key* に設定します。

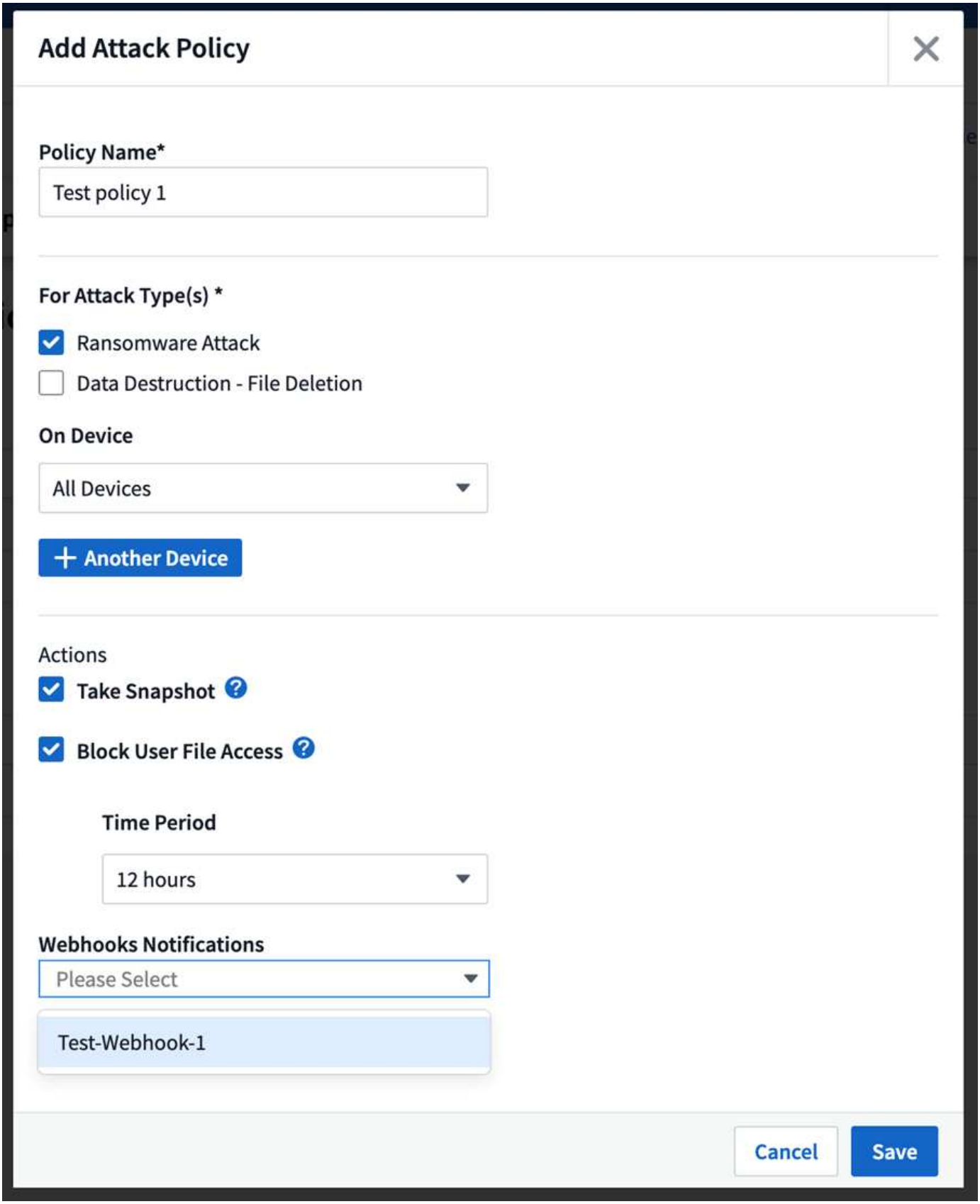




Webhook経由の通知

- Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_または+警告ポリシー_を選択します。
- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [*Webhooks Notifications*] ドロップダウンで、必要な PagerDuty Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。



Slack 向けワークロード セキュリティ Webhook の例

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、Slack 用の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。最新情報については、Slack のドキュメントを参照してください。

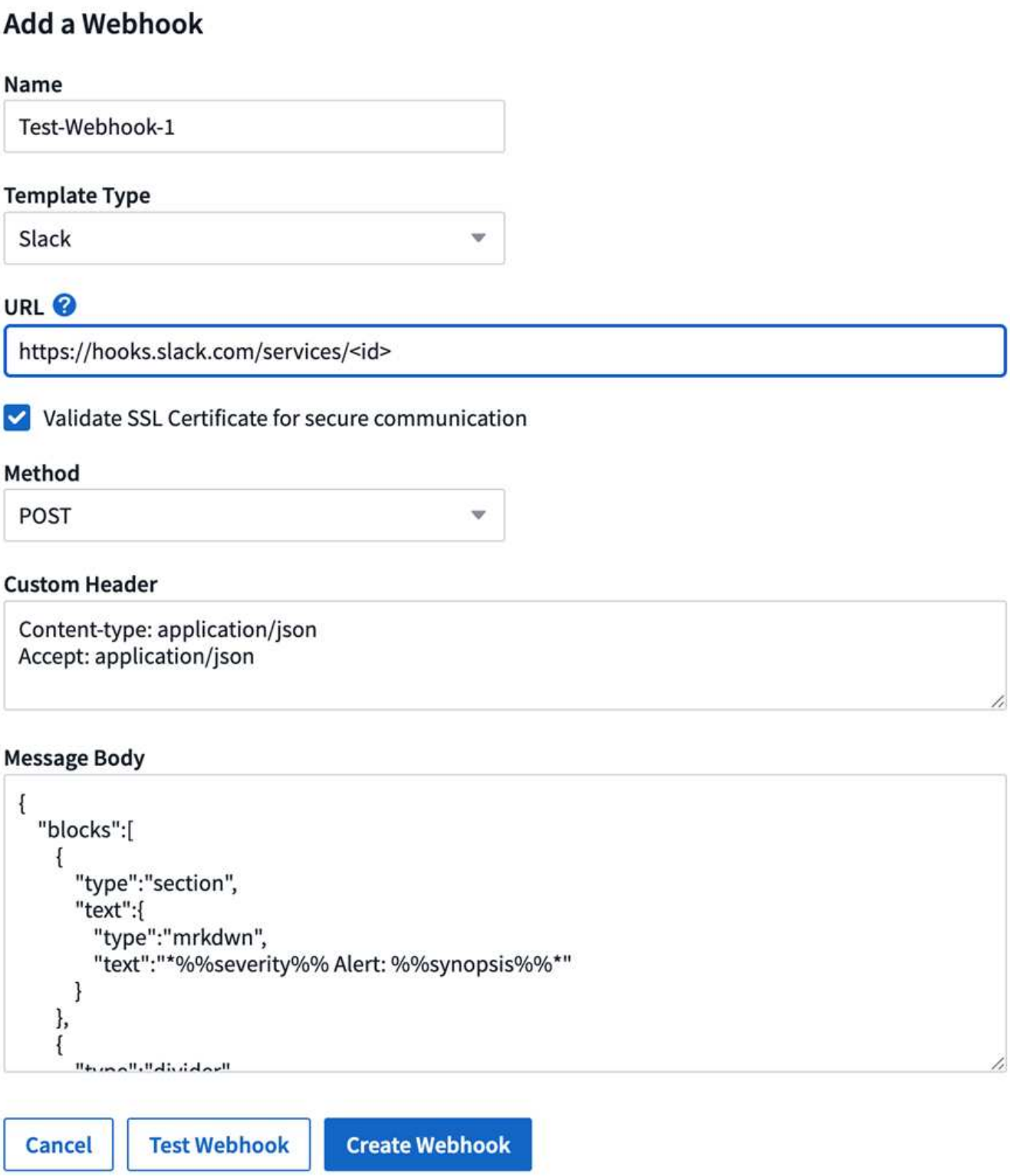
Slackの例

- へ移動 https://api.slack.com/apps新しいアプリを作成します。意味のある名前を付けて、ワークスペースを選択します。

- 「Incoming Webhooks」に移動し、「*Activate Incoming Webhooks*」をクリックし、「*Add New Webhook*」を選択して、投稿するチャネルを選択します。
- Webhook URL をコピーします。この URL は、Workload Security Webhook を作成するときに提供されます。

ワークロードセキュリティ **Slack Webhook** を作成する

1. 「管理」>「通知」に移動し、「*Workload Security Webhooks*」タブを選択します。新しい Webhook を作成するには、[+ *Webhook*] を選択します。
2. Webhook に意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、*Slack* を選択します。
4. 上記からコピーしたURLを貼り付けます。

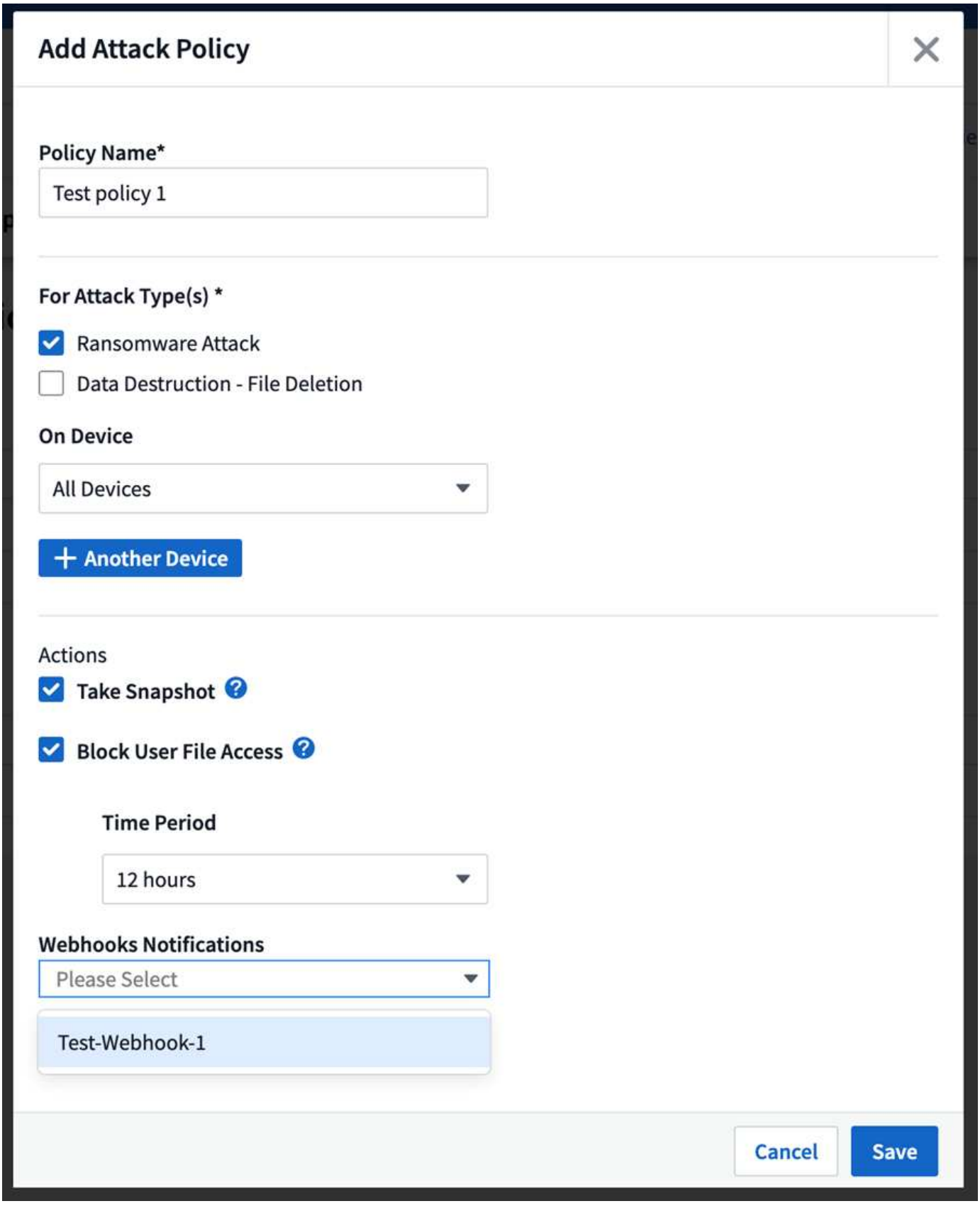


Webhook経由の通知

- Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_または+警告ポリシー_をクリックします。
- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。

- [*Webhooks Notifications*] ドロップダウンで、必要な Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。



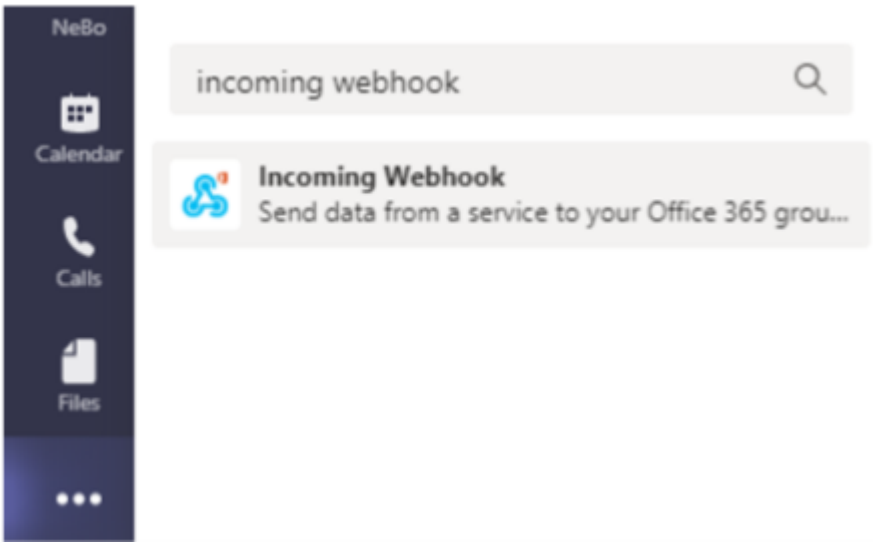
Microsoft Teams のワークロード セキュリティ Webhook の例

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、Teams の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Teamsドキュメント"最新情報についてはこちらをご覧ください。

Teams のセットアップ:

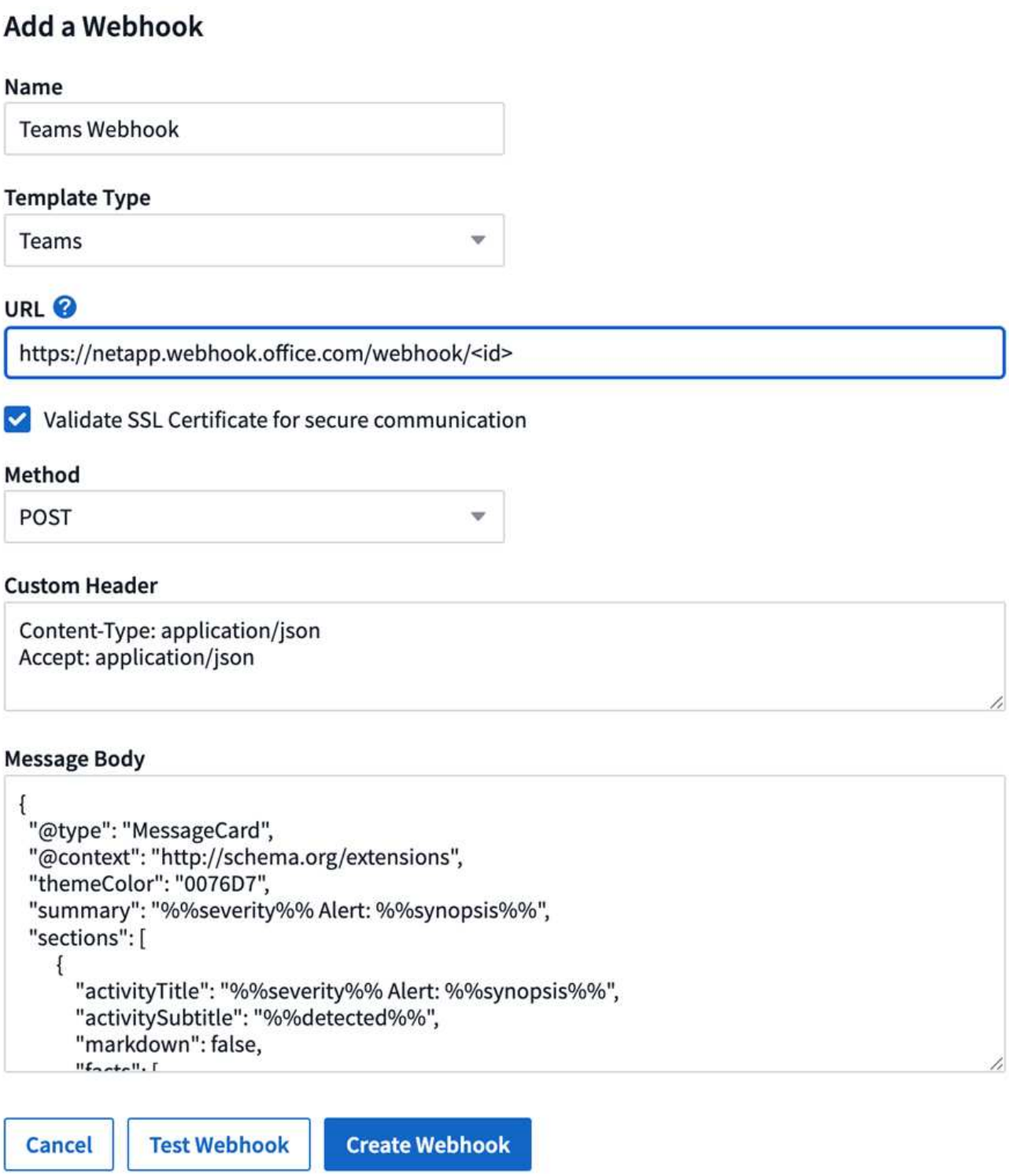
1. Teams でケバブを選択し、Incoming Webhook を検索します。



2. *チームに追加 > チームを選択 > コネクタの設定*を選択します。
3. Webhook URL をコピーします。これを Workload Security Webhook 設定に貼り付ける必要があります。

ワークロード セキュリティ チームの Webhook を作成します。

1. 「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。新しい Webhook を作成するには、[+ *Webhook*] を選択します。
2. Webhook に意味のある名前を付けます。
3. [テンプレート タイプ] ドロップダウンで、[**Teams**] を選択します。



4. 上記の URL を *URL* フィールドに貼り付けます。

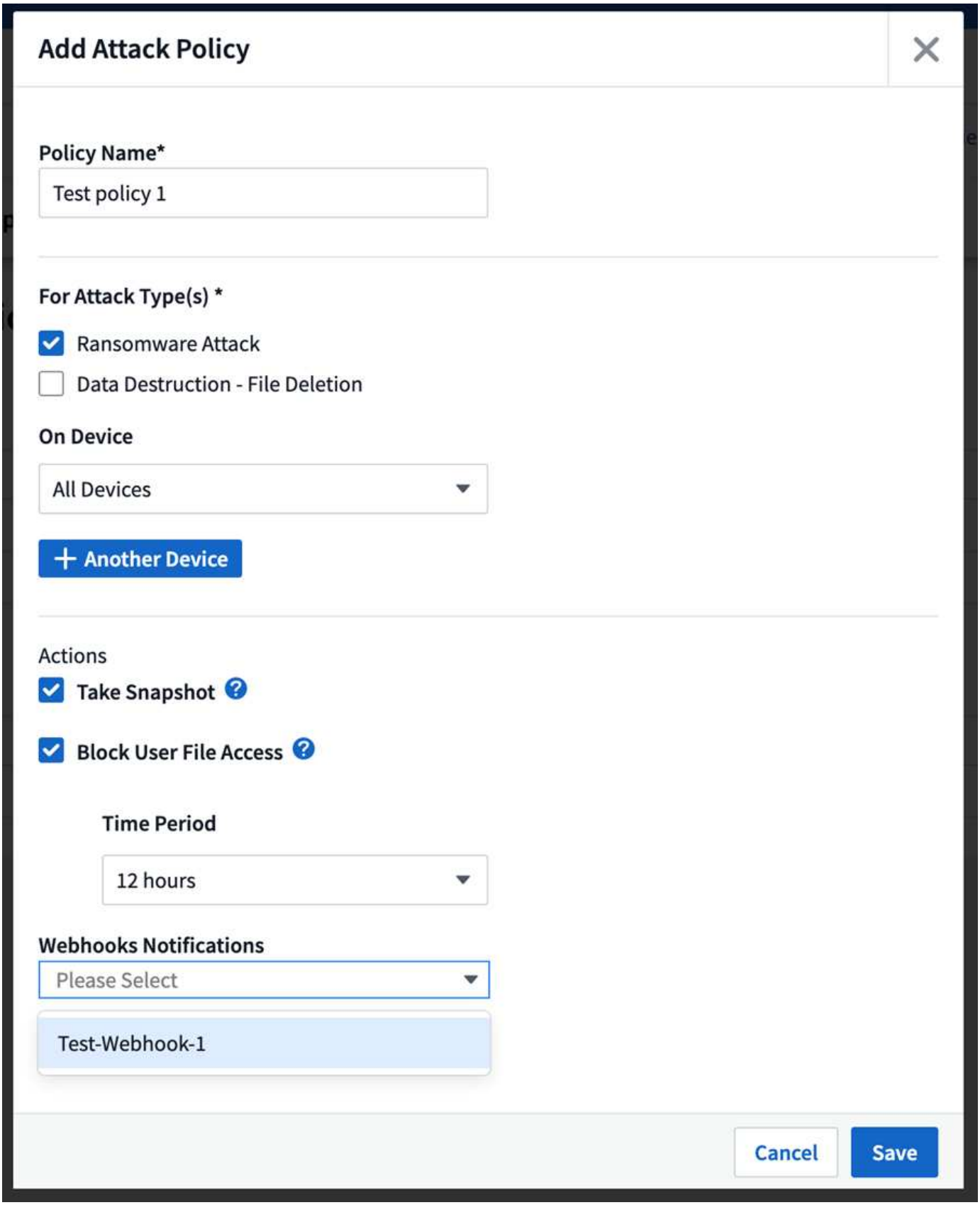
Webhook経由の通知

Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_ または+警告ポリシー_を選択します。

- 意味のあるポリシー名を入力します。

- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [*Webhooks Notifications*] ドロップダウンで、必要な Teams Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。


Add Attack Policy
Policy Name*
Test policy 1
For Attack Type(s) *
Ransomware Attack
Data Destruction - File Deletion
On Device
All Devices
+ Another Device
Actions
Take Snapshot
Block User File Access
Time Period
12 hours
Webhooks Notifications
Please Select
Test-Webhook-1
Cancel
Save

著作権に関する情報

商標に関する情報