Webhook-Benachrichtigungen

Data Infrastructure Insights

NetApp
February 11, 2026

Inhalt

Webhook-Benachrichtigungen

Workload-Sicherheitsbenachrichtigungen mithilfe von Webhooks

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal kritische Warnmeldungen oder Warnmeldungen an verschiedene Anwendungen senden.

Viele kommerzielle Anwendungen unterstützen Webhooks als Standardeingabeschnittstelle, zum Beispiel: Slack, PagerDuty, Teams und Discord. Durch die Unterstützung eines generischen, anpassbaren Webhook-Kanals kann Workload Security viele dieser Bereitstellungskanäle unterstützen. Informationen zur Konfiguration der Webhooks finden Sie auf den Webseiten der jeweiligen Anwendungen. Slack bietet beispielsweise"dieser nützliche Leitfaden" .

Sie können mehrere Webhook-Kanäle erstellen, wobei jeder Kanal einem anderen Zweck, separaten Anwendungen, verschiedenen Empfängern usw. dient.

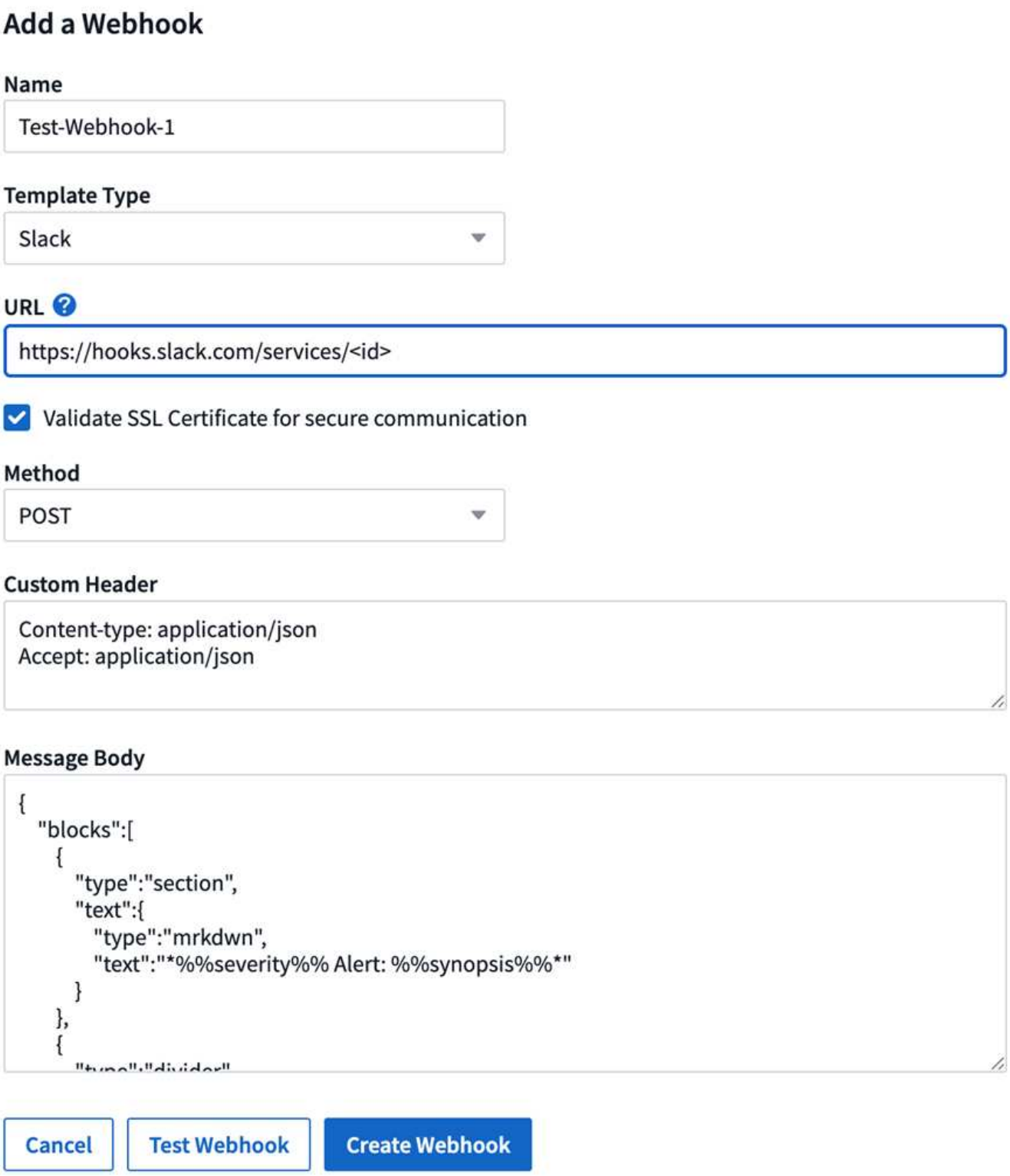
Die Webhook-Kanalinstanz besteht aus den folgenden Elementen

Name	Beschreibung
URL	Webhook-Ziel-URL, einschließlich des Präfixes http:// oder https:// zusammen mit den URL-Parametern
Verfahren	GET/POST – Standard ist POST
Benutzerdefinierter Header	Geben Sie hier alle benutzerdefinierten Header an
Nachrichtentext	Geben Sie hier den Text Ihrer Nachricht ein
Standard-Alarmparameter	Listet die Standardparameter für den Webhook auf
Benutzerdefinierte Parameter und Geheimnisse	Benutzerdefinierte Parameter und Geheimnisse ermöglichen Ihnen das Hinzufügen einzigartiger Parameter und sicherer Elemente wie Passwörter

Erstellen eines Webhooks

Um einen Workload Security Webhook zu erstellen, gehen Sie zu Admin > Benachrichtigungen und wählen Sie die Registerkarte „Workload Security Webhooks“. Das folgende Bild zeigt einen Beispielbildschirm zum Erstellen eines Slack-Webhooks.

Hinweis: Der Benutzer muss ein Workload Security-Administrator sein, um Workload Security-Webhooks erstellen und verwalten zu können.



- Geben Sie in jedes Feld die entsprechenden Informationen ein und klicken Sie auf „Speichern“.
- Sie können auch auf die Schaltfläche „Webhook testen“ klicken, um die Verbindung zu testen. Beachten Sie, dass dadurch der „Nachrichtentext“ (ohne Ersetzungen) gemäß der ausgewählten Methode an die definierte URL gesendet wird.
- SWS-Webhooks umfassen eine Reihe von Standardparametern. Darüber hinaus können Sie Ihre eigenen benutzerdefinierten Parameter oder Geheimnisse erstellen.

Parameter: Was sind sie und wie werden sie verwendet?

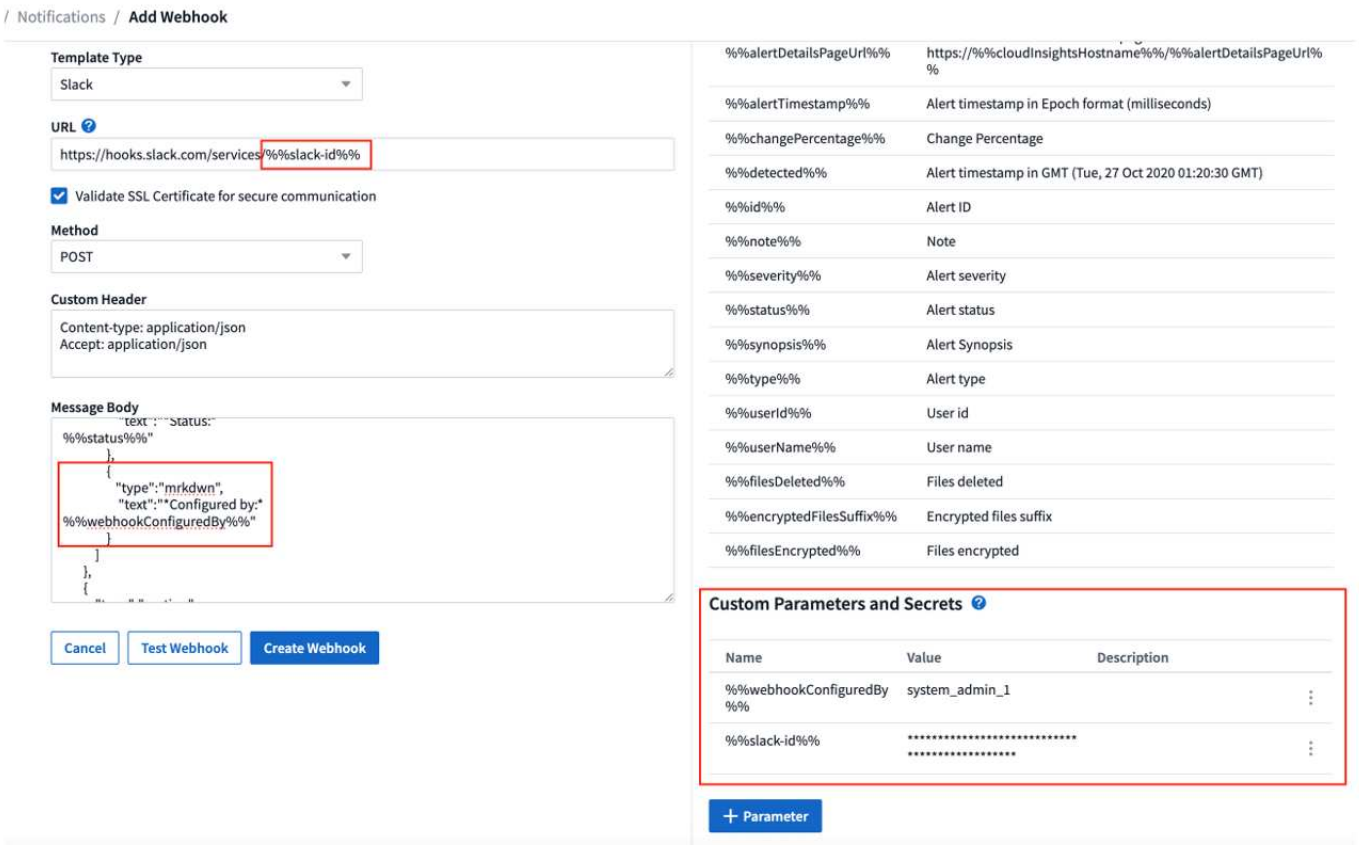
Alarmparameter sind dynamische Werte, die pro Alarm ausgefüllt werden. Beispielsweise wird der Parameter *%%severity%%* durch den Schweregradtyp der Warnung ersetzt.

Beachten Sie, dass beim Klicken auf die Schaltfläche „Webhook testen“ keine Ersetzungen durchgeführt werden. Der Test sendet eine Nutzlast, die die Platzhalter des Parameters (*%%<param-name>%%*) anzeigt, diese jedoch nicht durch Daten ersetzt.

Benutzerdefinierte Parameter und Geheimnisse

In diesem Abschnitt können Sie beliebige benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen. Ein benutzerdefinierter Parameter oder ein Geheimnis kann in der URL oder im Nachrichtentext enthalten sein. Mithilfe von Geheimnissen können Benutzer sichere benutzerdefinierte Parameter wie Kennwort, API-Schlüssel usw. konfigurieren.

Das folgende Beispielbild zeigt, wie benutzerdefinierte Parameter bei der Webhook-Erstellung verwendet werden.



Seite „Workload Security Webhooks – Liste“

Auf der Webhook-Listenseite werden die Felder „Name“, „Erstellt von“, „Erstellt am“, „Status“, „Sicher“ und „Zuletzt gemeldet“ angezeigt. Hinweis: Der Wert der Spalte „Status“ ändert sich ständig basierend auf dem Ergebnis des letzten Webhook-Triggers. Nachfolgend finden Sie Beispiele für Statusergebnisse.

Status	Beschreibung
OK	Benachrichtigung erfolgreich gesendet.

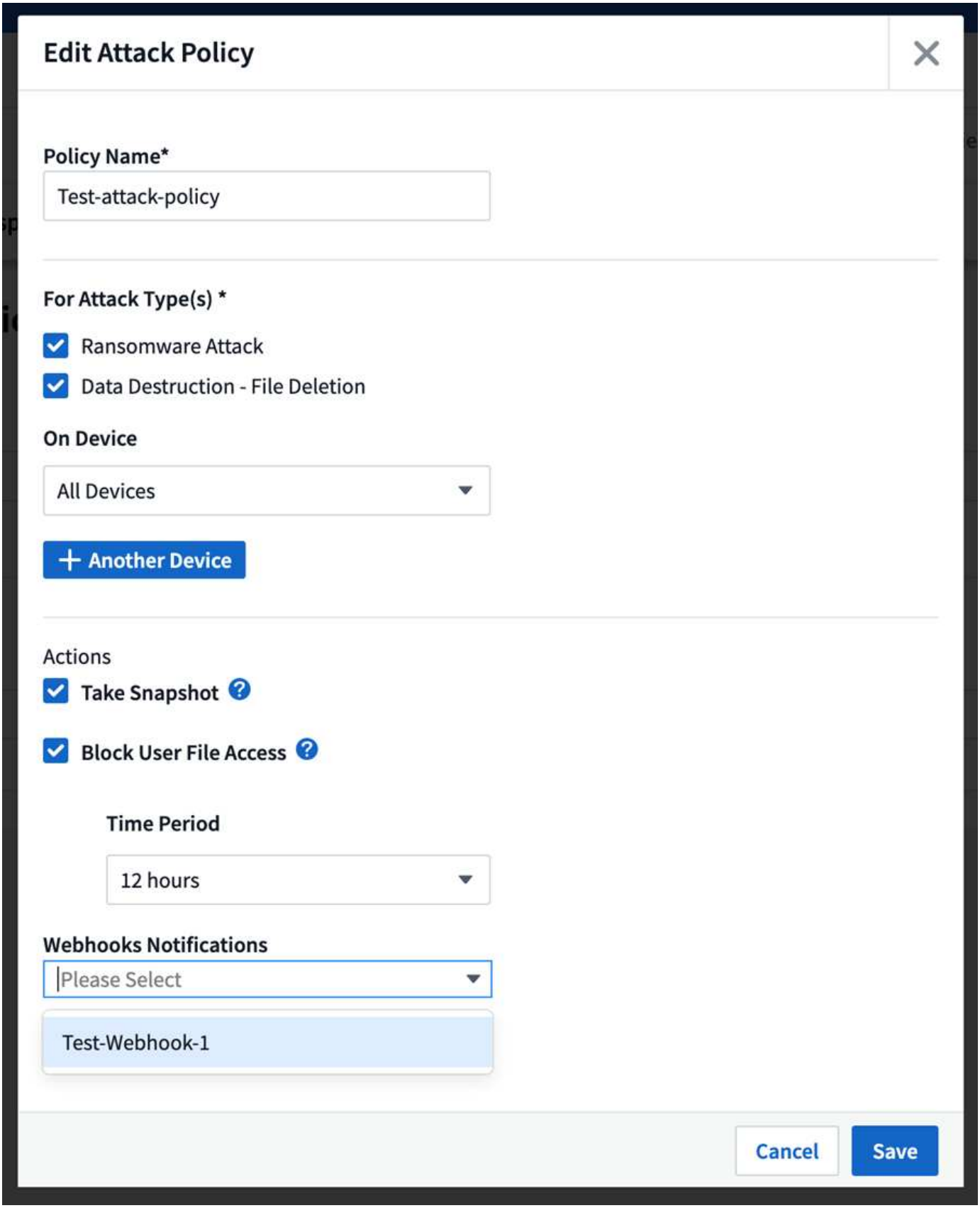
403	Verboten.
404	URL nicht gefunden.
400	Ungültige Anforderung. Dieser Status wird möglicherweise angezeigt, wenn im Nachrichtentext ein Fehler vorliegt, beispielsweise: • Schlecht formatiertes JSON. • Bereitstellung eines ungültigen Werts für reservierte Schlüssel. Beispielsweise akzeptiert PagerDuty für „Schweregrad“ nur „kritisch“/„Warnung“/„Fehler“/„Info“. Jedes andere Ergebnis kann zu einem 400-Status führen. • Anwendungsspezifische Validierungsfehler. Beispielsweise erlaubt Slack maximal 10 Felder innerhalb eines Abschnitts. Wenn Sie mehr als 10 angeben, kann dies zu einem 400-Status führen.
410	Ressource ist nicht mehr verfügbar

Die Spalte „Zuletzt gemeldet“ gibt den Zeitpunkt an, zu dem der Webhook zuletzt ausgelöst wurde.

Auf der Webhook-Listenseite können Benutzer Webhooks auch bearbeiten/duplizieren/löschen.

Konfigurieren der Webhook-Benachrichtigung in der Warnrichtlinie

Um einer Warnrichtlinie eine Webhook-Benachrichtigung hinzuzufügen, gehen Sie zu -Workload-Sicherheit > Richtlinien- und wählen Sie eine vorhandene Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu. Wählen Sie im Abschnitt „Aktionen“ > Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus.



Webhook-Benachrichtigungen sind an Richtlinien gebunden. Wenn der Angriff (RW/DD/WARN) stattfindet, wird die konfigurierte Aktion (Snapshot erstellen/Benutzer blockieren) ausgeführt und anschließend die zugehörige Webhook-Benachrichtigung ausgelöst.

Hinweis: E-Mail-Benachrichtigungen sind unabhängig von Richtlinien und werden wie gewohnt ausgelöst.

- Wenn eine Richtlinie angehalten wird, werden keine Webhook-Benachrichtigungen ausgelöst.
- An eine einzelne Richtlinie können mehrere Webhooks angehängt werden. Es wird jedoch empfohlen, nicht mehr als 5 Webhooks an eine Richtlinie anzuhängen.

Beispiele für Workload-Sicherheits-Webhooks

Webhooks für"Locker"

Webhooks für"PagerDuty" Webhooks für"Teams" Webhooks für"Zwietracht"

Workload Security Webhook-Beispiel für Discord

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Discord.

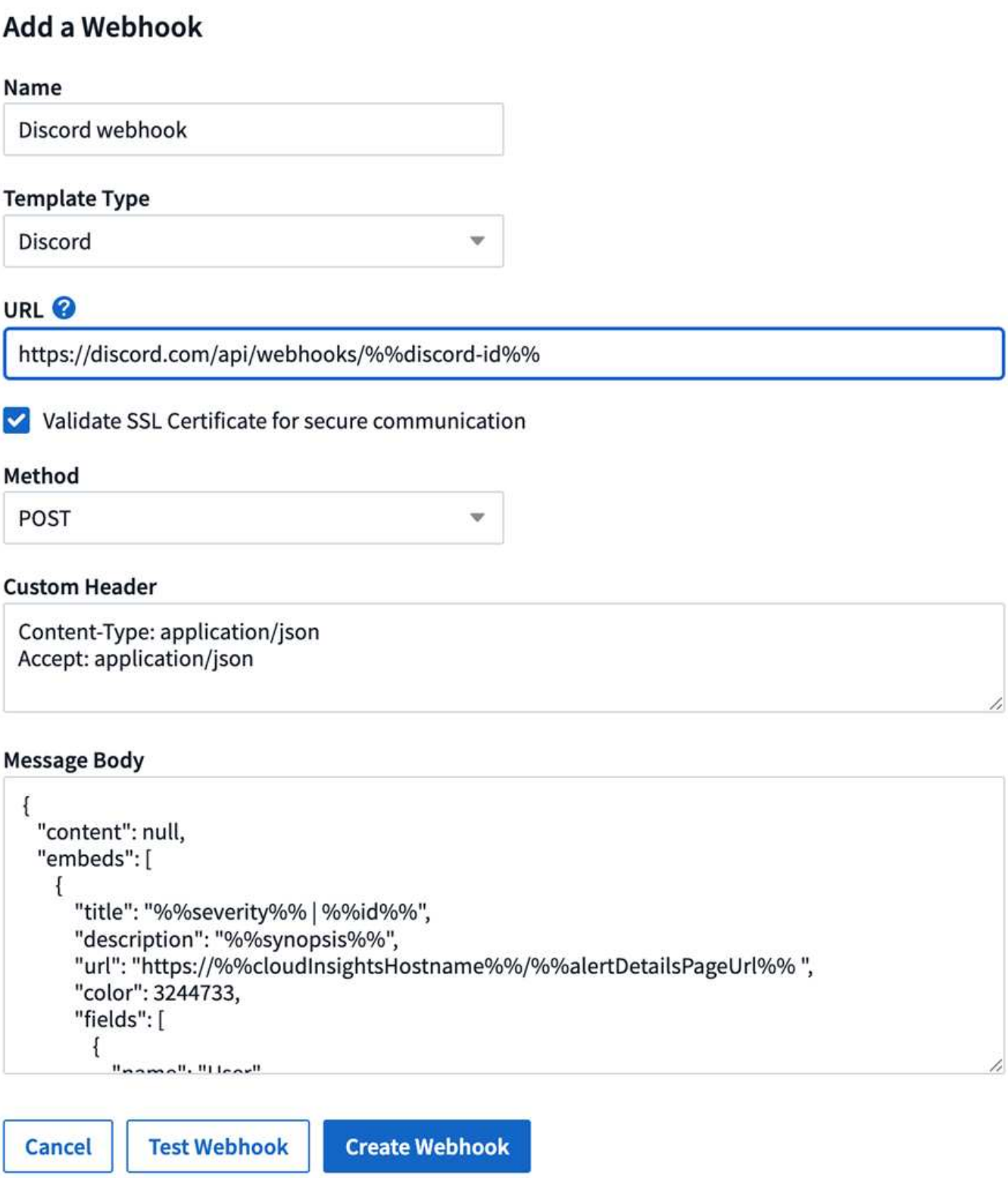
Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"Discord-Dokumentation" für die aktuellsten Informationen.

Discord-Setup:

- Wählen Sie in Discord den Server aus und wählen Sie unter „Textkanäle“ die Option „Kanal bearbeiten“ (Zahnradsymbol).
- Wählen Sie **Integrationen > Webhooks anzeigen** und klicken Sie auf **Neuer Webhook**
- Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload-Sicherheits-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Klicken Sie auf „+ Webhook“, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Discord** aus.
4. Fügen Sie die Discord-URL von oben in das Feld *URL* ein.



Um den Webhook zu testen, ersetzen Sie den URL-Wert im Nachrichtentext vorübergehend durch eine beliebige gültige URL (z. B. *https://netapp.com*) und klicken Sie dann auf die Schaltfläche *Webhook testen*. Discord erfordert die Angabe einer gültigen URL, damit die Test-Webhook-Funktionalität funktioniert.

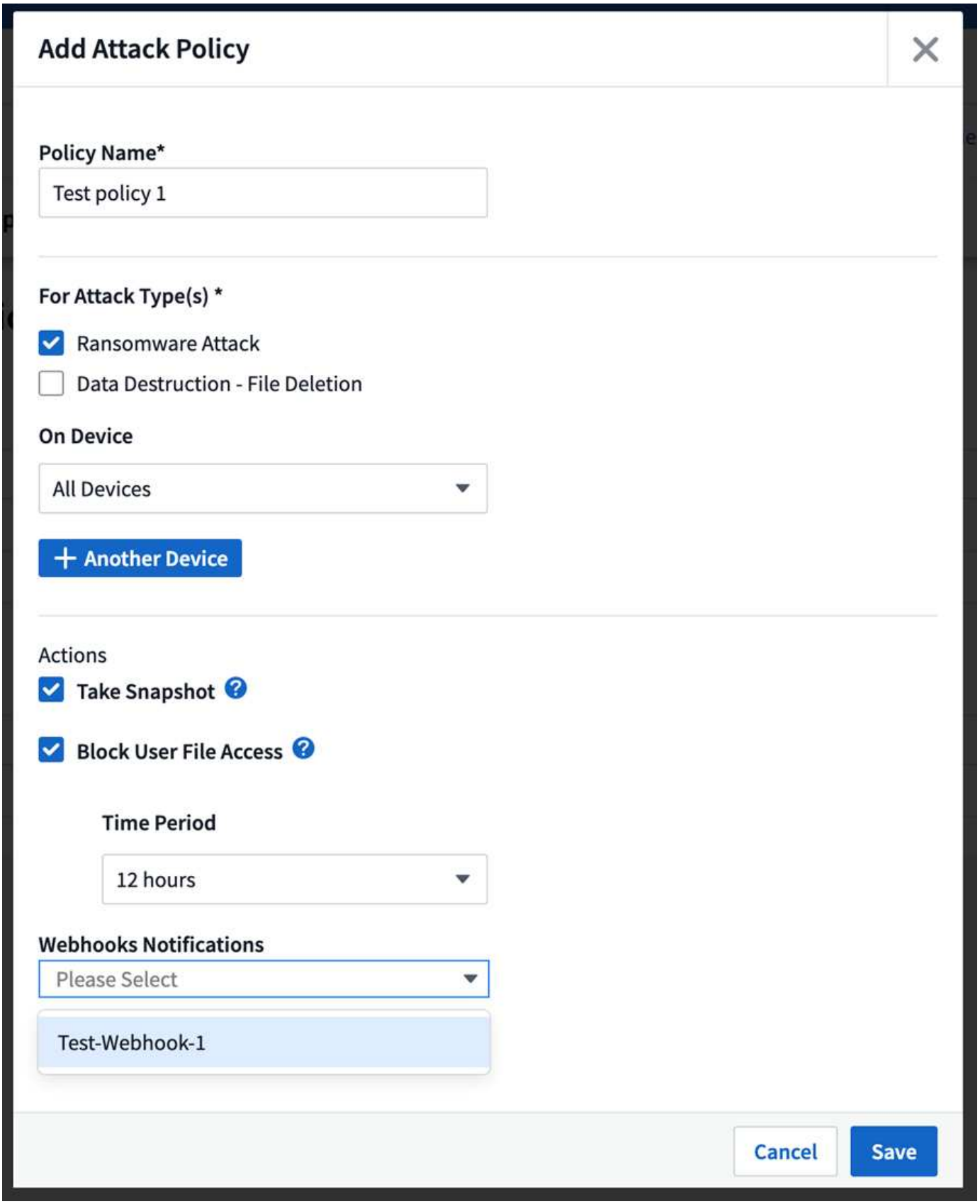
Denken Sie daran, den Nachrichtentext nach Abschluss des Tests wiederherzustellen.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, denen die Richtlinie zugeordnet werden soll, und erforderliche Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die gewünschten Discord-Webhooks aus und speichern Sie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload Security Webhook-Beispiel für PagerDuty

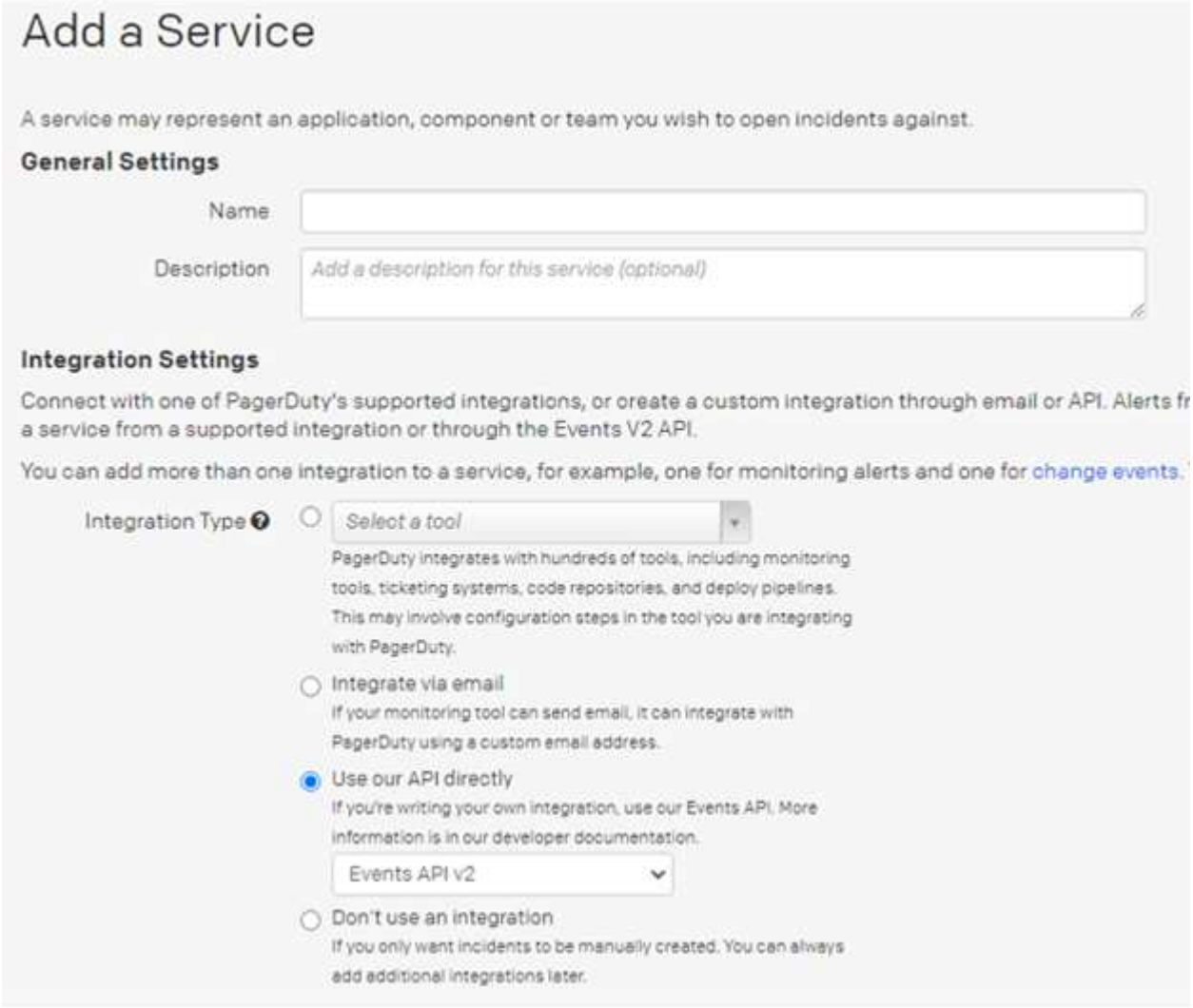
Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal

Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für PagerDuty.

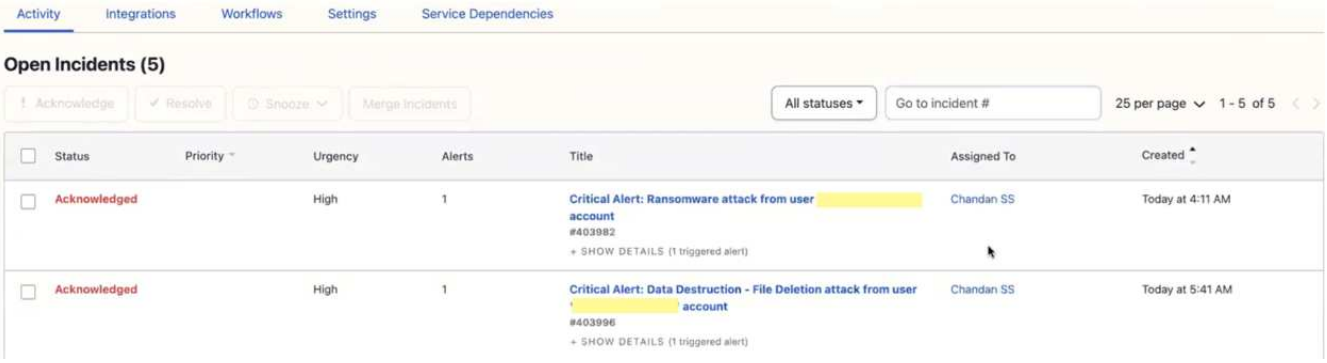
Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"PagerDuty-Dokumentation" für die aktuellsten Informationen.

PagerDuty-Setup:

1. Navigieren Sie in PagerDuty zu **Dienste > Dienstverzeichnis** und klicken Sie auf die Schaltfläche **+Neuer Dienst**.
2. Geben Sie einen *Namen* ein und wählen Sie *Unsere API direkt verwenden*. Wählen Sie *Dienst hinzufügen*.

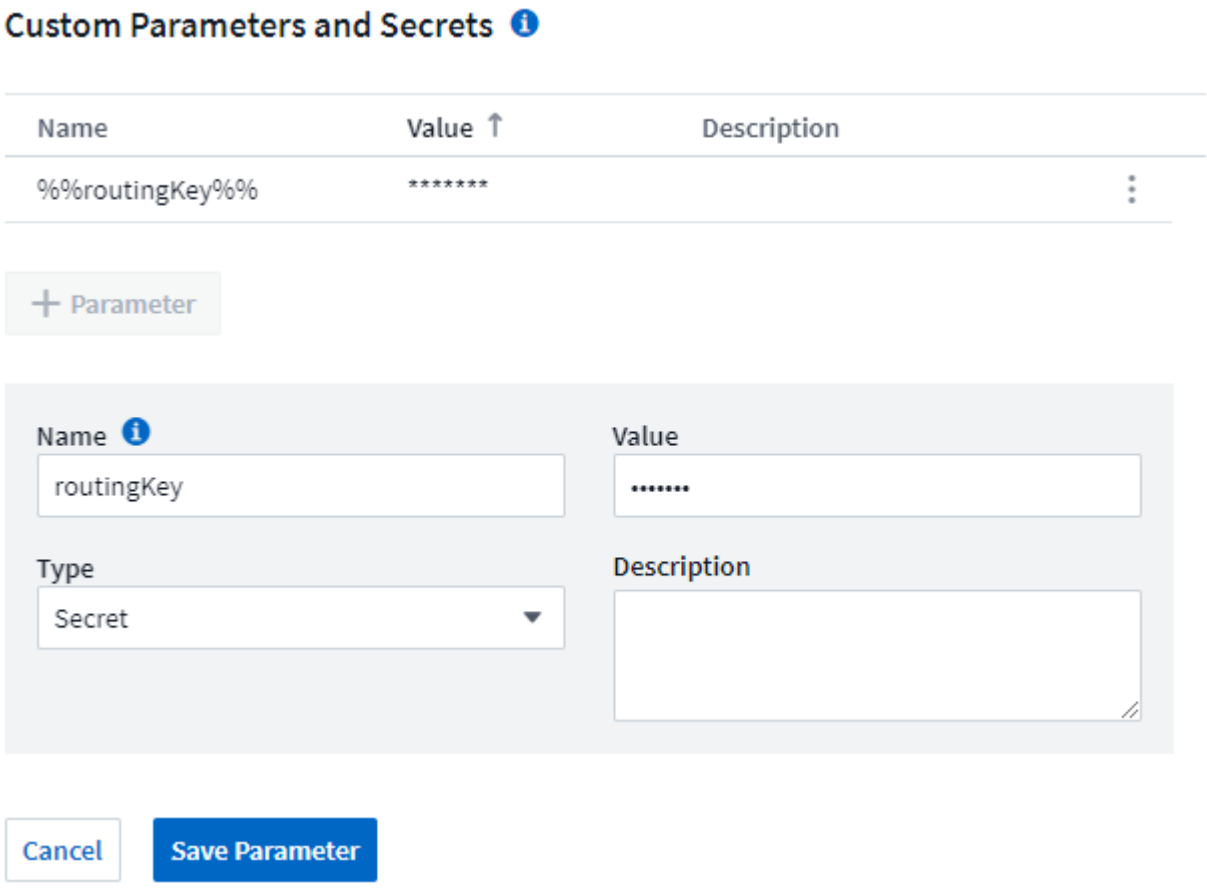


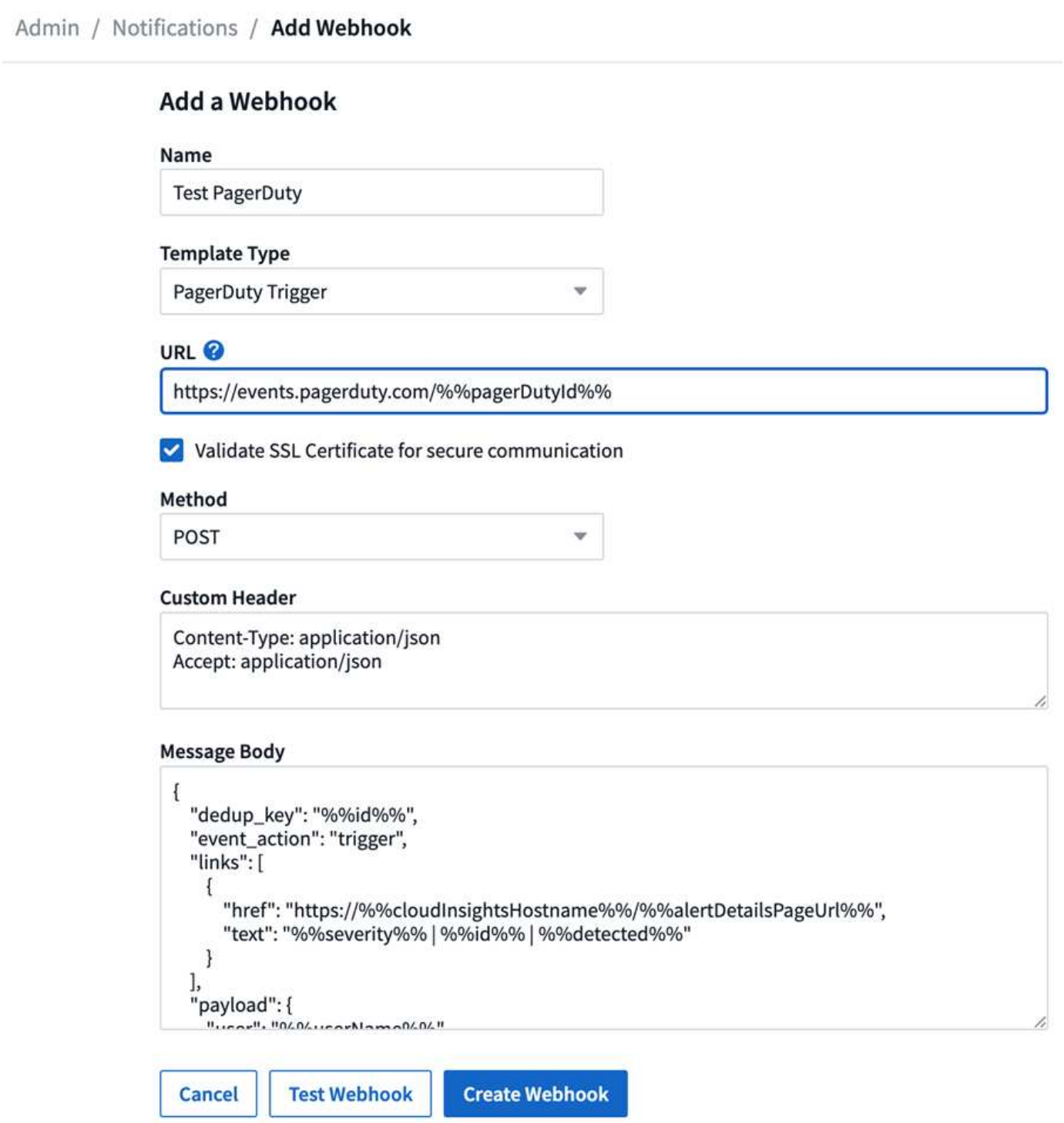
3. Wählen Sie die Registerkarte *Integrationen*, um den **Integrationsschlüssel** anzuzeigen. Sie benötigen diesen Schlüssel, wenn Sie unten den Workload Security-Webhook erstellen.
4. Gehen Sie zu **Vorfälle** oder **Dienste**, um Warnungen anzuzeigen.



Erstellen Sie einen Workload Security PagerDuty-Webhook:

- Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie „+ Webhook“, um einen neuen Webhook zu erstellen.
- Geben Sie dem Webhook einen aussagekräftigen Namen.
- Wählen Sie im Dropdown-Menü *Vorlagentyp* die Option *PagerDuty-Trigger* aus.
- Erstellen Sie ein benutzerdefiniertes Parametergeheimnis mit dem Namen *routingKey* und legen Sie den Wert auf den oben erstellten PagerDuty-*Integrationsschlüssel* fest.

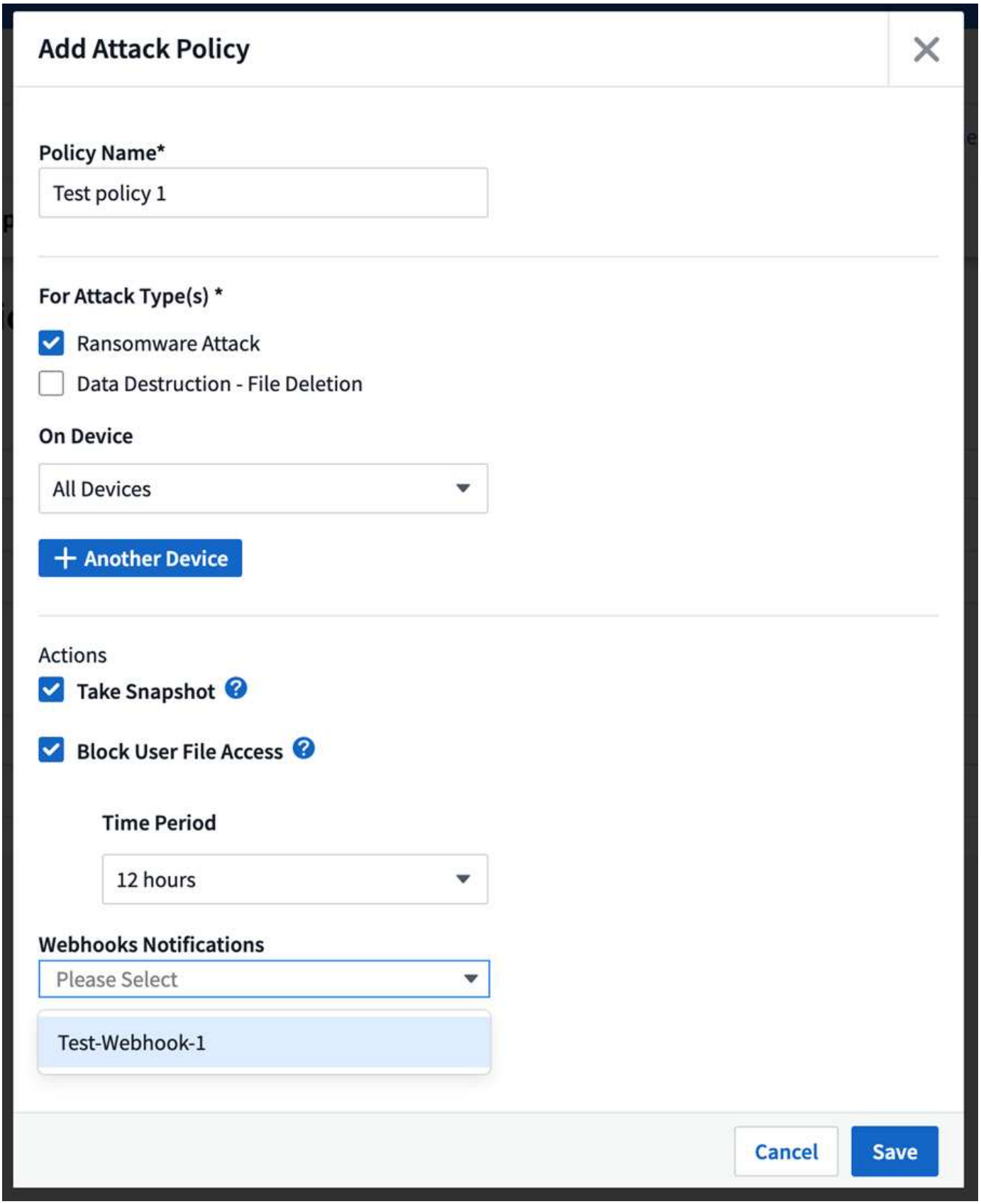




Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Wählen Sie *+Angriffsrichtlinie* oder *+Warnrichtlinie*.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die erforderlichen Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen PagerDuty-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload Security Webhook-Beispiel für Slack

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Slack.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Die aktuellsten Informationen finden Sie in der Slack-Dokumentation.

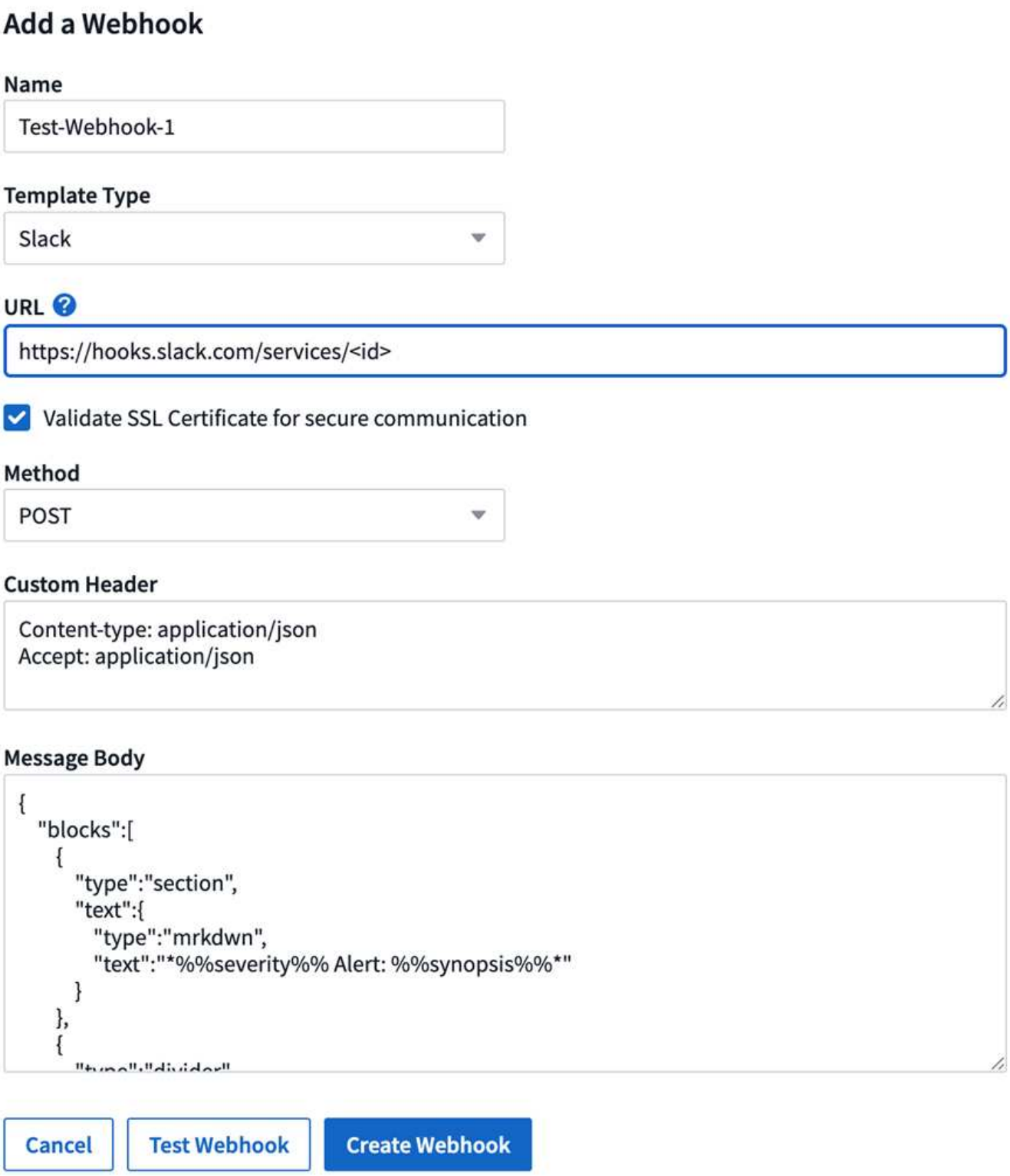
Slack-Beispiel

- Gehe zu https://api.slack.com/apps und erstellen Sie eine neue App. Geben Sie ihm einen aussagekräftigen Namen und wählen Sie einen Arbeitsbereich aus.

- Gehen Sie zu „Eingehende Webhooks“, klicken Sie auf „Eingehende Webhooks aktivieren“, wählen Sie „Neuen Webhook hinzufügen“ und wählen Sie den Kanal aus, auf dem gepostet werden soll.
- Kopieren Sie die Webhook-URL. Diese URL wird beim Erstellen eines Workload Security-Webhooks angegeben.

Erstellen Sie einen Slack-Webhook für die Workload-Sicherheit

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie + *Webhook*, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü *Vorlagentyp* die Option *Slack* aus.
4. Fügen Sie die oben kopierte URL ein.

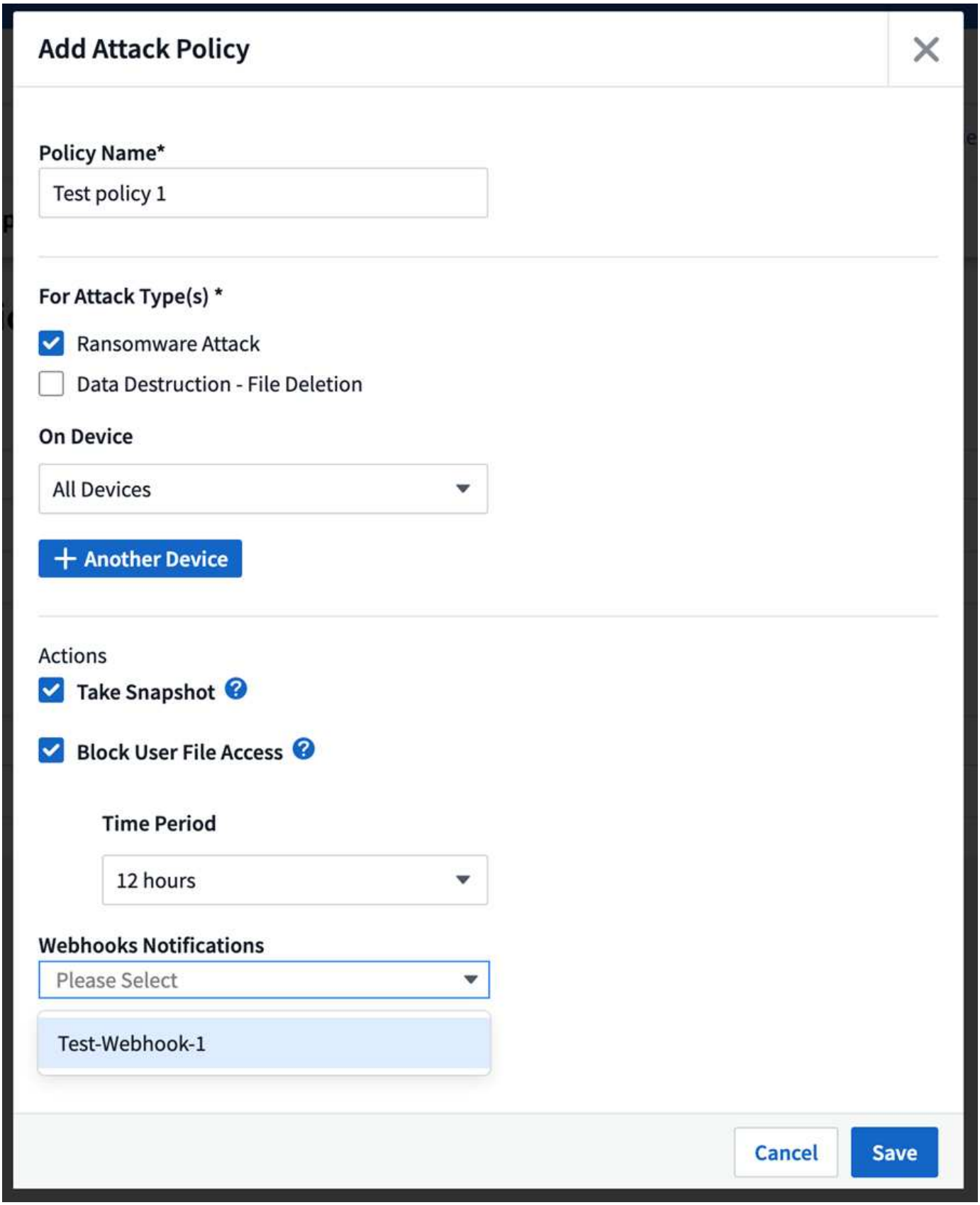


Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und erforderliche Aktionen aus.

- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.


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

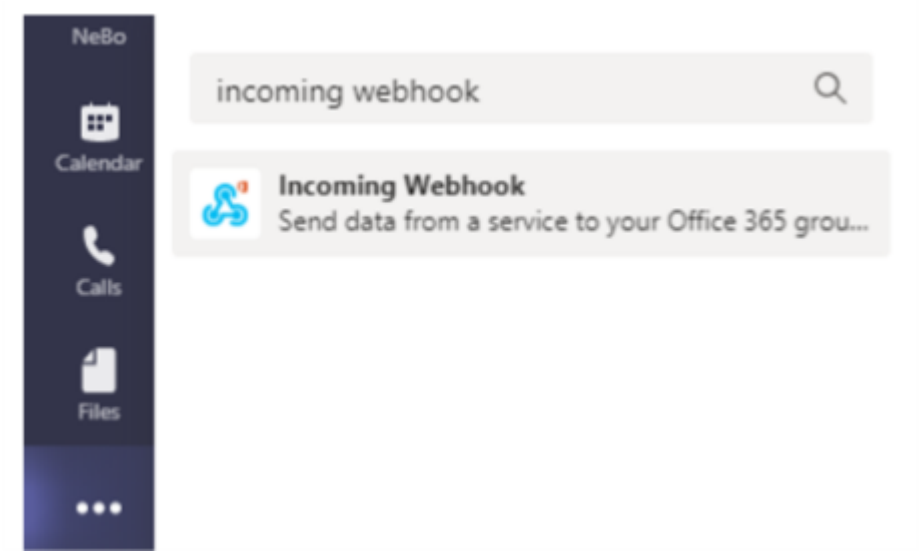
Beispiel für einen Workload-Sicherheits-Webhook für Microsoft Teams

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Teams.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"Teams-Dokumentation" für die aktuellsten Informationen.

Teams-Setup:

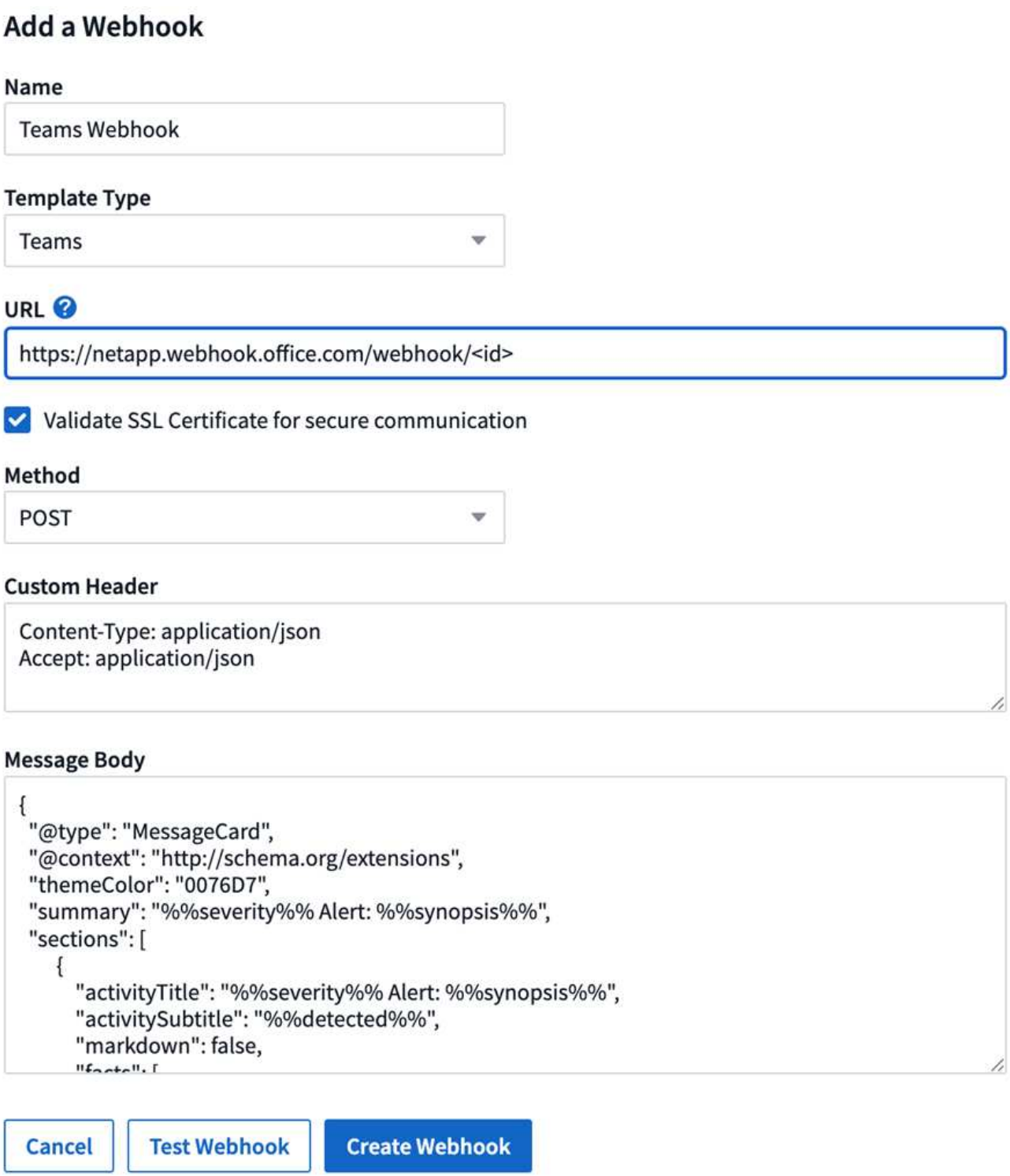
1. Wählen Sie in Teams den Kebab aus und suchen Sie nach „Eingehender Webhook“.



2. Wählen Sie **Zu einem Team hinzufügen > Ein Team auswählen > Einen Connector einrichten**.
3. Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload Security Teams-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie + *Webhook*, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „Teams“ aus.



4. Fügen Sie die URL von oben in das Feld *URL* ein.

Schritte zum Erstellen einer Teams-Benachrichtigung mit der Adaptive Card-Vorlage

1. Ersetzen Sie den Nachrichtentext durch die folgende Vorlage:

```
{
"type": "message",
```

```
"attachments": [
  {
    "contentType": "application/vnd.microsoft.card.adaptive",
    "content": {
      "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
      "type": "AdaptiveCard",
      "version": "1.2",
      "body": [
        {
          "type": "TextBlock",
          "text": "%%severity%% Alert: %%synopsis%%",
          "wrap": true,
          "weight": "Bolder",
          "size": "Large"
        },
        {
          "type": "TextBlock",
          "text": "%%detected%%",
          "wrap": true,
          "isSubtle": true,
          "spacing": "Small"
        },
        {
          "type": "FactSet",
          "facts": [
            {
              "title": "User",
              "value": "%%userName%%"
            },
            {
              "title": "Attack/Abnormal Behavior",
              "value": "%%type%%"
            },
            {
              "title": "Action taken",
              "value": "%%actionTaken%%"
            },
            {
              "title": "Files encrypted",
              "value": "%%filesEncrypted%%"
            },
            {
              "title": "Encrypted files suffix",
              "value": "%%encryptedFilesSuffix%%"
            },
            {
```

```
                "title": "Files deleted",
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Wenn Sie Power Automate Flows verwenden, sind die Abfrageparameter in der URL im codierten Format. Sie müssen die URL decodieren, bevor Sie sie eingeben.
3. Klicken Sie auf „Test Webhook“, um sicherzustellen, dass keine Fehler vorliegen.
4. Speichern Sie den Webhook.

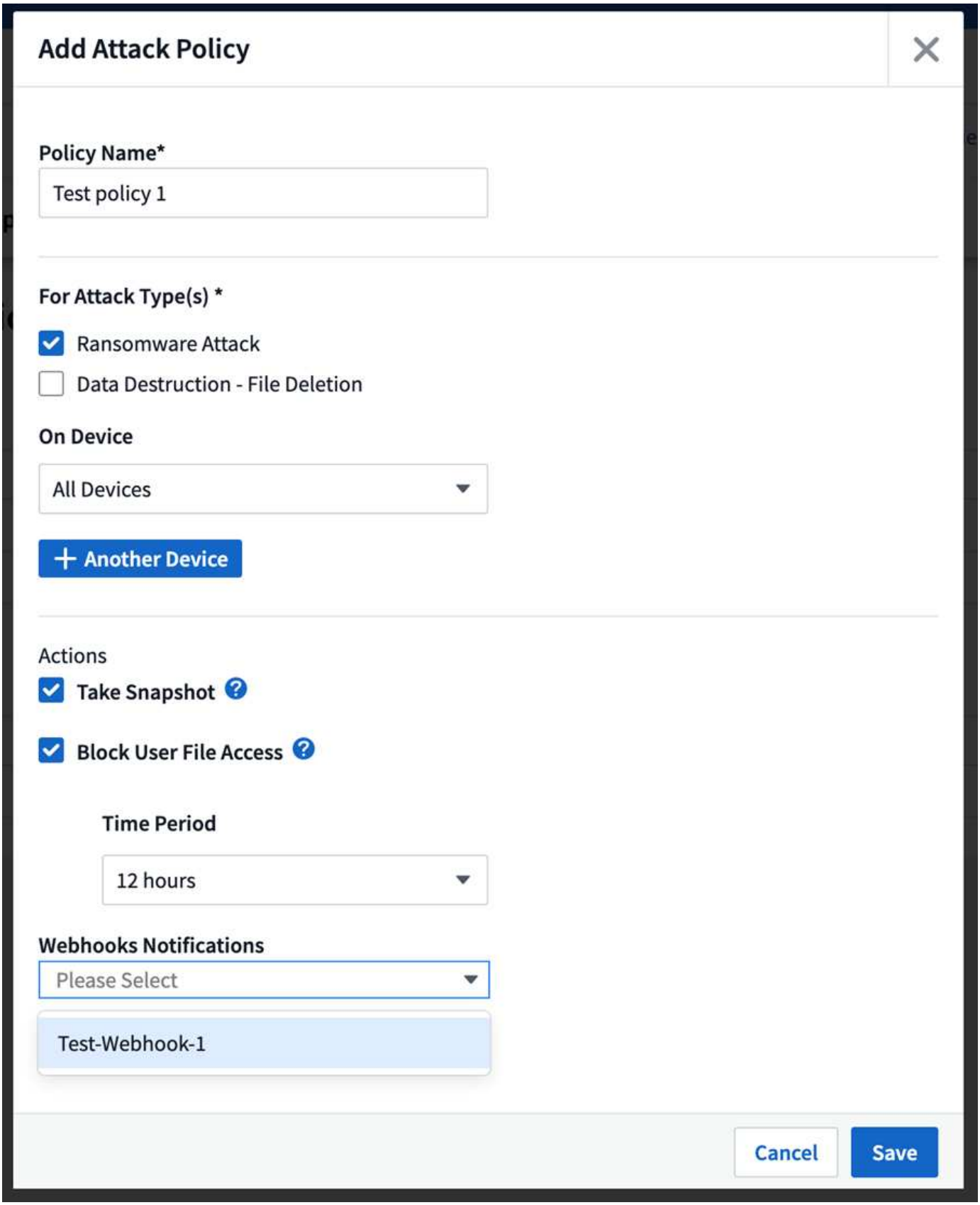
Benachrichtigungen per Webhook

Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Wählen Sie *+Angriffsrichtlinie* oder *+Warnrichtlinie*.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.

- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die erforderlichen Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Teams-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.


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