Notifications Webhook

Data Infrastructure Insights

NetApp
February 03, 2026

Sommaire

Notifications Webhook

Notifications de sécurité de la charge de travail à l'aide de webhooks

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte critiques ou d'avertissement à diverses applications à l'aide d'un canal webhook personnalisé.

De nombreuses applications commerciales prennent en charge les webhooks comme interface d'entrée standard, par exemple : Slack, PagerDuty, Teams et Discord. En prenant en charge un canal webhook générique et personnalisable, Workload Security peut prendre en charge bon nombre de ces canaux de diffusion. Des informations sur la configuration des webhooks peuvent être trouvées sur les sites Web des applications respectives. Par exemple, Slack fournit"ce guide utile" .

Vous pouvez créer plusieurs canaux webhook, chaque canal ciblant un objectif différent, des applications distinctes, des destinataires différents, etc.

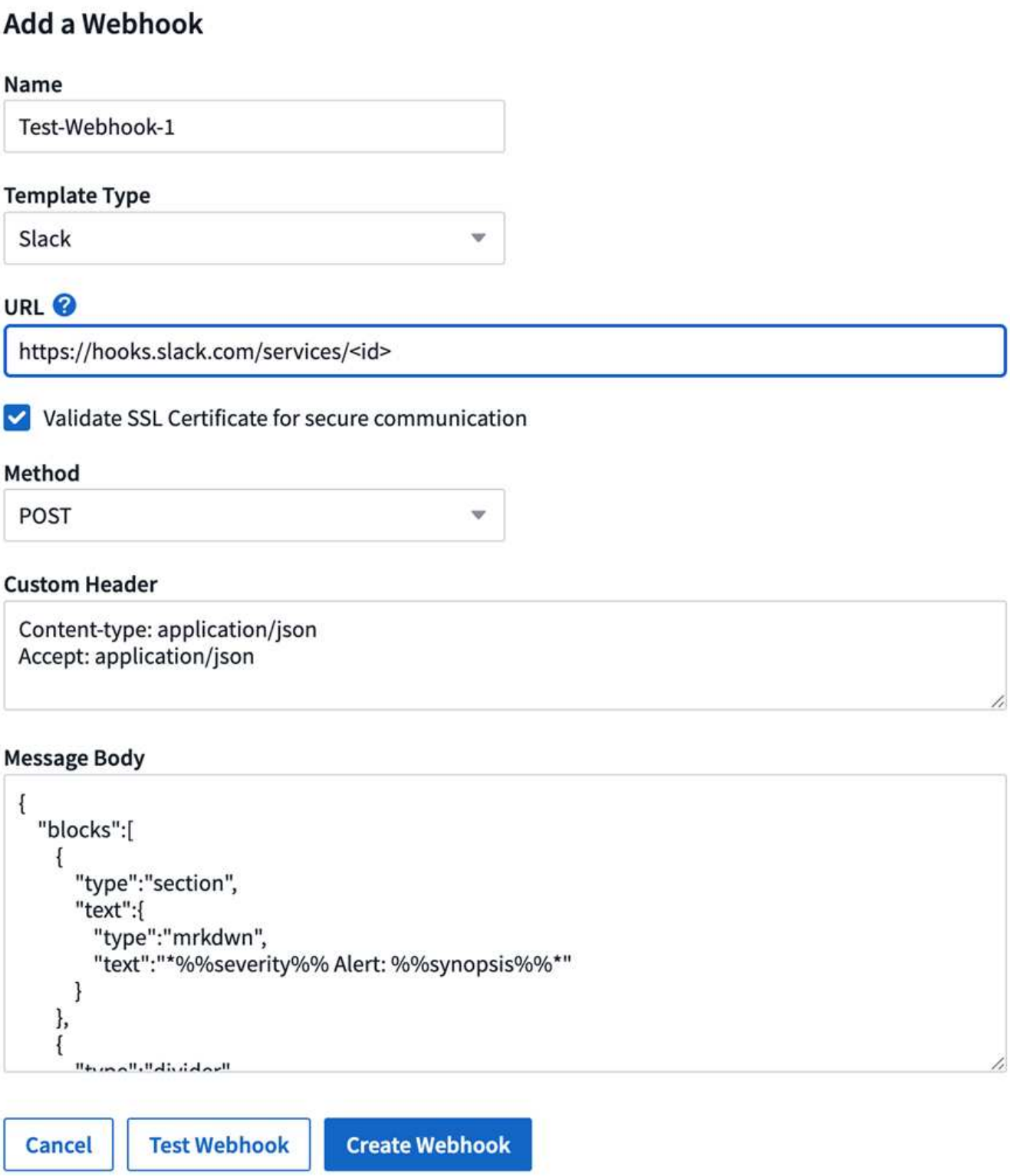
L'instance de canal webhook est composée des éléments suivants

Nom	Description
URL	URL cible du webhook, y compris le préfixe http:// ou https:// ainsi que les paramètres d'URL
Méthode	GET/POST - La valeur par défaut est POST
En-tête personnalisé	Spécifiez ici les en-têtes personnalisés
Corps du message	Mettez le corps de votre message ici
Paramètres d'alerte par défaut	Répertorie les paramètres par défaut du webhook
Paramètres et secrets personnalisés	Les paramètres et secrets personnalisés vous permettent d'ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Créer un webhook

Pour créer un Webhook de sécurité de charge de travail, accédez à Admin > Notifications et sélectionnez l'onglet « Webhooks de sécurité de charge de travail ». L'image suivante montre un exemple d'écran de création de webhook Slack.

Remarque : l'utilisateur doit être un administrateur de Workload Security pour créer et gérer les Webhooks de Workload Security.



- Saisissez les informations appropriées pour chacun des champs et cliquez sur « Enregistrer ».
- Vous pouvez également cliquer sur le bouton « Tester le Webhook » pour tester la connexion. Notez que cela enverra le « Corps du message » (sans substitutions) à l'URL définie selon la méthode sélectionnée.
- Les webhooks SWS comprennent un certain nombre de paramètres par défaut. De plus, vous pouvez créer vos propres paramètres ou secrets personnalisés.

Paramètres : que sont-ils et comment les utiliser ?

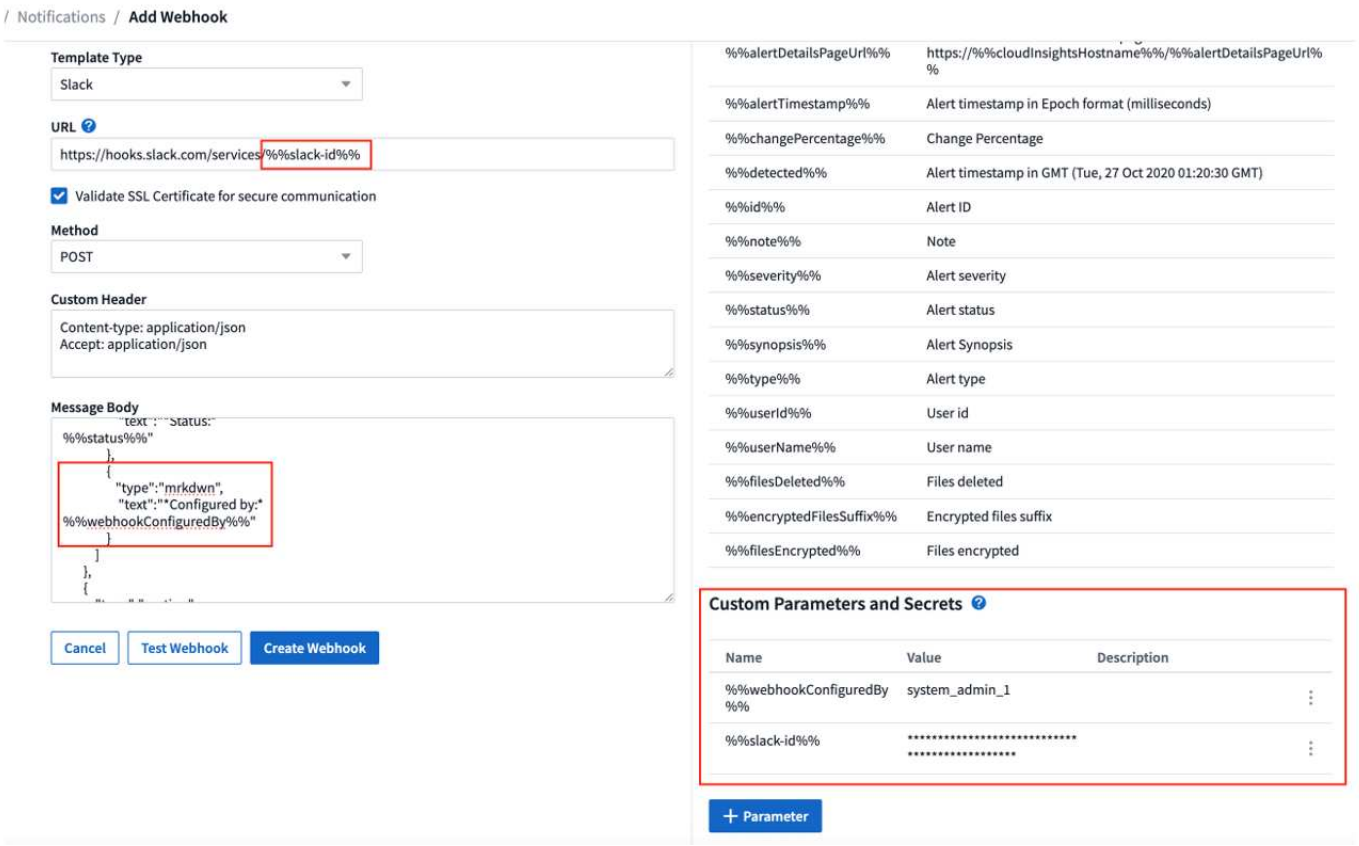
Les paramètres d'alerte sont des valeurs dynamiques renseignées par alerte. Par exemple, le paramètre *%%severity%%* sera remplacé par le type de gravité de l'alerte.

Notez que les substitutions ne sont pas effectuées lorsque vous cliquez sur le bouton « Tester le Webhook » ; le test envoie une charge utile qui affiche les espaces réservés du paramètre (*%%<param-name>%%*) mais ne les remplace pas par des données.

Paramètres et secrets personnalisés

Dans cette section, vous pouvez ajouter tous les paramètres personnalisés et/ou secrets que vous souhaitez. Un paramètre personnalisé ou un secret peut figurer dans l'URL ou le corps du message. Les secrets permettent à l'utilisateur de configurer un paramètre personnalisé sécurisé comme un mot de passe, une clé API, etc.

L'exemple d'image suivant montre comment les paramètres personnalisés sont utilisés dans la création de webhook.



Page de liste des webhooks de sécurité de la charge de travail

Sur la page de liste des Webhooks, les champs Nom, Créé par, Créé le, Statut, Sécurisé et Dernier signalement sont affichés. Remarque : la valeur de la colonne « statut » continuera de changer en fonction du résultat du dernier déclencheur de webhook. Voici quelques exemples de résultats d'état.

Statut	Description
OK	Notification envoyée avec succès.

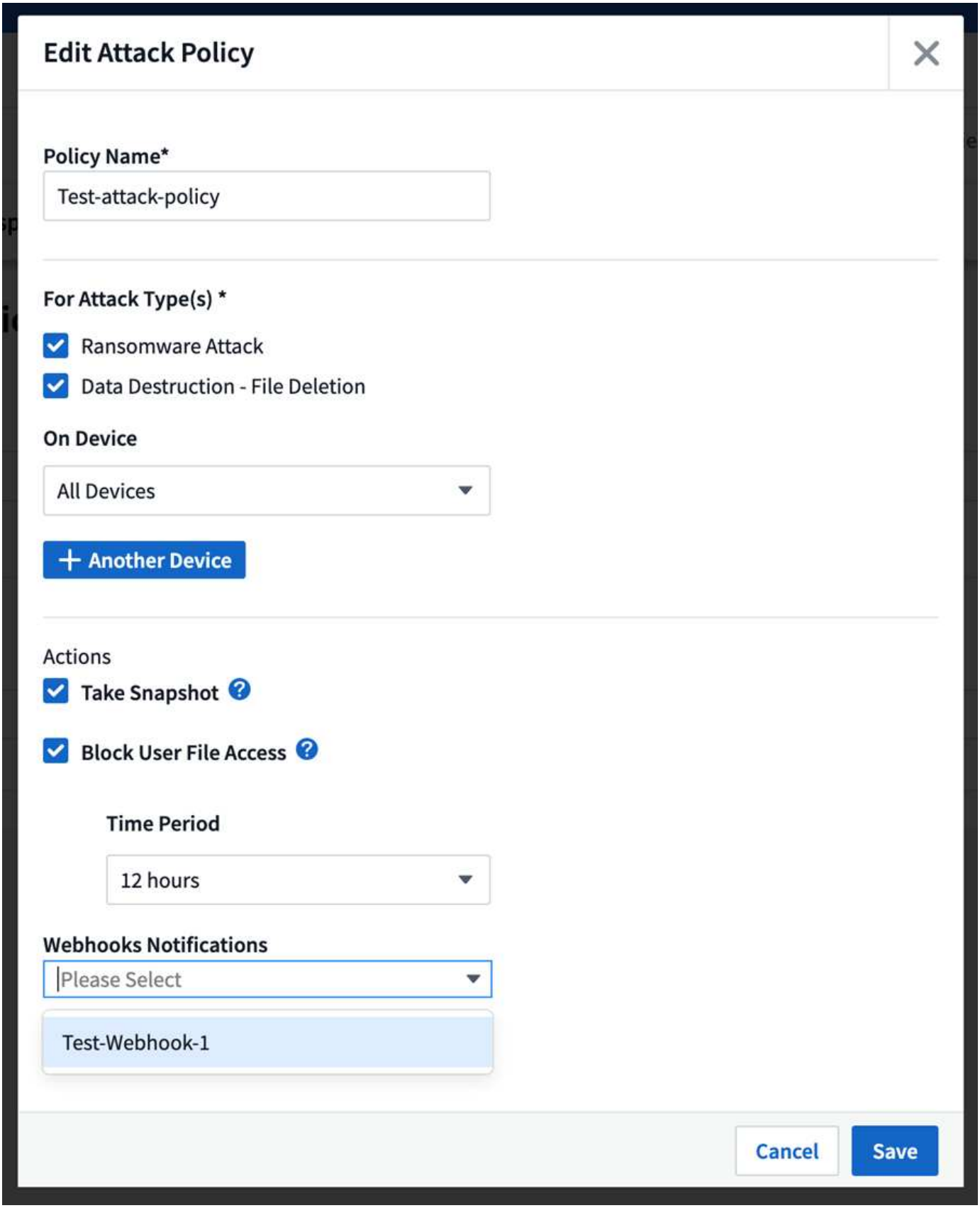
403	Interdit.
404	URL non trouvée.
400	Mauvaise demande. Vous pouvez voir ce statut s'il y a une erreur dans le corps du message, par exemple : • Json mal formaté. • Fourniture d'une valeur non valide pour les clés réservées. Par exemple, PagerDuty accepte uniquement les valeurs critiques/avertissements/erreurs/informations pour « Gravité ». Tout autre résultat peut donner un statut 400. • Erreurs de validation spécifiques à l'application. Par exemple, Slack autorise un maximum de 10 champs dans une section. L'inclusion de plus de 10 peut entraîner un statut 400.
410	La ressource n'est plus disponible

La colonne « Dernier signalement » indique l'heure à laquelle le webhook a été déclenché pour la dernière fois.

À partir de la page de liste des webhooks, les utilisateurs peuvent également modifier/dupliquer/supprimer les webhooks.

Configurer la notification Webhook dans la politique d'alerte

Pour ajouter une notification webhook à une politique d'alerte, accédez à - Sécurité de la charge de travail > Politiques - et sélectionnez une politique existante ou ajoutez une nouvelle politique. Dans la section *Actions* > liste déroulante *Notifications Webhook*, sélectionnez les webhooks requis.



Les notifications Webhook sont liées aux politiques. Lorsque l'attaque (RW/DD/WARN) se produit, l'action configurée (Prendre un instantané / blocage de l'utilisateur) sera effectuée, puis la notification webhook associée sera déclenchée.

Remarque : les notifications par e-mail sont indépendantes des politiques, elles seront déclenchées comme d'habitude.

- Si une politique est suspendue, les notifications webhook ne seront pas déclenchées.
- Plusieurs webhooks peuvent être attachés à une seule politique, mais il est recommandé de ne pas attacher plus de 5 webhooks à une politique.

Exemples de webhooks de sécurité de charge de travail

Webhooks pour"Mou"

Webhooks pour"PagerDuty" Webhooks pour"Équipes" Webhooks pour"Discorde"

Exemple de webhook de sécurité de charge de travail pour Discord

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Discord.

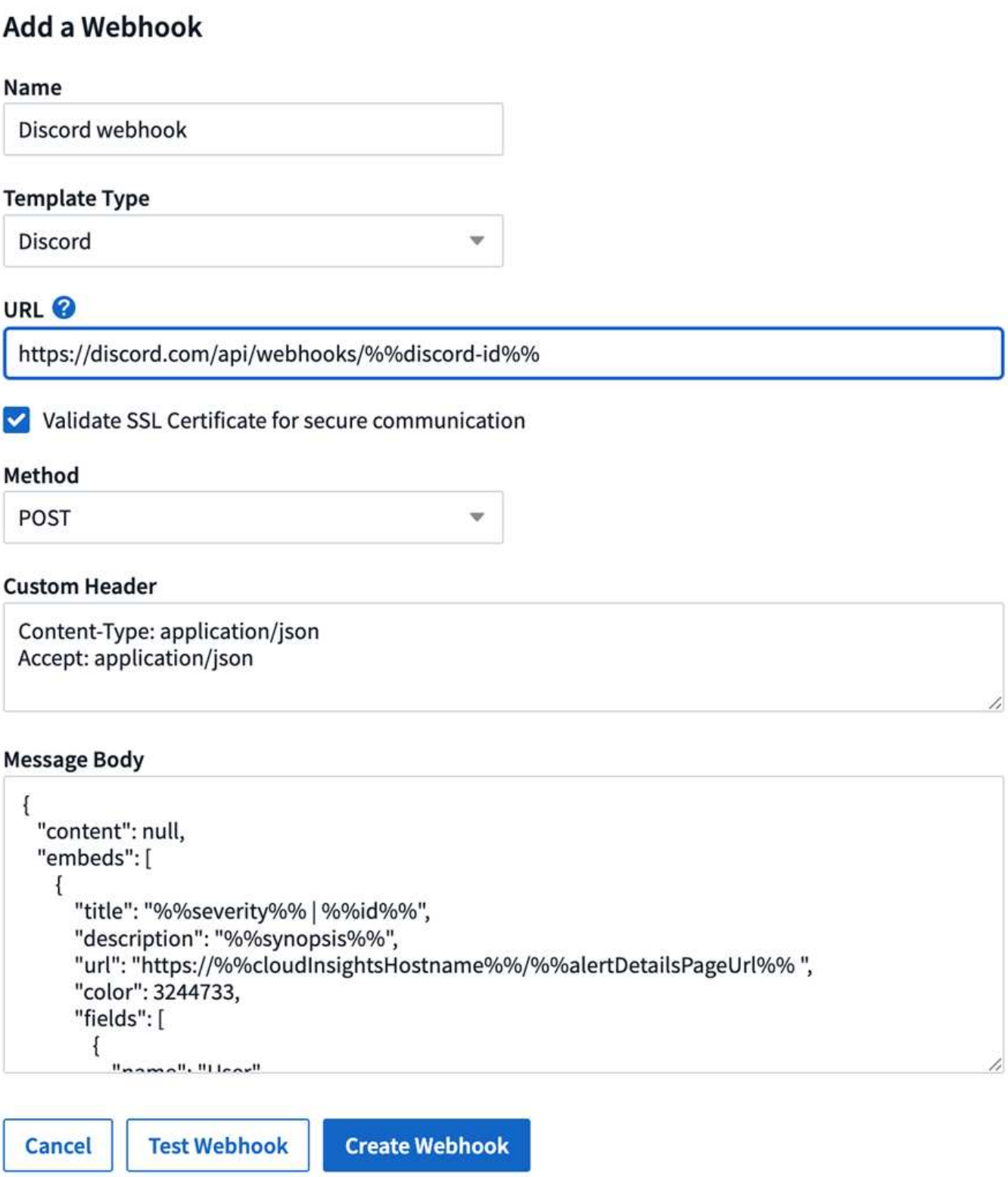
Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation Discord" pour les informations les plus récentes.

Configuration de Discord :

- Dans Discord, sélectionnez le serveur, sous Canaux texte, sélectionnez Modifier le canal (icône en forme d'engrenage)
- Sélectionnez **Intégrations > Afficher les webhooks** et cliquez sur **Nouveau webhook**
- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook de sécurité de charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Cliquez sur « + Webhook » pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Discord**.
4. Collez l'URL Discord ci-dessus dans le champ *URL*.



Afin de tester le webhook, remplacez temporairement la valeur de l'URL dans le corps du message par n'importe quelle URL valide (telle que *https://netapp.com*), puis cliquez sur le bouton *Tester le Webhook*. Discord exige qu'une URL valide soit fournie pour que la fonctionnalité Test Webhook fonctionne.

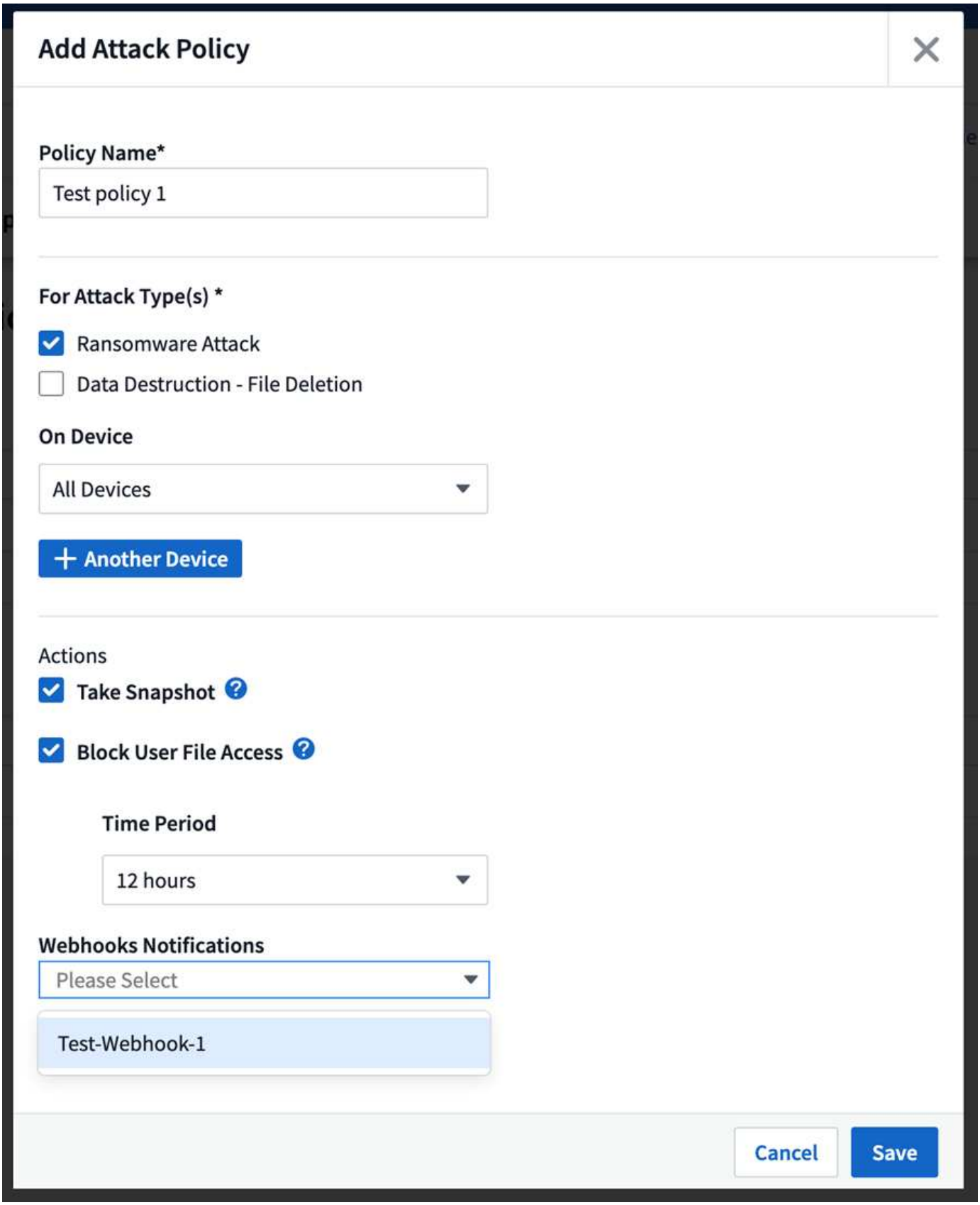
Assurez-vous de réinitialiser le corps du message une fois le test terminé.

Notifications via Webhook

Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Discord requis et enregistrez.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.


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

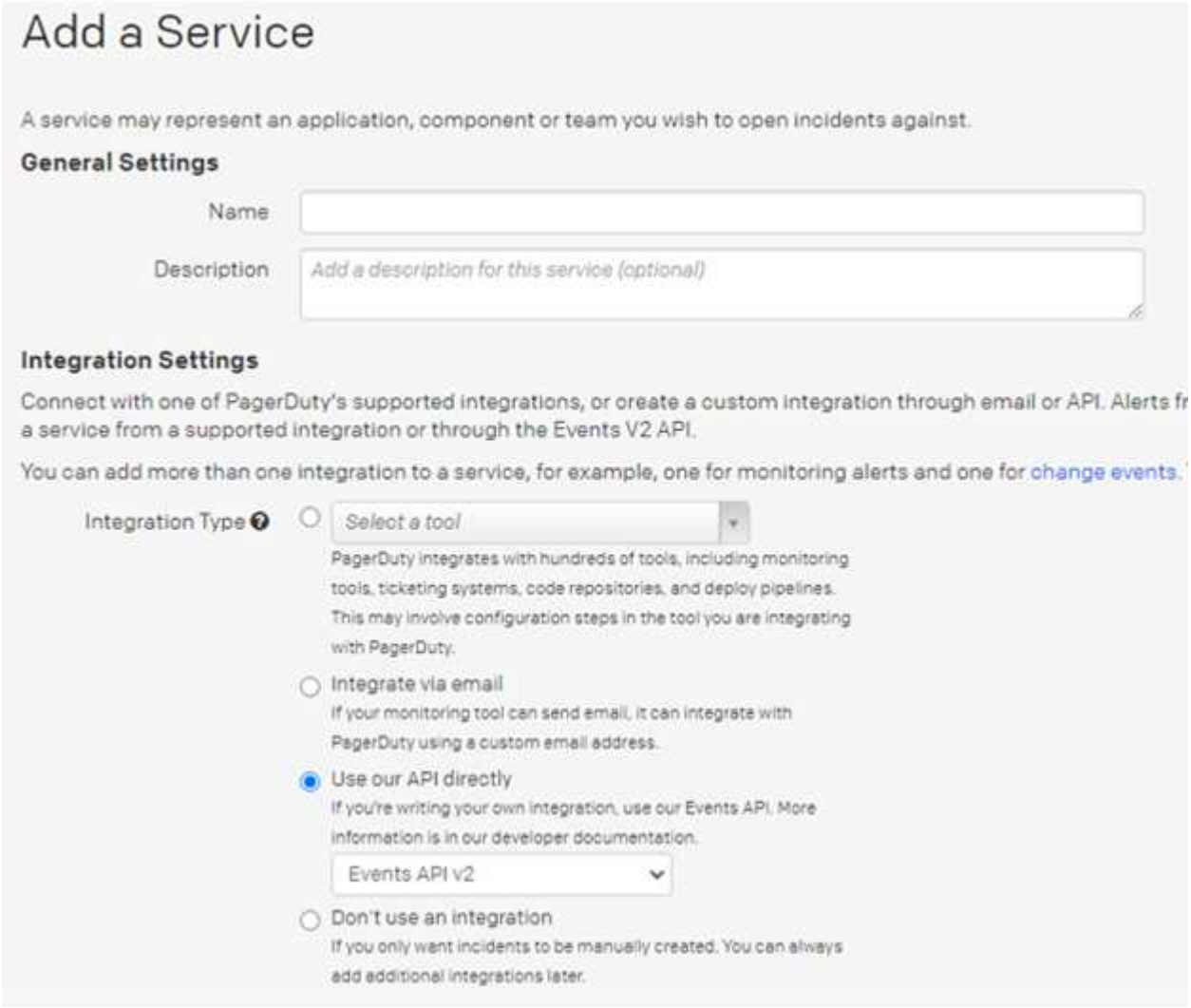
Exemple de webhook de sécurité de charge de travail pour PagerDuty

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour PagerDuty.

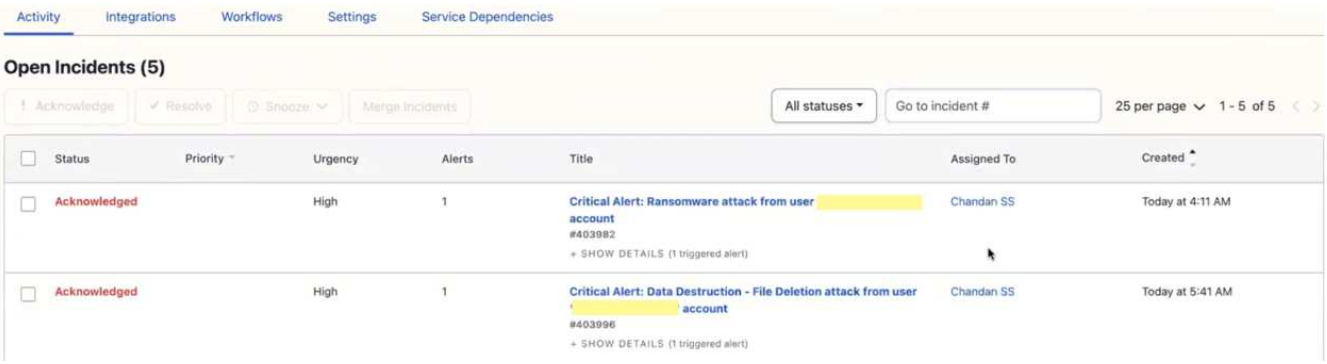
Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation de PagerDuty" pour les informations les plus récentes.

Configuration de PagerDuty :

1. Dans PagerDuty, accédez à **Services > Répertoire des services** et cliquez sur le bouton **+Nouveau service**.
2. Saisissez un *Nom* et sélectionnez *Utiliser directement notre API*. Sélectionnez *Ajouter un service*.

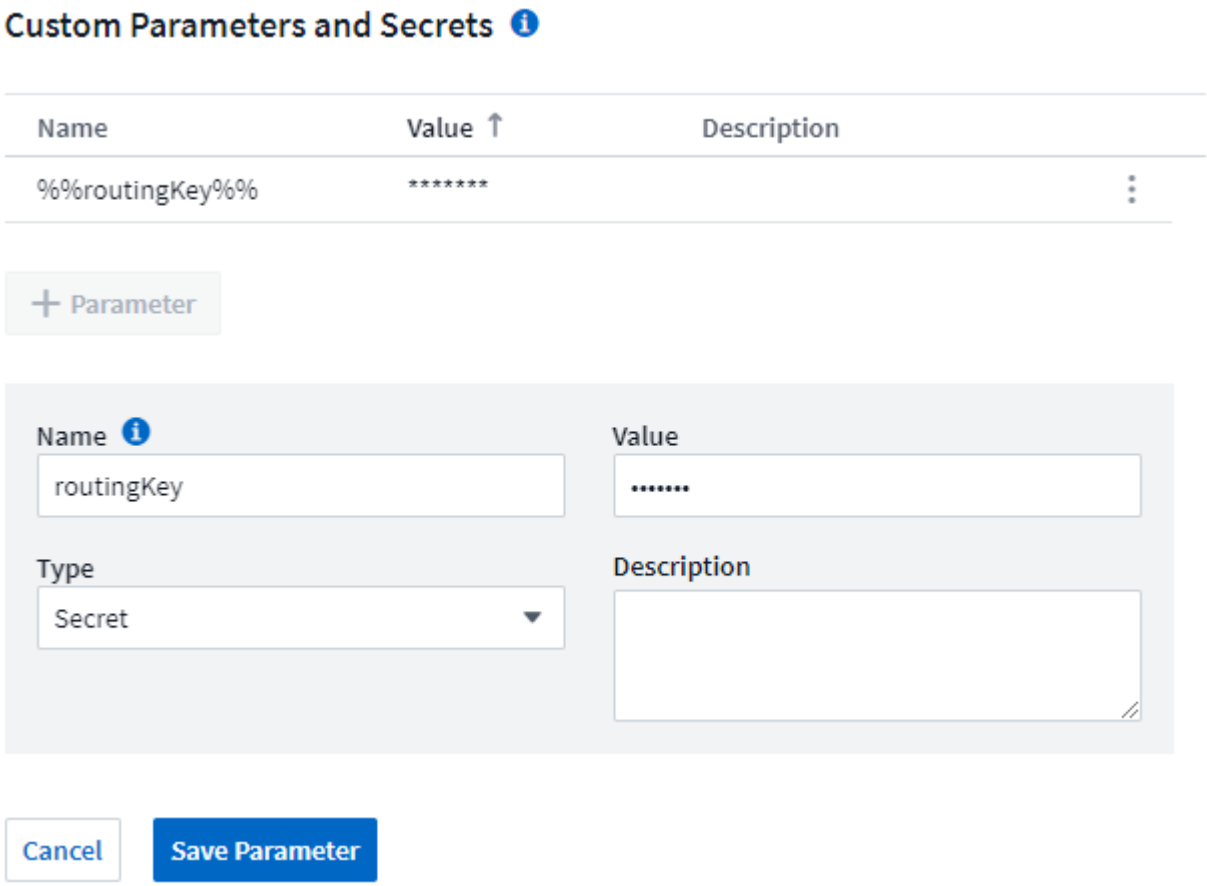


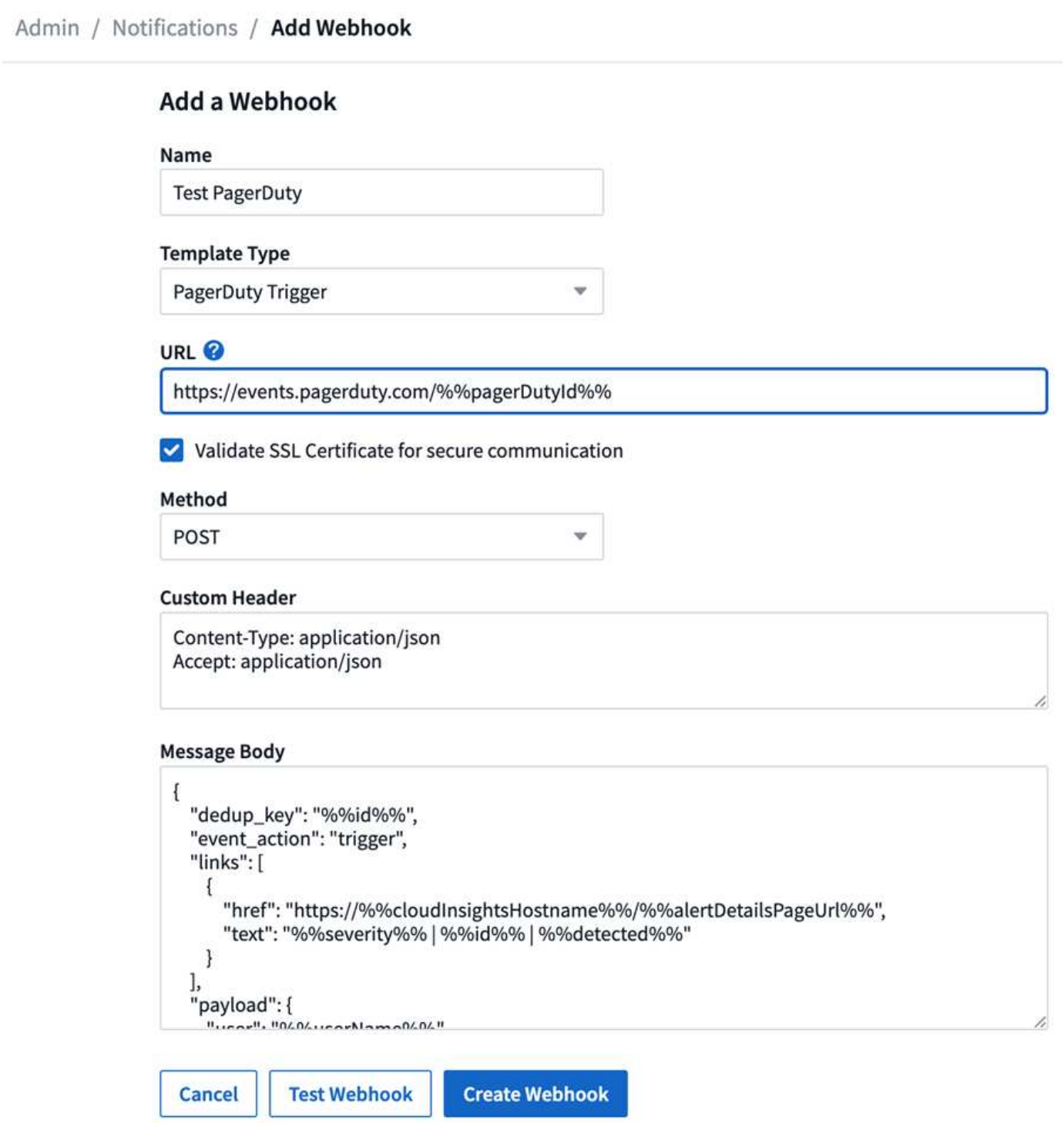
3. Sélectionnez l'onglet *Intégrations* pour voir la **Clé d'intégration**. Vous aurez besoin de cette clé lorsque vous créerez le webhook Workload Security ci-dessous.
4. Accédez à **Incidents** ou **Services** pour afficher les alertes.



Créer un Webhook PagerDuty de sécurité de charge de travail :

- Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez « + Webhook » pour créer un nouveau webhook.
- Donnez au webhook un nom significatif.
- Dans la liste déroulante *Type de modèle*, sélectionnez *Déclencheur PagerDuty*.
- Créez un secret de paramètre personnalisé nommé *routingKey* et définissez la valeur sur la clé d'intégration PagerDuty *Integration Key* créée ci-dessus.

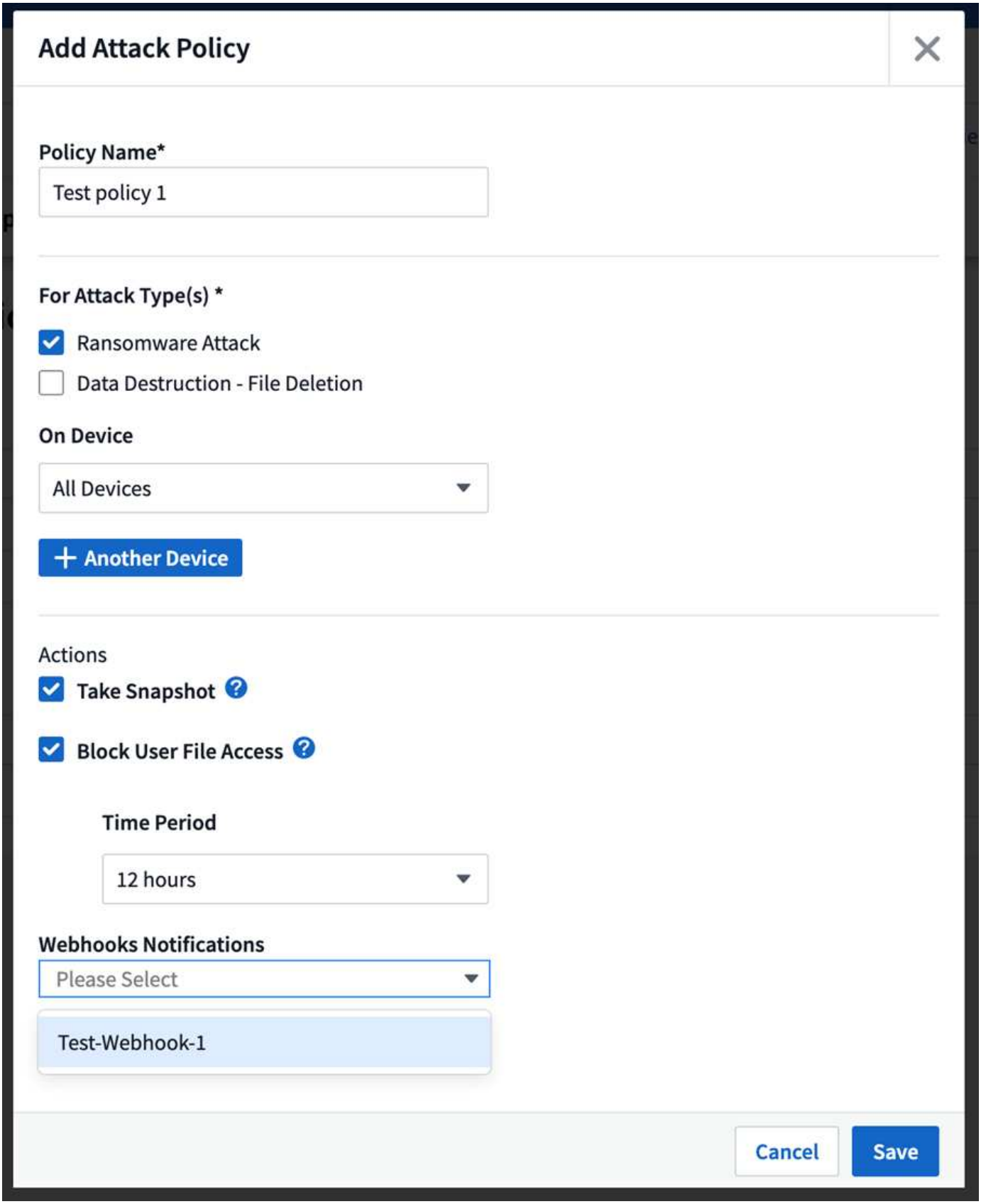




Notifications via Webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la politique doit être attachée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks PagerDuty requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



Exemple de webhook de sécurité de charge de travail pour Slack

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Slack.

Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Consultez la documentation Slack pour obtenir les informations les plus récentes.

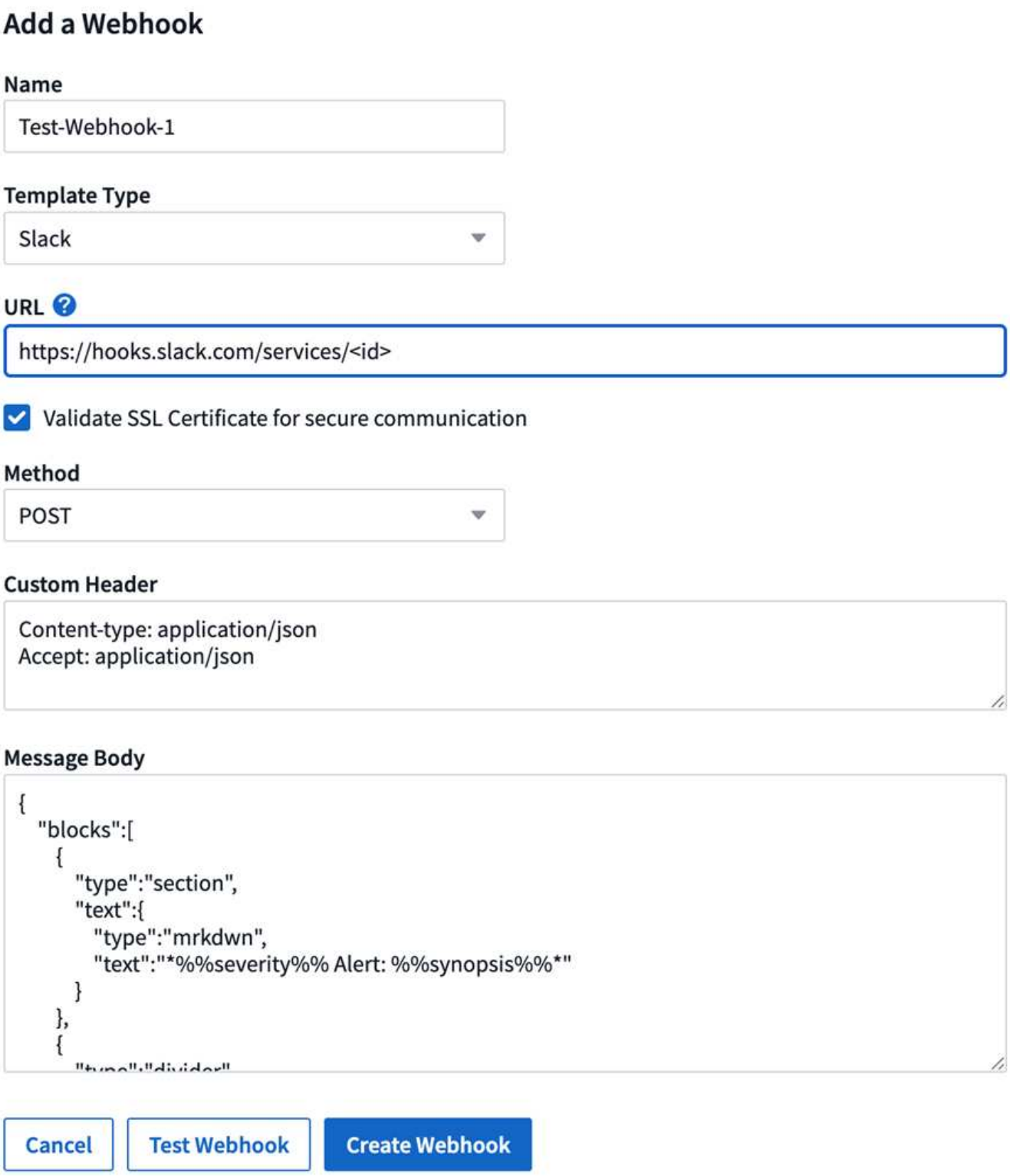
Exemple de Slack

- Aller à https://api.slack.com/apps et créez une nouvelle application. Donnez-lui un nom significatif et sélectionnez un espace de travail.

- Accédez à Webhooks entrants, cliquez sur *Activer les Webhooks entrants*, sélectionnez *Ajouter un nouveau Webhook* et sélectionnez le canal sur lequel publier.
- Copiez l'URL du Webhook. Cette URL sera fournie lors de la création d'un webhook Workload Security.

Créer un webhook Slack pour la sécurité de la charge de travail

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez _+ *Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez *Slack*.
4. Collez l'URL copiée ci-dessus.

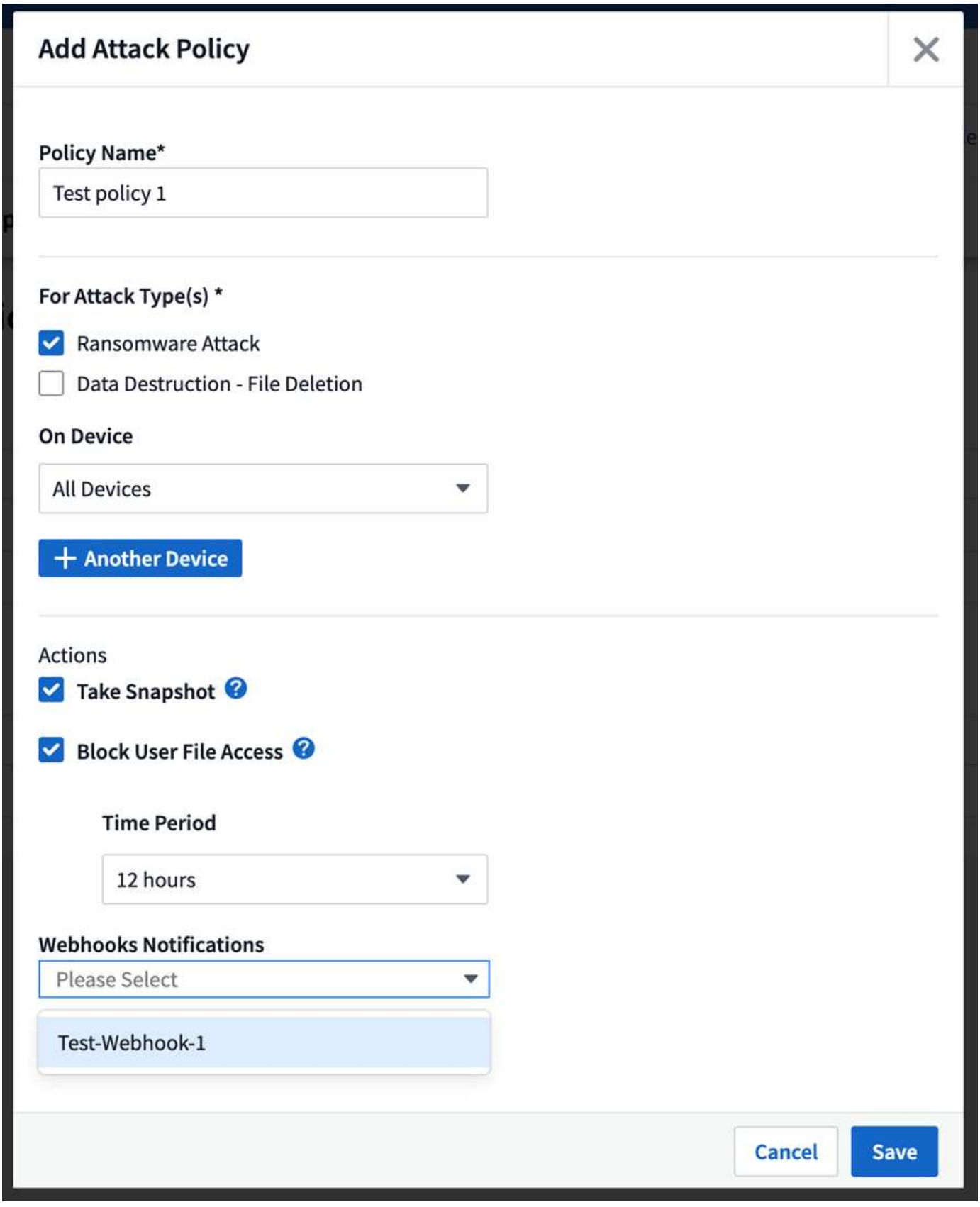


Notifications via webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail* > *Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les appareils auxquels la politique doit être attachée et les actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



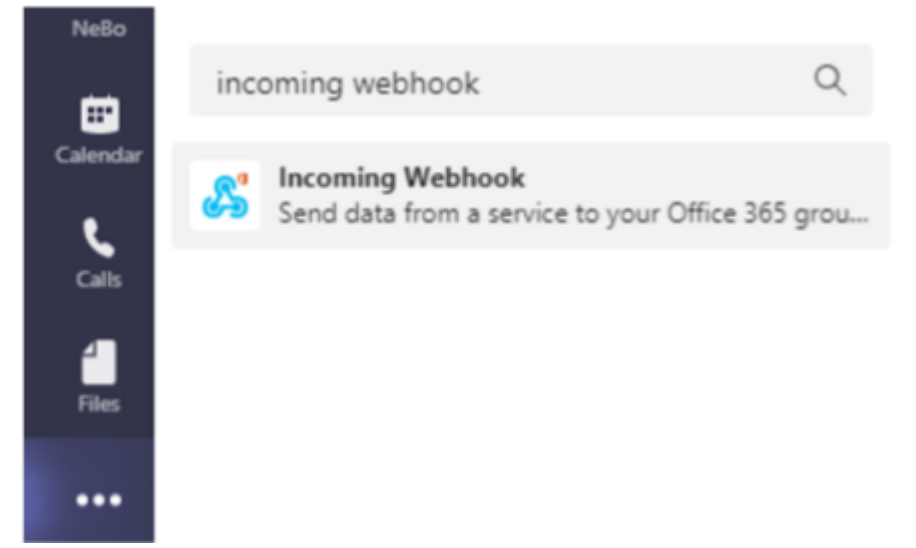
Exemple de webhook de sécurité de charge de travail pour Microsoft Teams

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Teams.

Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation des équipes" pour les informations les plus récentes.

Configuration des équipes :

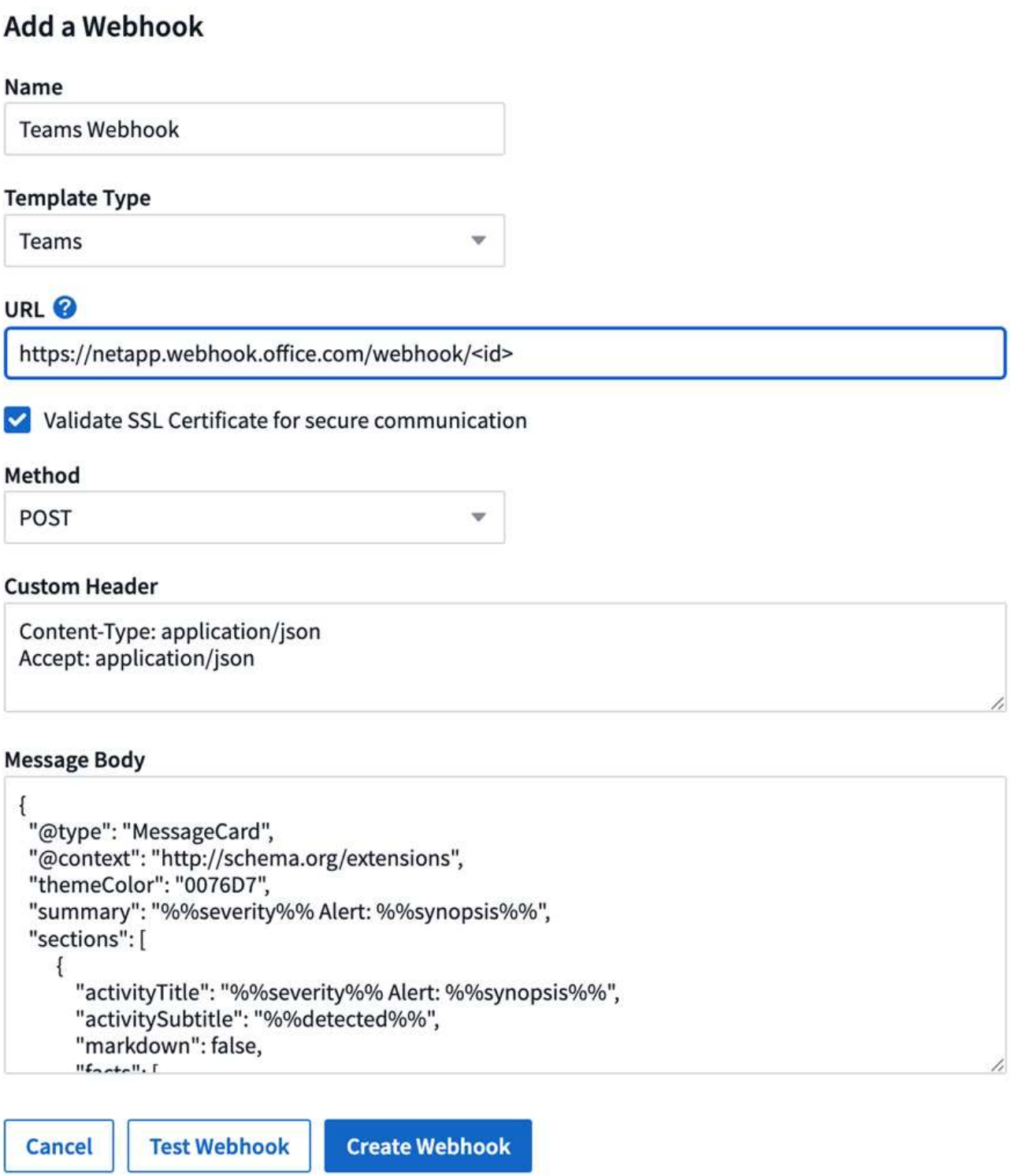
1. Dans Teams, sélectionnez le kebab et recherchez Webhook entrant.



2. Sélectionnez **Ajouter à une équipe > Sélectionner une équipe > Configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook pour les équipes de sécurité de la charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *« Webhooks de sécurité de la charge de travail »*. Sélectionnez _+ *Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Équipes**.



4. Collez l'URL ci-dessus dans le champ *URL*.

Notifications via Webhook

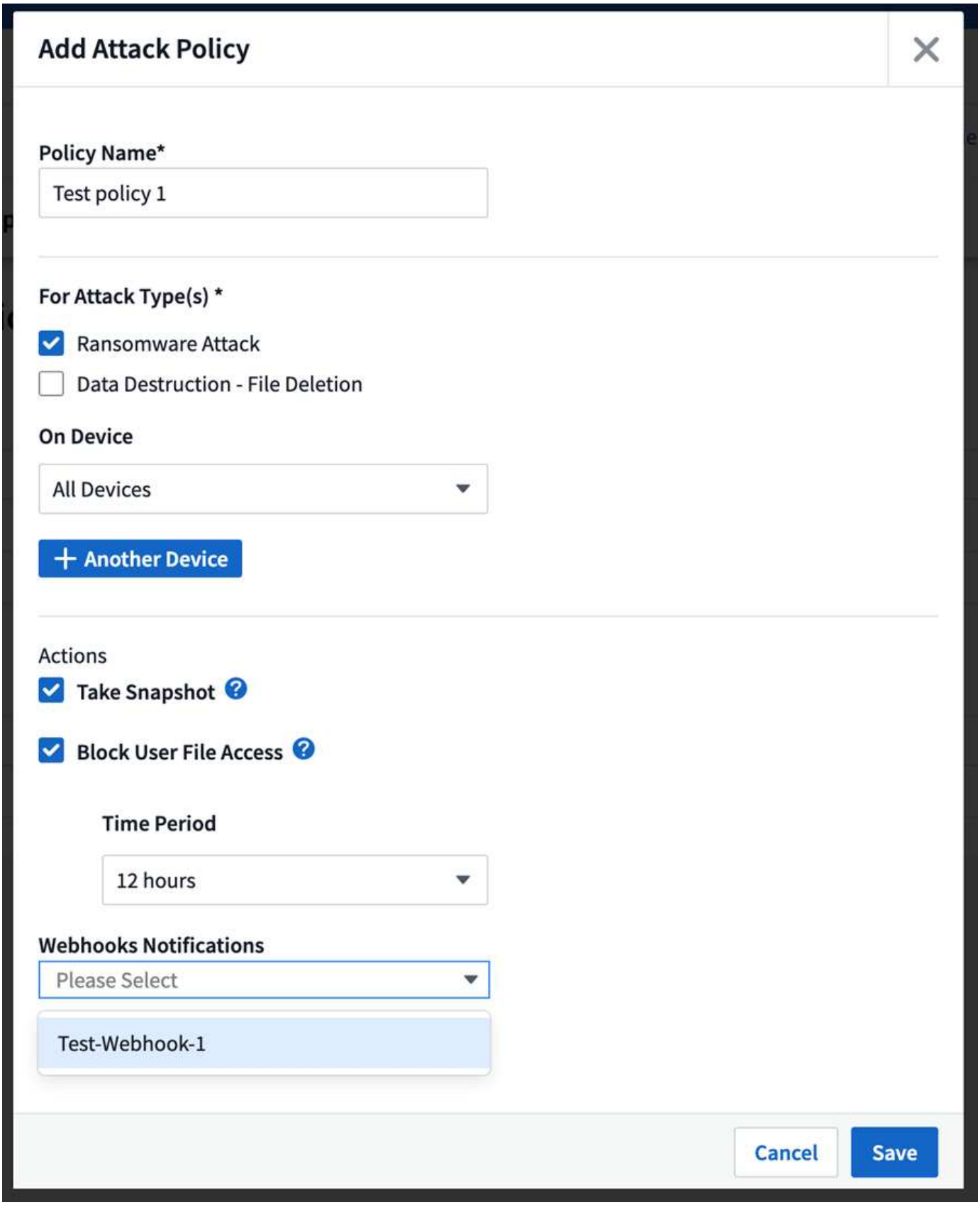
Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les

actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Teams requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.


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

Informations sur le copyright

Informations sur les marques commerciales