Notifiche webhook

Data Infrastructure Insights

NetApp
February 03, 2026

Sommario

Notifiche webhook

Notifiche di sicurezza del carico di lavoro tramite webhook

I webhook consentono agli utenti di inviare notifiche di avviso critiche o di avvertimento a varie applicazioni utilizzando un canale webhook personalizzato.

Molte applicazioni commerciali supportano i webhook come interfaccia di input standard, ad esempio: Slack, PagerDuty, Teams e Discord. Supportando un canale webhook generico e personalizzabile, Workload Security può supportare molti di questi canali di distribuzione. Le informazioni sulla configurazione dei webhook sono disponibili sui siti web delle rispettive applicazioni. Ad esempio, Slack fornisce"questa guida utile" .

È possibile creare più canali webhook, ognuno dei quali è destinato a uno scopo diverso, ad applicazioni separate, a destinatari diversi, ecc.

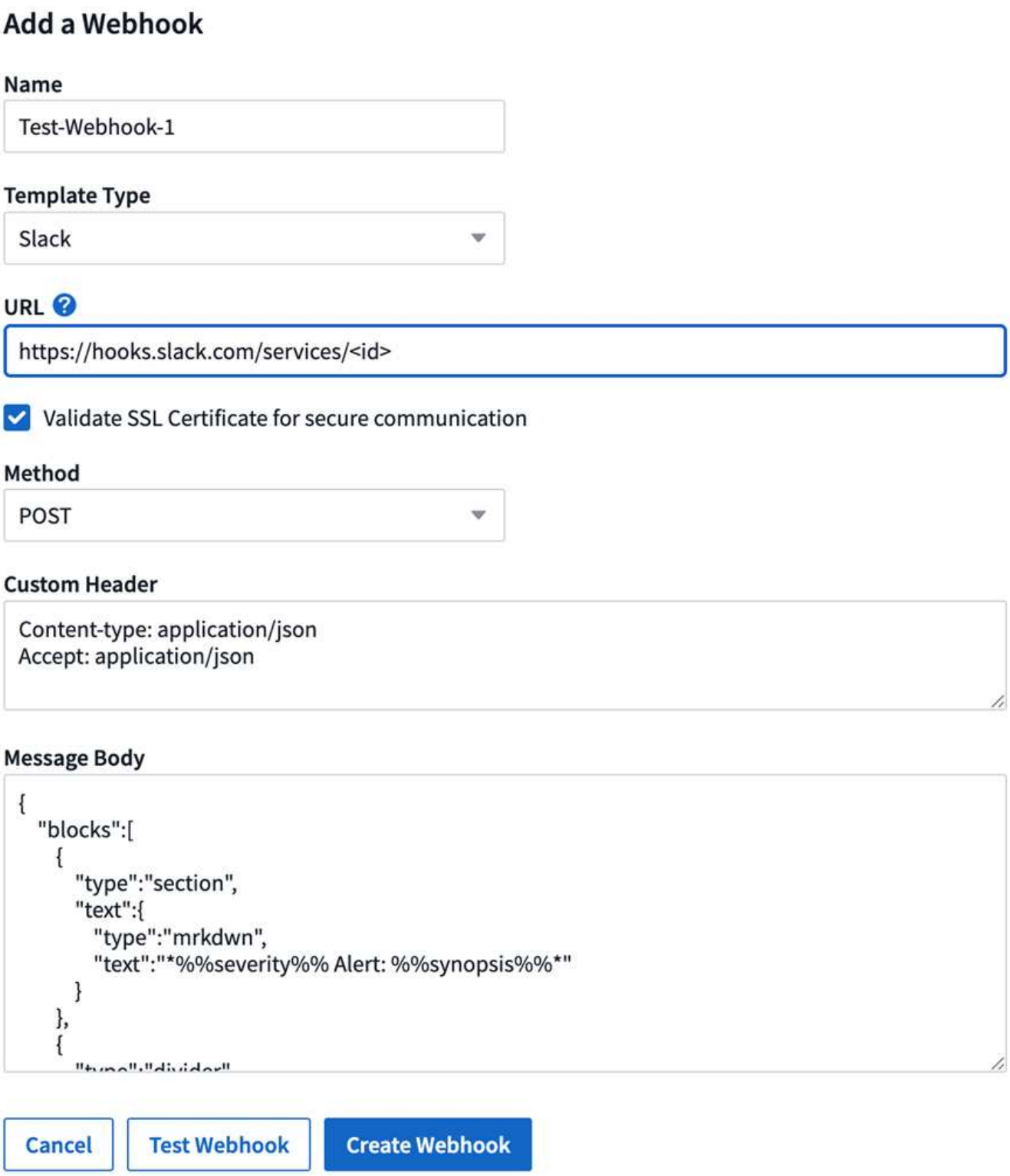
L'istanza del canale webhook è composta dai seguenti elementi

Nome	Descrizione
URL	URL di destinazione del webhook, incluso il prefisso http:// o https:// insieme ai parametri URL
Metodo	GET/POST - Il valore predefinito è POST
Intestazione personalizzata	Specifica qui eventuali intestazioni personalizzate
Corpo del messaggio	Inserisci qui il corpo del tuo messaggio
Parametri di avviso predefiniti	Elenca i parametri predefiniti per il webhook
Parametri e segreti personalizzati	I parametri e i segreti personalizzati consentono di aggiungere parametri univoci ed elementi sicuri come le password

Creazione di un webhook

Per creare un webhook di sicurezza del carico di lavoro, vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". L'immagine seguente mostra un esempio di schermata di creazione di un webhook Slack.

Nota: per creare e gestire i webhook di Workload Security, l'utente deve essere un amministratore di Workload Security.



- Inserisci le informazioni appropriate per ciascun campo e fai clic su "Salva".
- Puoi anche cliccare sul pulsante "Test Webhook" per testare la connessione. Si noti che in questo modo verrà inviato il "Corpo del messaggio" (senza sostituzioni) all'URL definito in base al metodo selezionato.
- I webhook SWS comprendono una serie di parametri predefiniti. Inoltre, puoi creare parametri o segreti personalizzati.

Parametri: cosa sono e come utilizzarli?

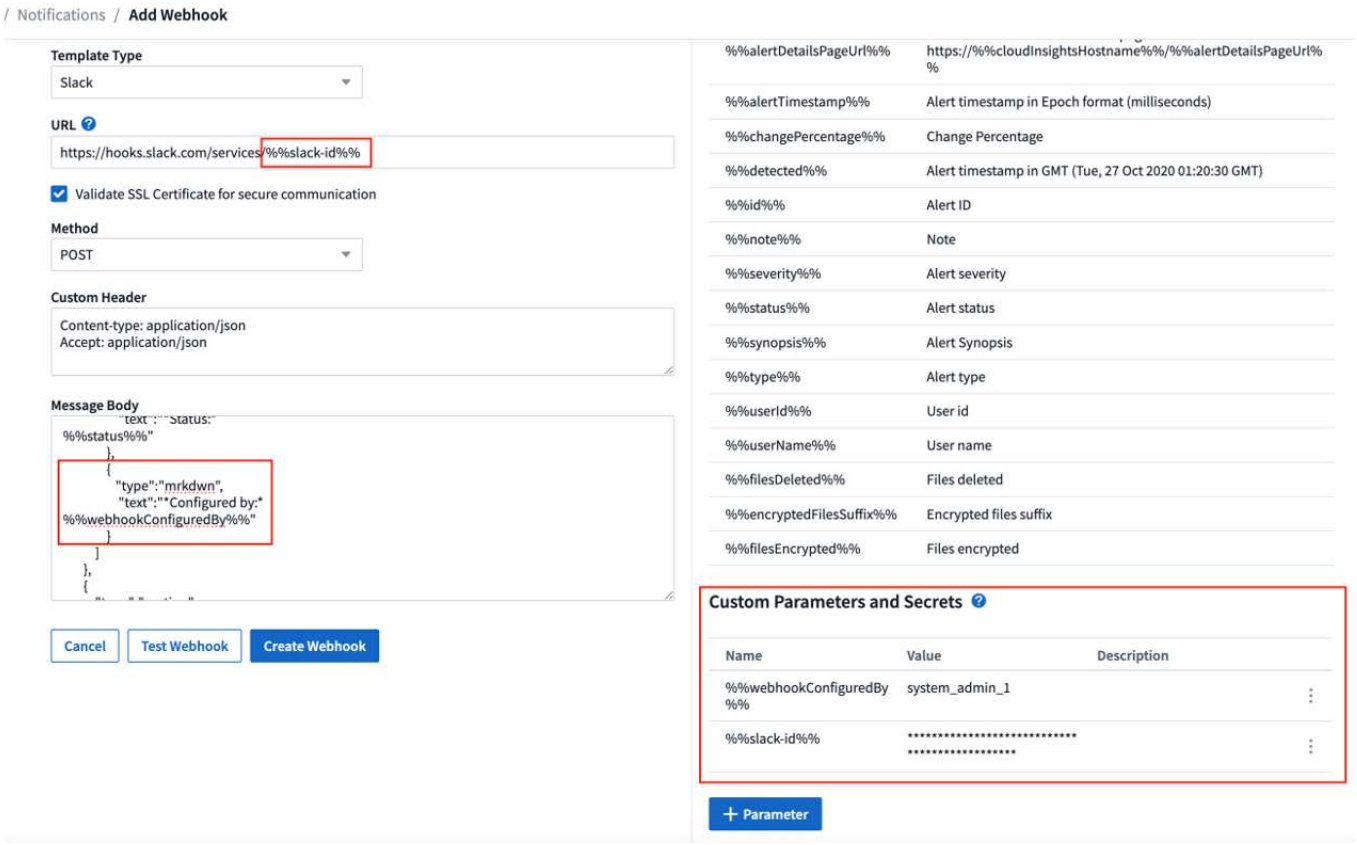
I parametri di avviso sono valori dinamici popolati per avviso. Ad esempio, il parametro *%%severity%%* verrà sostituito con il tipo di gravità dell'avviso.

Si noti che le sostituzioni non vengono eseguite quando si fa clic sul pulsante "Test Webhook"; il test invia un payload che mostra i segnaposto del parametro (*%%<param-name>%%*) ma non li sostituisce con i dati.

Parametri e segreti personalizzati

In questa sezione puoi aggiungere tutti i parametri personalizzati e/o segreti che desideri. Un parametro personalizzato o un segreto può essere presente nell'URL o nel corpo del messaggio. I segreti consentono all'utente di configurare un parametro personalizzato sicuro come password, apiKey ecc.

L'immagine di esempio seguente mostra come vengono utilizzati i parametri personalizzati nella creazione di webhook.



Pagina elenco webhook sicurezza carico di lavoro

Nella pagina dell'elenco dei webhook vengono visualizzati i campi Nome, Creato da, Creato il, Stato, Sicuro e Ultimo segnalato. Nota: il valore della colonna "stato" continuerà a cambiare in base al risultato dell'ultimo trigger del webhook. Di seguito sono riportati alcuni esempi di risultati di stato.

Stato	Descrizione
OK	Notifica inviata correttamente.
403	Vietato.

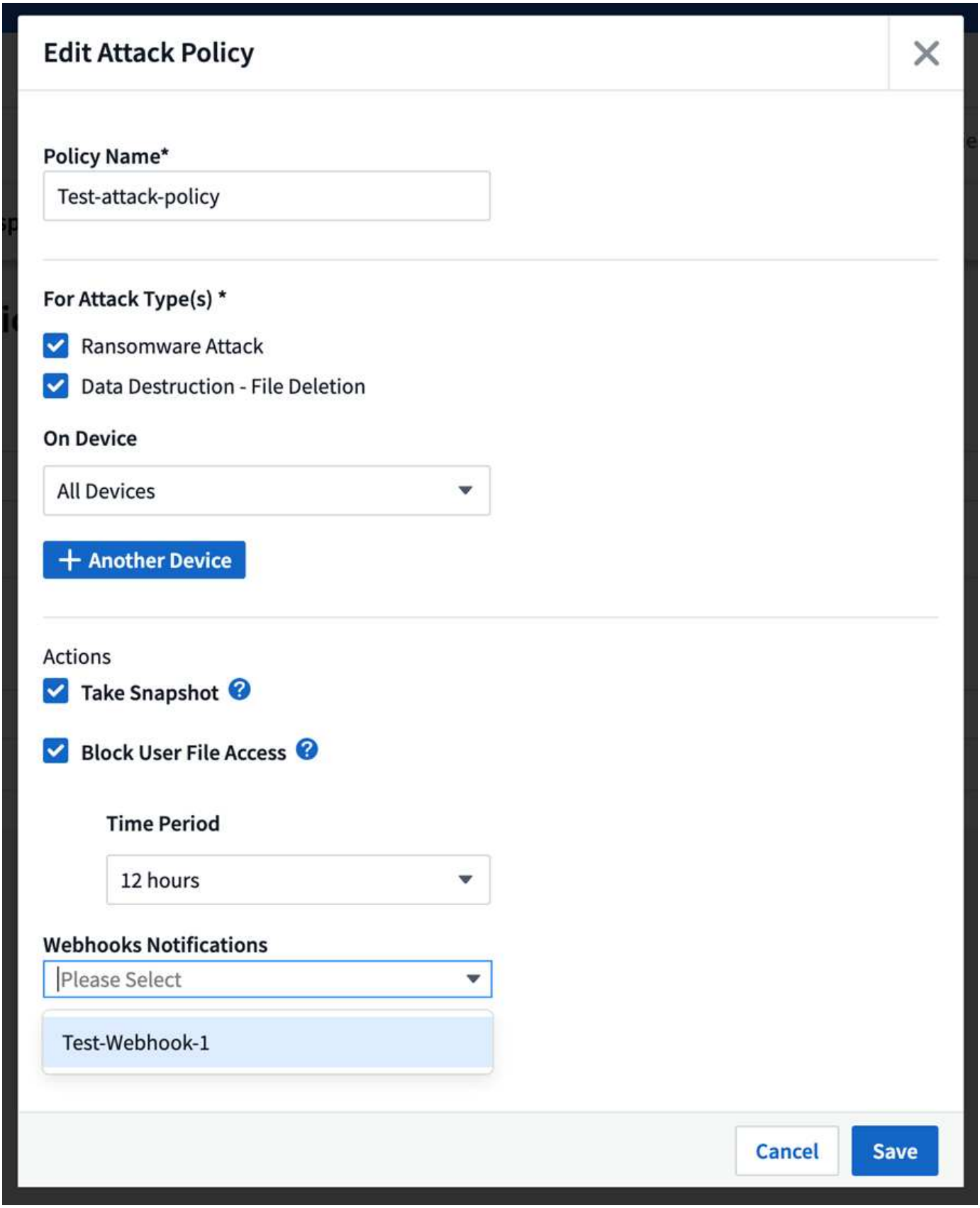
404	URL non trovato.
400	Brutta richiesta. Potresti visualizzare questo stato se c'è un errore nel corpo del messaggio, ad esempio: • JSON formattato male. • Fornito valore non valido per le chiavi riservate. Ad esempio, PagerDuty accetta solo informazioni critiche/avviso/errore/informazioni per "Gravità". Qualsiasi altro risultato potrebbe comportare lo stato 400. • Errori di convalida specifici dell'applicazione. Ad esempio, Slack consente un massimo di 10 campi all'interno di una sezione. Includerne più di 10 può comportare lo stato 400.
410	La risorsa non è più disponibile

La colonna "Ultimo segnalato" indica l'ora in cui il webhook è stato attivato l'ultima volta.

Dalla pagina dell'elenco dei webhook gli utenti possono anche modificare/duplicare/eliminare i webhook.

Configurare la notifica Webhook nel criterio di avviso

Per aggiungere una notifica webhook a un criterio di avviso, vai su -Sicurezza del carico di lavoro > Criteri- e seleziona un criterio esistente o aggiungine uno nuovo. Nella sezione *Azioni* > menu a discesa *Notifiche webhook*, seleziona i webhook richiesti.



Le notifiche webhook sono collegate alle policy. Quando si verifica l'attacco (RW/DD/WARN), verrà eseguita l'azione configurata (Scatta snapshot/blocco utente) e verrà quindi attivata la notifica webhook associata.

Nota: le notifiche e-mail sono indipendenti dalle policy e verranno attivate come di consueto.

- Se una policy viene sospesa, le notifiche webhook non verranno attivate.
- È possibile associare più webhook a una singola policy, ma si consiglia di non associarne più di 5.

Esempi di webhook sulla sicurezza del carico di lavoro

Webhook per"Slack"

Webhook per"PagerDuty" Webhook per"Squadre" Webhook per"Discordia"

Esempio di webhook di sicurezza del carico di lavoro per Discord

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Discord.

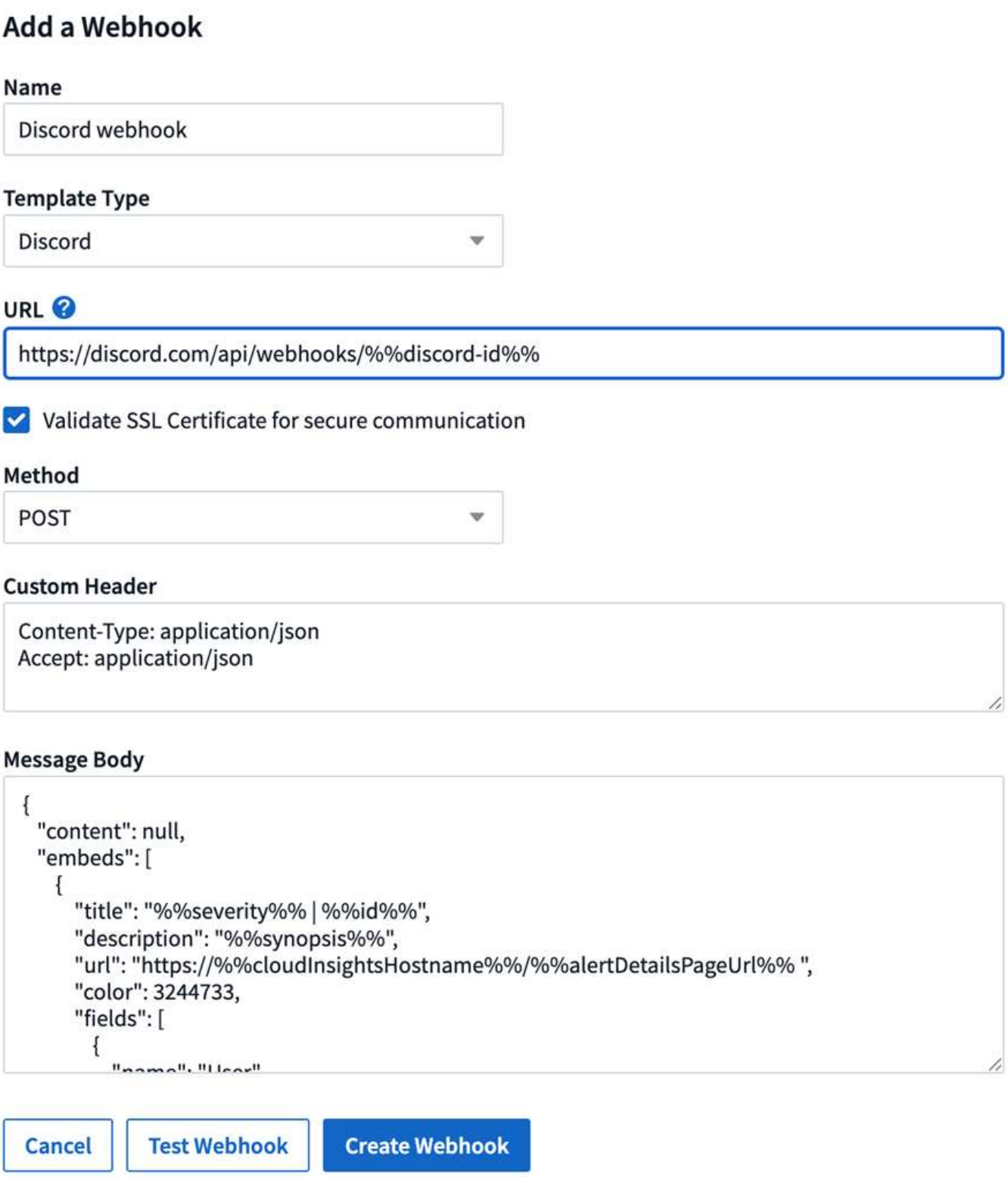
Questa pagina fa riferimento a istruzioni di terze parti, che sono soggette a modifiche. Fare riferimento al"Documentazione Discord" per le informazioni più aggiornate.

Configurazione Discord:

- In Discord, seleziona il server, in Canali di testo, seleziona Modifica canale (icona a forma di ingranaggio)
- Seleziona **Integrazioni > Visualizza webhook** e fai clic su **Nuovo webhook**
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook sulla sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Fare clic su '+ Webhook' per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Discord**.
4. Incolla l'URL di Discord riportato sopra nel campo *URL*.



Per testare il webhook, sostituisci temporaneamente il valore URL nel corpo del messaggio con un URL valido (ad esempio *https://netapp.com*), quindi fai clic sul pulsante *Test Webhook*. Per far funzionare la funzionalità Test Webhook, Discord richiede che venga fornito un URL valido.

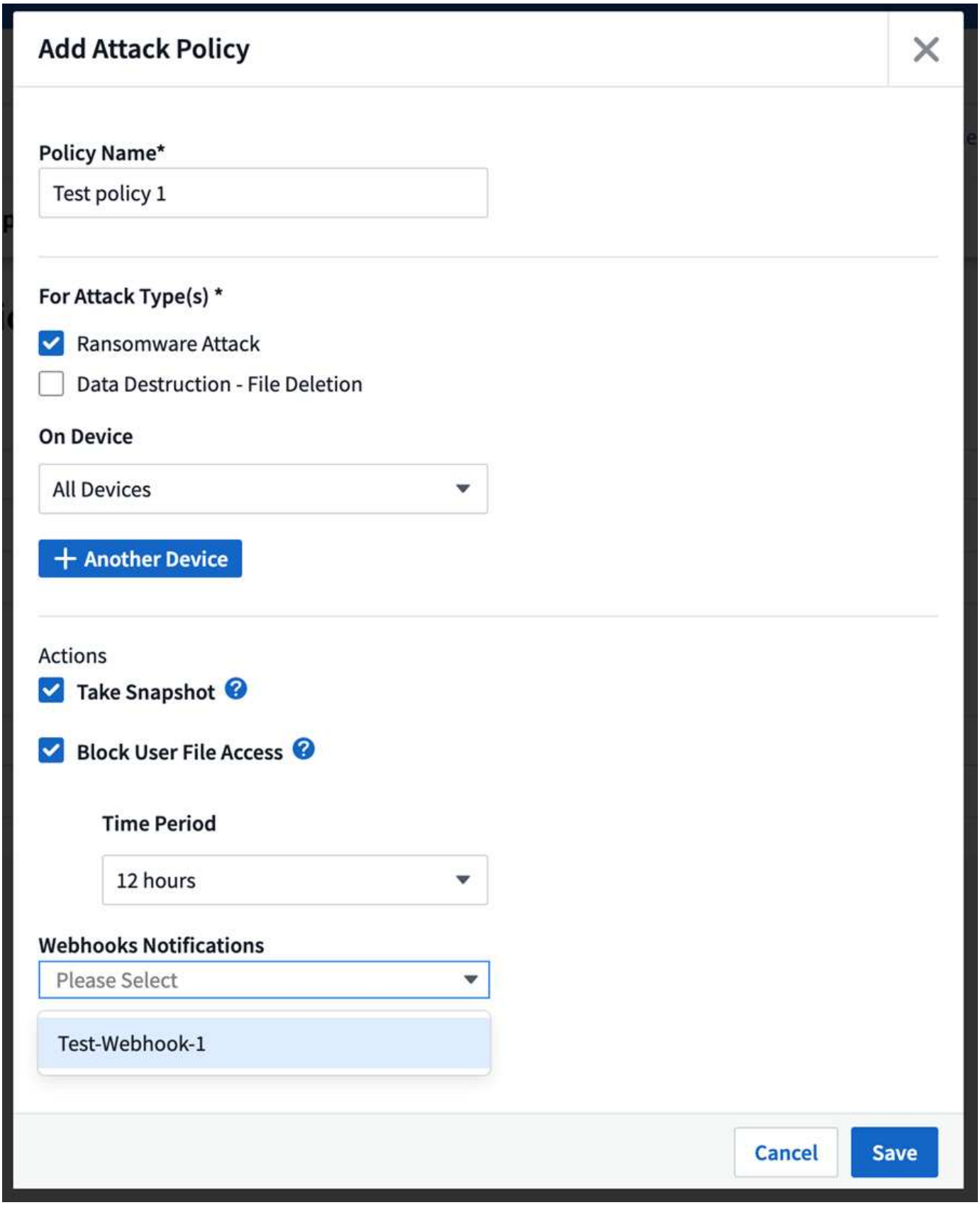
Una volta completato il test, assicurati di reimpostare il corpo del messaggio.

Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui associare la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook Discord desiderati e salva.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.


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

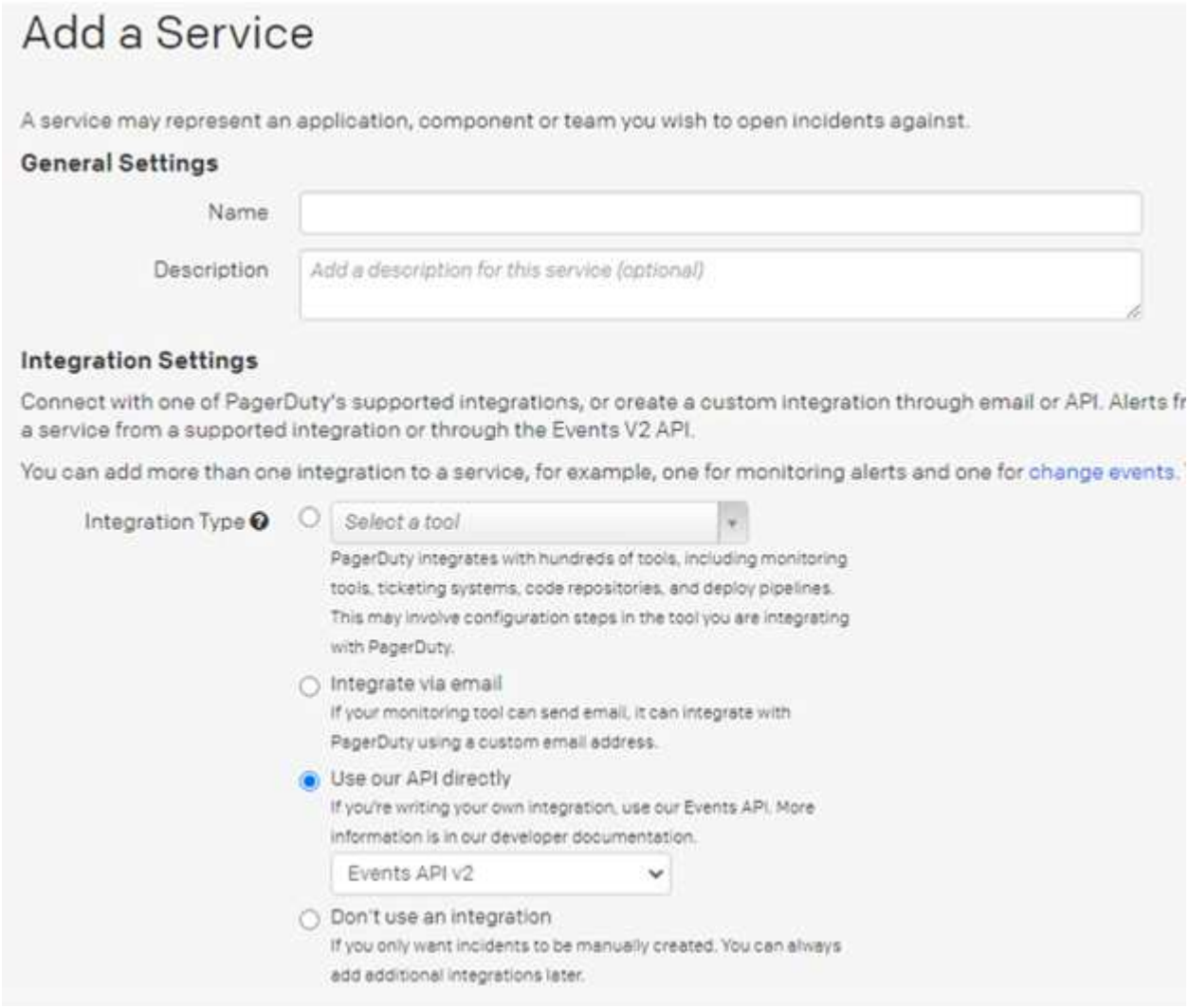
Esempio di webhook di sicurezza del carico di lavoro per PagerDuty

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per PagerDuty.

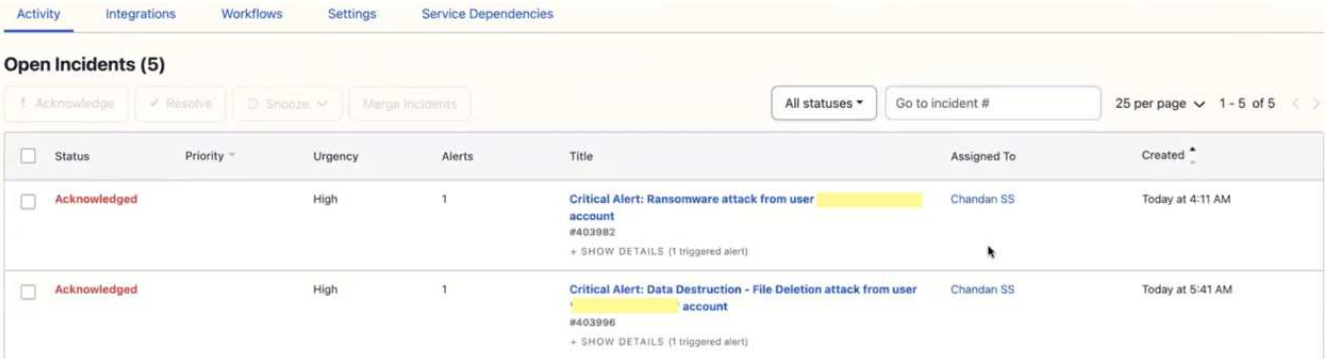
Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento al"Documentazione PagerDuty" per le informazioni più aggiornate.

Configurazione PagerDuty:

1. In PagerDuty, vai su **Servizi > Directory dei servizi** e clicca sul pulsante **+Nuovo servizio**.
2. Inserisci un *Nome* e seleziona *Usa direttamente la nostra API*. Selezionare *Aggiungi servizio*.

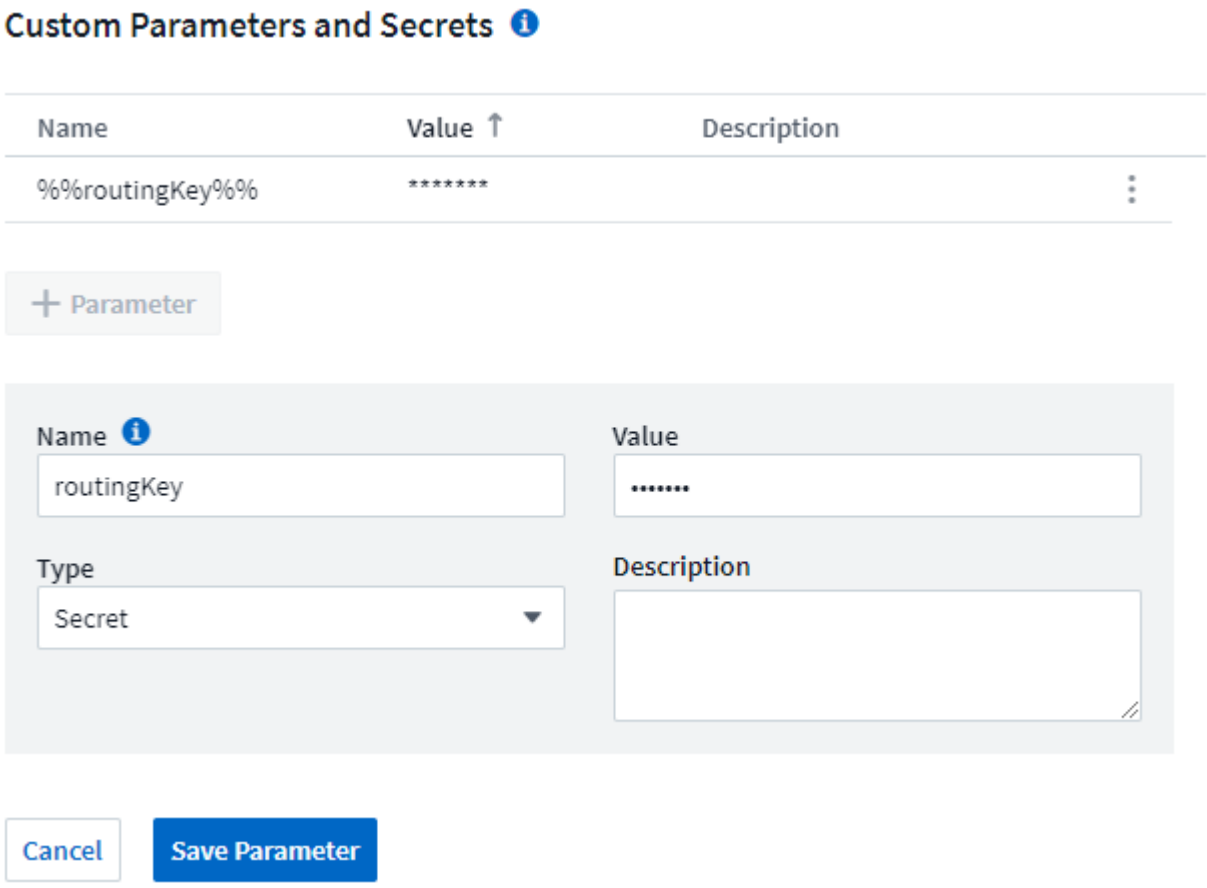


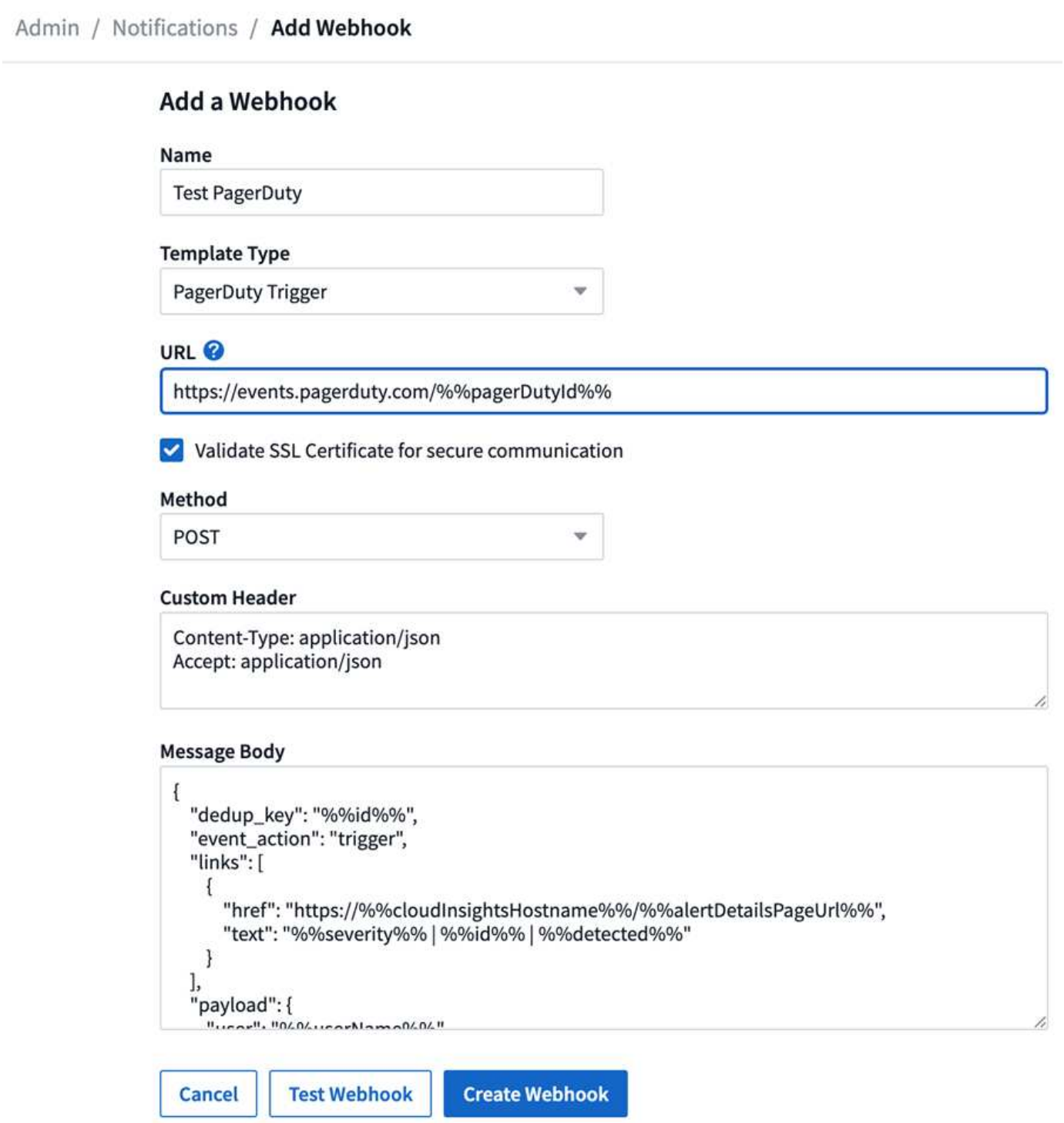
3. Selezionare la scheda *Integrazioni* per visualizzare la **Chiave di integrazione**. Questa chiave ti servirà quando creerai il webhook Workload Security qui sotto.
4. Vai a **Incidenti** o **Servizi** per visualizzare gli avvisi.



Crea webhook Workload Security PagerDuty:

- Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare '+ Webhook' per creare un nuovo webhook.
- Assegnare al webhook un nome significativo.
- Nel menu a discesa *Tipo di modello*, seleziona *Trigger PagerDuty*.
- Crea un parametro segreto personalizzato denominato *routingKey* e imposta il valore sulla *Chiave di integrazione* PagerDuty creata in precedenza.

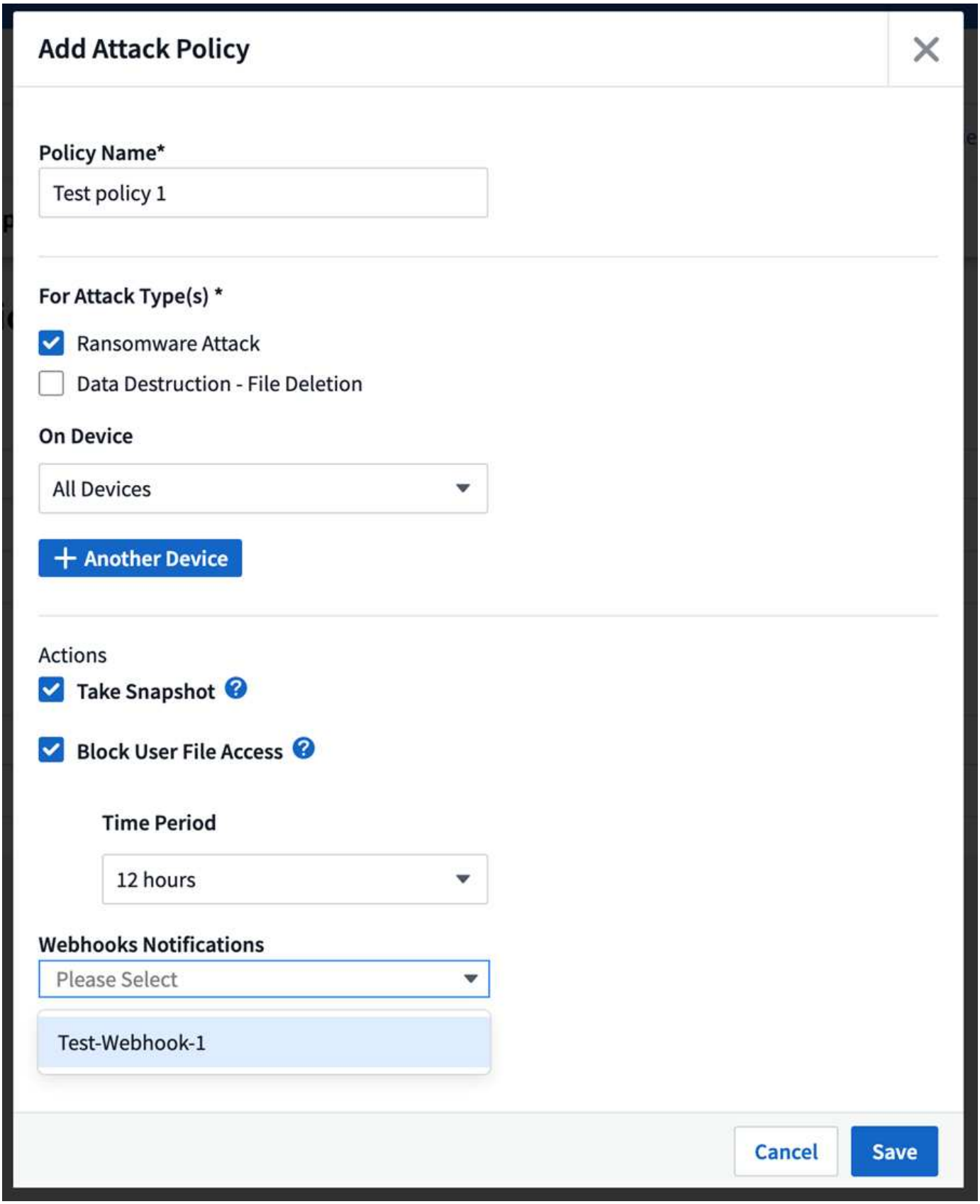




Notifiche tramite Webhook

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro > Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook PagerDuty desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.


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

Esempio di webhook di sicurezza del carico di lavoro per Slack

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Slack.

Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Per informazioni più aggiornate, consultare la documentazione di Slack.

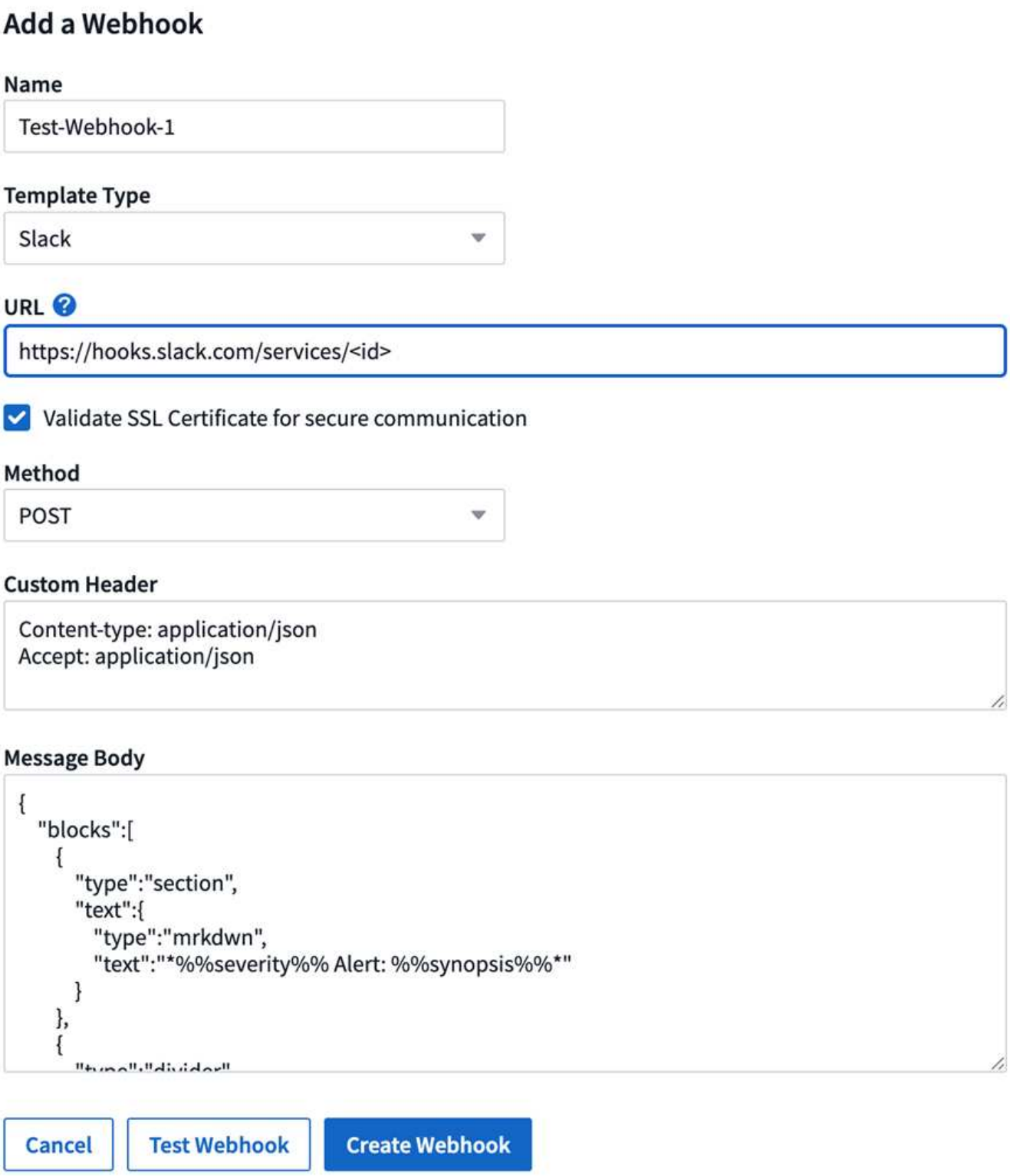
Esempio di Slack

- Vai a https://api.slack.com/apps e crea una nuova app. Assegnagli un nome significativo e seleziona un'area di lavoro.

- Vai a Webhook in arrivo, clicca su *Attiva webhook in arrivo*, seleziona *Aggiungi nuovo webhook* e seleziona il canale su cui pubblicare.
- Copia l'URL del webhook. Questo URL verrà fornito durante la creazione di un webhook di Workload Security.

Crea un webhook Slack per la sicurezza del carico di lavoro

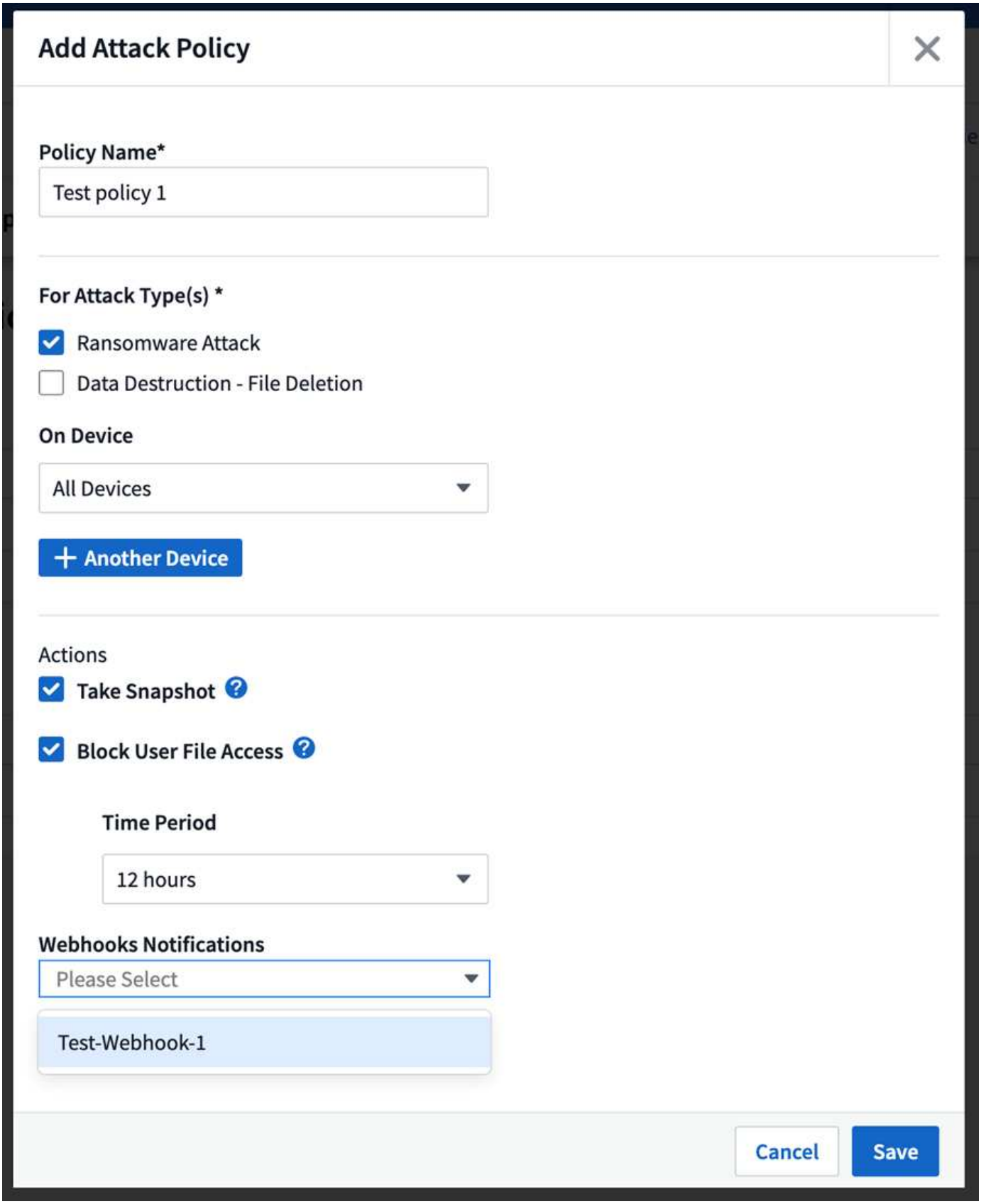
1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona *Slack*.
4. Incolla l'URL copiato sopra.



Notifiche tramite webhook

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



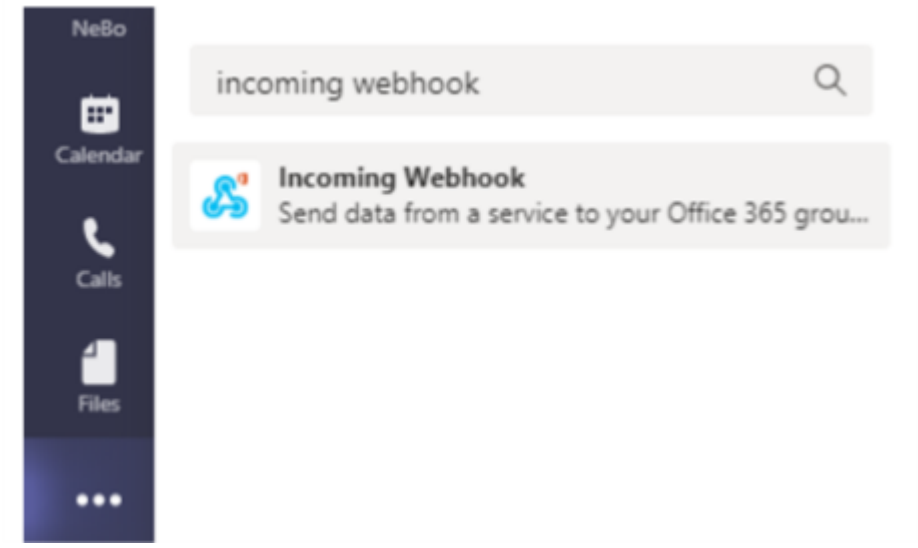
Esempio di webhook di sicurezza del carico di lavoro per Microsoft Teams

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per la configurazione di webhook per Teams.

Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento al"Documentazione dei team" per le informazioni più aggiornate.

Configurazione delle squadre:

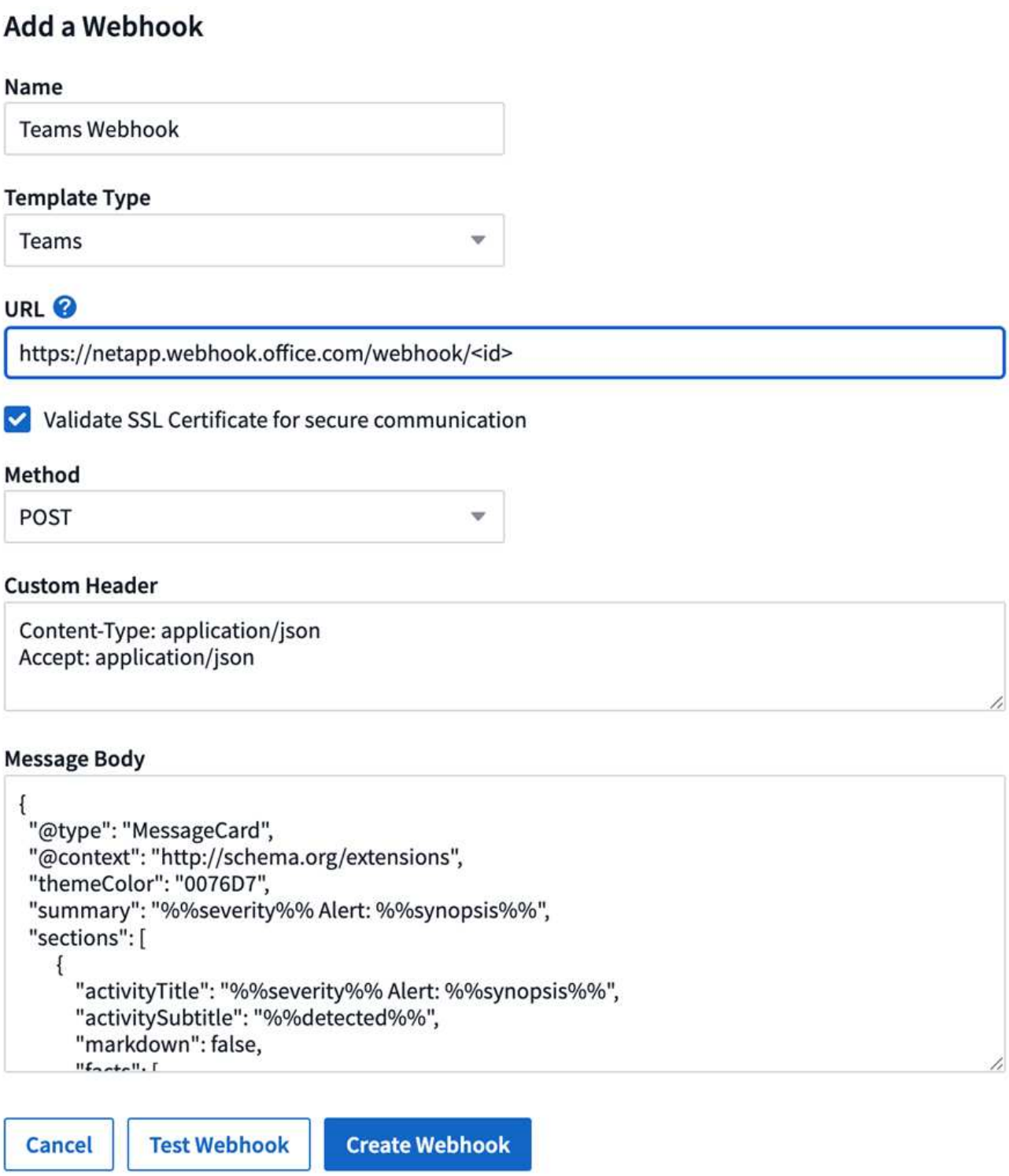
1. In Teams, seleziona il kebab e cerca Webhook in arrivo.



2. Seleziona **Aggiungi a un team > Seleziona un team > Imposta un connettore**.
3. Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook per i team di sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Team**.



4. Incolla l'URL sopra nel campo *URL*.

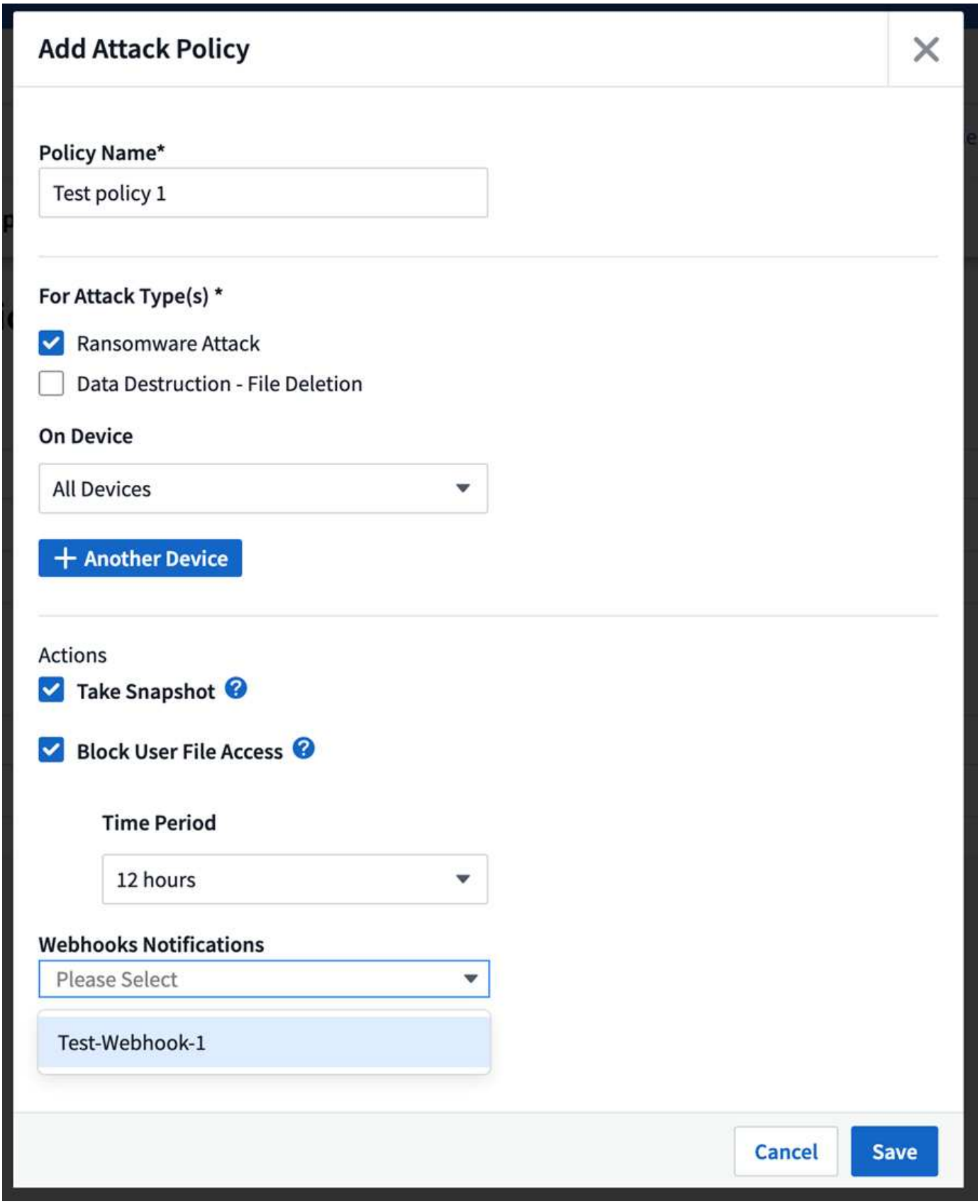
Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.

- Nel menu a discesa *Notifiche webhook*, seleziona i webhook di Teams desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



Informazioni sul copyright

Informazioni sul marchio commerciale