Notificaciones de webhook

Data Infrastructure Insights

NetApp
February 11, 2026

Tabla de contenidos

Notificaciones de webhook

Notificaciones de seguridad de la carga de trabajo mediante webhooks

Los webhooks permiten a los usuarios enviar notificaciones de alerta críticas o de advertencia a varias aplicaciones utilizando un canal webhook personalizado.

Muchas aplicaciones comerciales admiten webhooks como interfaz de entrada estándar, por ejemplo: Slack, PagerDuty, Teams y Discord. Al admitir un canal webhook genérico y personalizable, Workload Security puede admitir muchos de estos canales de entrega. Puede encontrar información sobre la configuración de los webhooks en los sitios web de las respectivas aplicaciones. Por ejemplo, Slack ofrece"Esta útil guía" .

Puede crear múltiples canales webhook, cada uno destinado a un propósito diferente, aplicaciones independientes, diferentes destinatarios, etc.

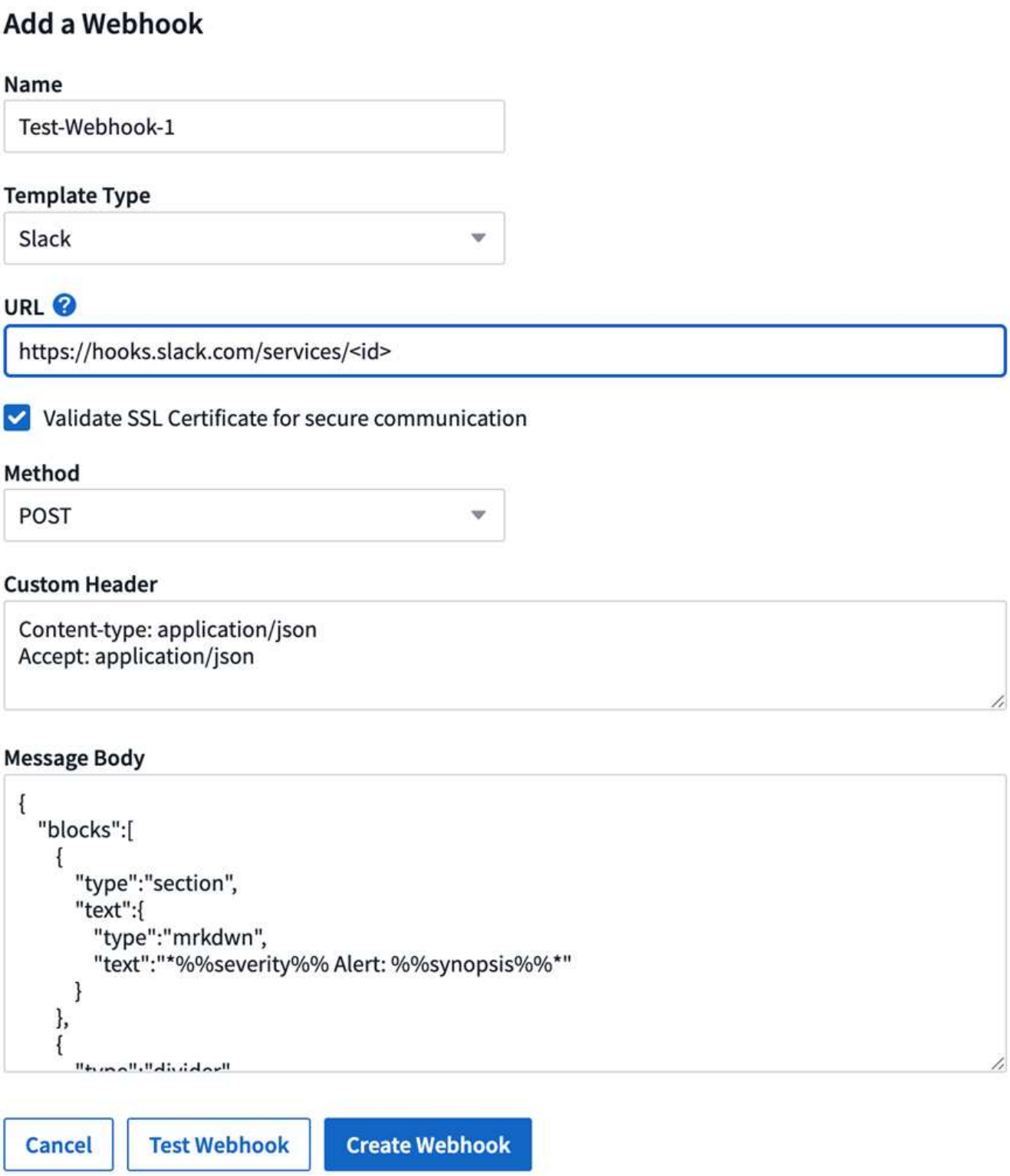
La instancia del canal webhook se compone de los siguientes elementos

Nombre	Descripción
URL	URL de destino del webhook, incluido el prefijo http:// o https:// junto con los parámetros de la URL
Método	GET/POST - El valor predeterminado es POST
Encabezado personalizado	Especifique aquí cualquier encabezado personalizado
Cuerpo del mensaje	Coloque el cuerpo de su mensaje aquí
Parámetros de alerta predeterminados	Enumera los parámetros predeterminados para el webhook
Parámetros y secretos personalizados	Los parámetros y secretos personalizados le permiten agregar parámetros únicos y elementos seguros como contraseñas.

Creando un webhook

Para crear un webhook de seguridad de carga de trabajo, vaya a Admin > Notificaciones y seleccione la pestaña “Webhooks de seguridad de carga de trabajo”. La siguiente imagen muestra un ejemplo de pantalla de creación de webhook de Slack.

Nota: El usuario debe ser un *Admin* de seguridad de carga de trabajo para poder crear y administrar webhooks de seguridad de carga de trabajo.



- Ingrese la información adecuada para cada uno de los campos y haga clic en "Guardar".
- También puede hacer clic en el botón "Probar webhook" para probar la conexión. Tenga en cuenta que esto enviará el "Cuerpo del mensaje" (sin sustituciones) a la URL definida según el método seleccionado.
- Los webhooks de SWS comprenden una serie de parámetros predeterminados. Además, puedes crear tus propios parámetros o secretos personalizados.

Parámetros: ¿Qué son y cómo utilizarlos?

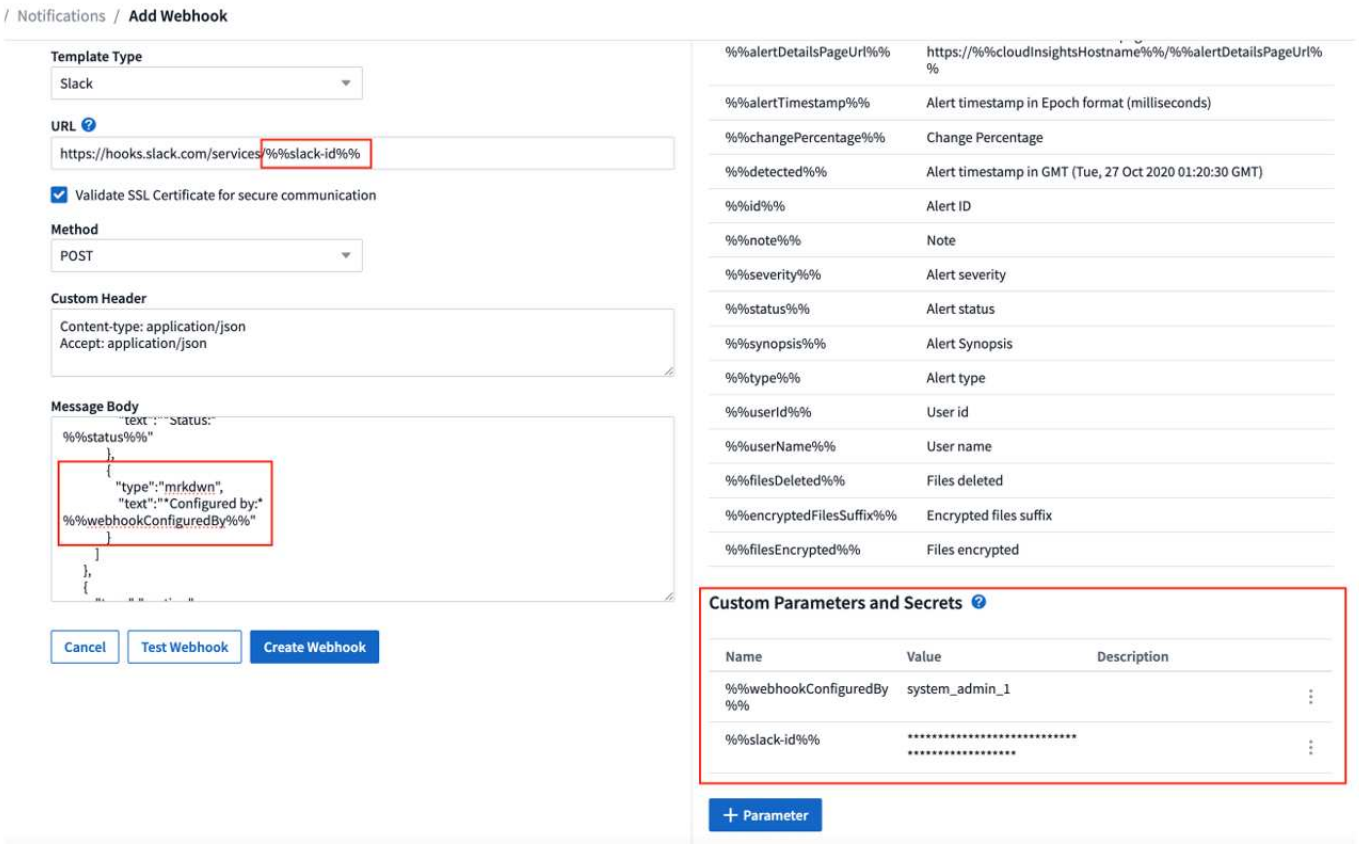
Los parámetros de alerta son valores dinámicos que se completan por cada alerta. Por ejemplo, el parámetro *%%severity%%* se reemplazará con el tipo de gravedad de la alerta.

Tenga en cuenta que no se realizan sustituciones al hacer clic en el botón "Probar webhook"; la prueba envía una carga útil que muestra los marcadores de posición del parámetro (*%%<param-name>%%*) pero no los reemplaza con datos.

Parámetros y secretos personalizados

En esta sección puedes agregar cualquier parámetro personalizado y/o secretos que desees. Un parámetro personalizado o secreto puede estar en la URL o en el cuerpo del mensaje. Los secretos permiten al usuario configurar un parámetro personalizado seguro como contraseña, apiKey, etc.

La siguiente imagen de muestra muestra cómo se utilizan los parámetros personalizados en la creación de webhooks.



Página de lista de webhooks de seguridad de carga de trabajo

En la página de lista de Webhooks, se muestran los campos Nombre, Creado por, Creado el, Estado, Seguro y Último informe. Nota: El valor de la columna 'estado' seguirá cambiando según el resultado del último activador del webhook. Los siguientes son ejemplos de resultados de estado.

Estado	Descripción
DE ACUERDO	Notificación enviada exitosamente.
403	Prohibido.

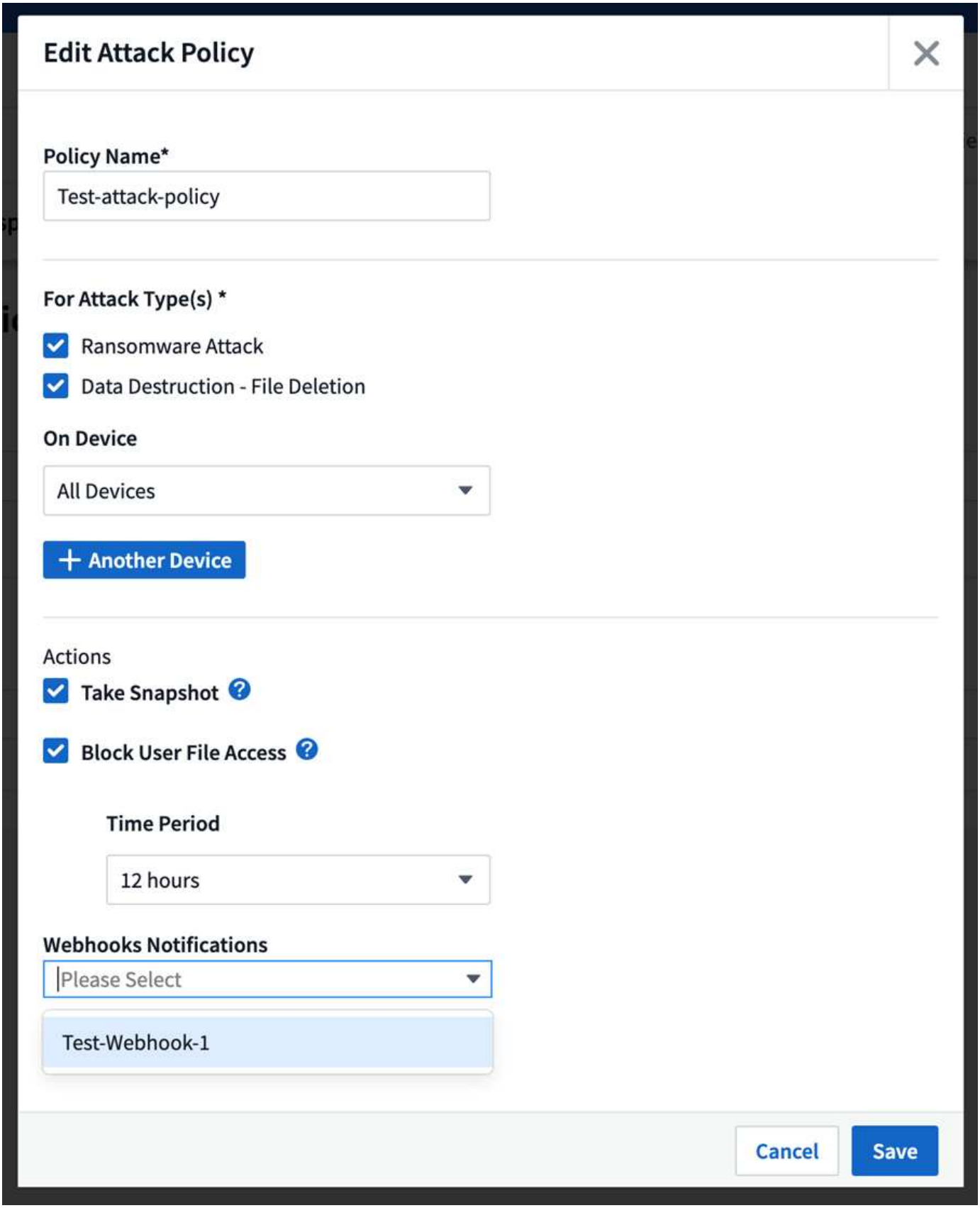
404	URL no encontrada.
400	Solicitud incorrecta. Es posible que vea este estado si hay algún error en el cuerpo del mensaje, por ejemplo: • Json mal formateado. • Proporcionar valor no válido para claves reservadas. Por ejemplo, PagerDuty solo acepta información/advertencia/error/crítico para “Gravedad”. Cualquier otro resultado puede producir un estado 400. • Errores de validación específicos de la aplicación. Por ejemplo, Slack permite un máximo de 10 campos dentro de una sección. Incluir más de 10 puede dar como resultado un estado 400.
410	El recurso ya no está disponible

La columna “Último informe” indica el momento en que se activó el webhook por última vez.

Desde la página de listado de webhooks, los usuarios también pueden editar, duplicar y eliminar webhooks.

Configurar la notificación de webhook en la política de alertas

Para agregar una notificación de webhook a una política de alerta, vaya a -Seguridad de carga de trabajo > Políticas- y seleccione una política existente o agregue una nueva. En la sección *Acciones* > menú desplegable *Notificaciones de webhook*, seleccione los webhooks necesarios.



Las notificaciones de webhook están vinculadas a las políticas. Cuando ocurre el ataque (RW/DD/WARN), se tomará la acción configurada (Tomar instantánea/bloqueo de usuario) y luego se activará la notificación de webhook asociada.

Nota: Las notificaciones por correo electrónico son independientes de las políticas y se activarán como de costumbre.

- Si se pausa una política, no se activarán las notificaciones de webhook.
- Se pueden adjuntar varios webhooks a una sola política, pero se recomienda no adjuntar más de 5 webhooks a una política.

Ejemplos de webhooks de seguridad de carga de trabajo

Webhooks para"Flojo"

Webhooks para"PagerDuty" Webhooks para"Equipos" Webhooks para"Discordia"

Ejemplo de webhook de seguridad de carga de trabajo para Discord

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Discord.

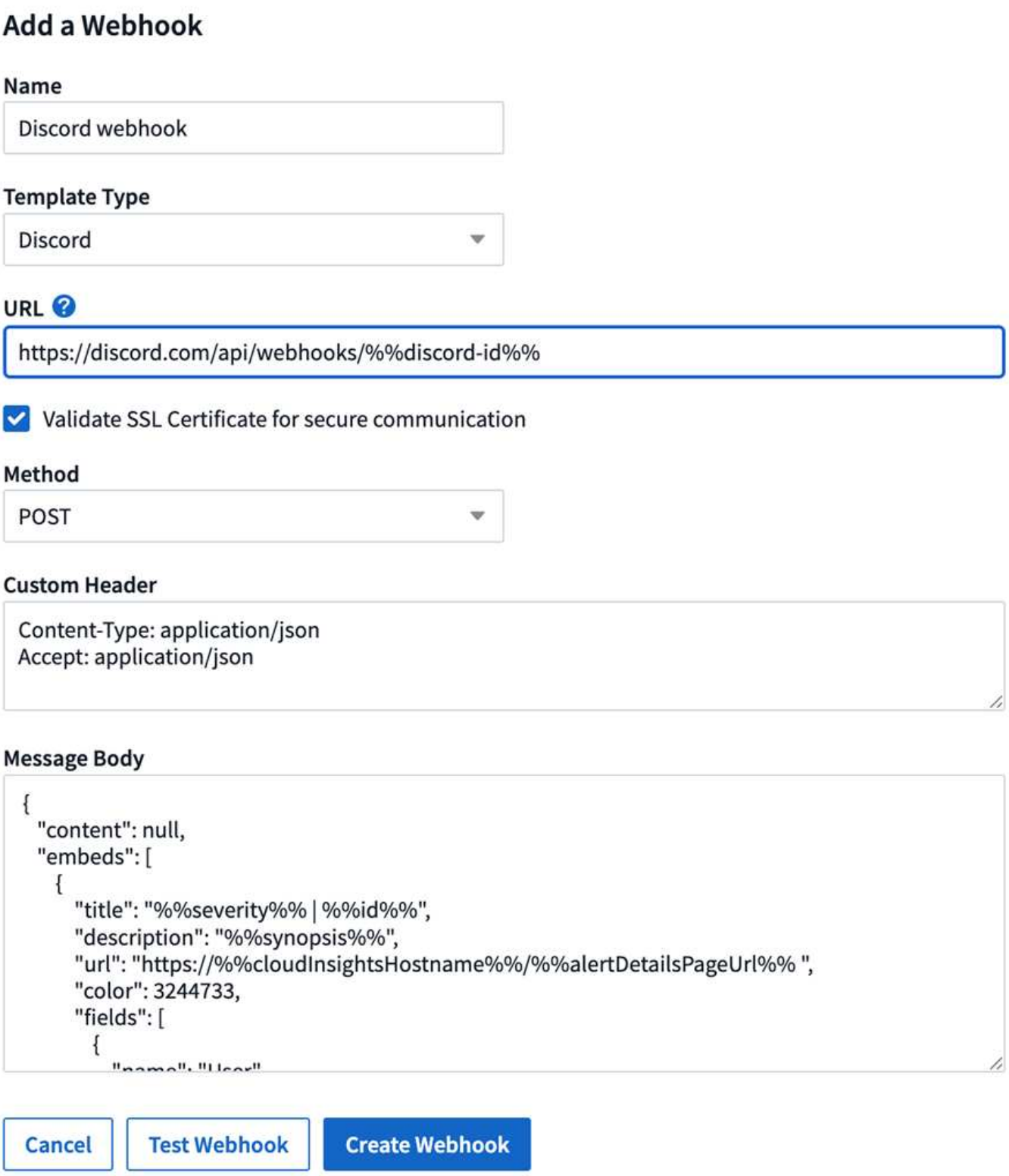
Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la"Documentación de Discord" para obtener la información más actualizada.

Configuración de Discord:

- En Discord, selecciona el Servidor, en Canales de texto, selecciona Editar canal (ícono de engranaje)
- Seleccione **Integraciones > Ver webhooks** y haga clic en **Nuevo webhook**
- Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de seguridad de carga de trabajo.

Crear un webhook de seguridad de carga de trabajo:

1. Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Haga clic en “+ Webhook” para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione **Discord**.
4. Pegue la URL de Discord de arriba en el campo *URL*.



Para probar el webhook, reemplace temporalmente el valor de la URL en el cuerpo del mensaje con cualquier URL válida (como *https://netapp.com*) y luego haga clic en el botón *Probar webhook*. Discord requiere que se proporcione una URL válida para que la funcionalidad de prueba webhook funcione.

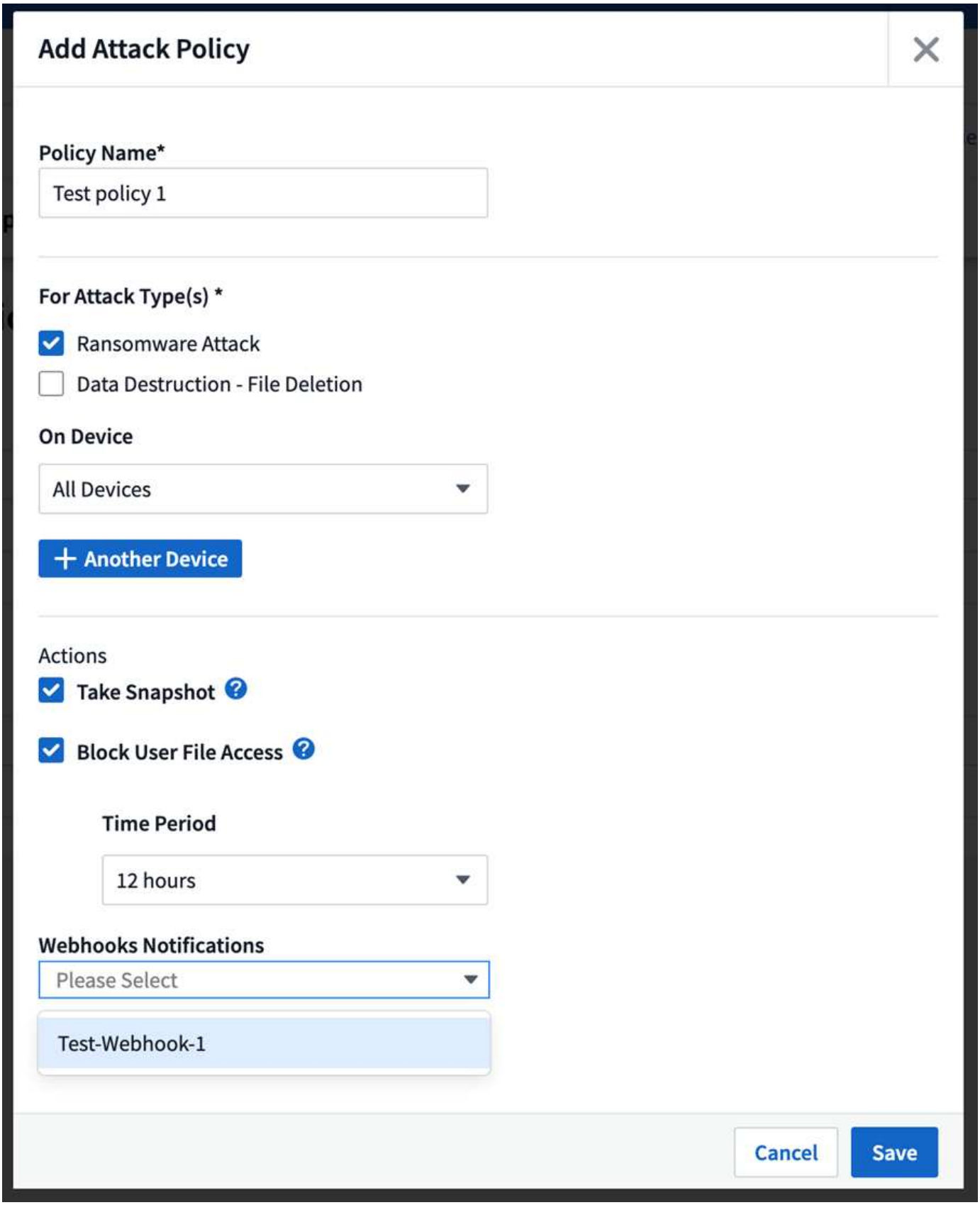
Asegúrese de volver a configurar el cuerpo del mensaje una vez que se complete la prueba.

Notificaciones mediante webhook

Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo* > *Políticas*. Haga clic en *+Política de ataque* o *+Política de advertencia*.

- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de Discord necesarios y guárdelos.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.


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

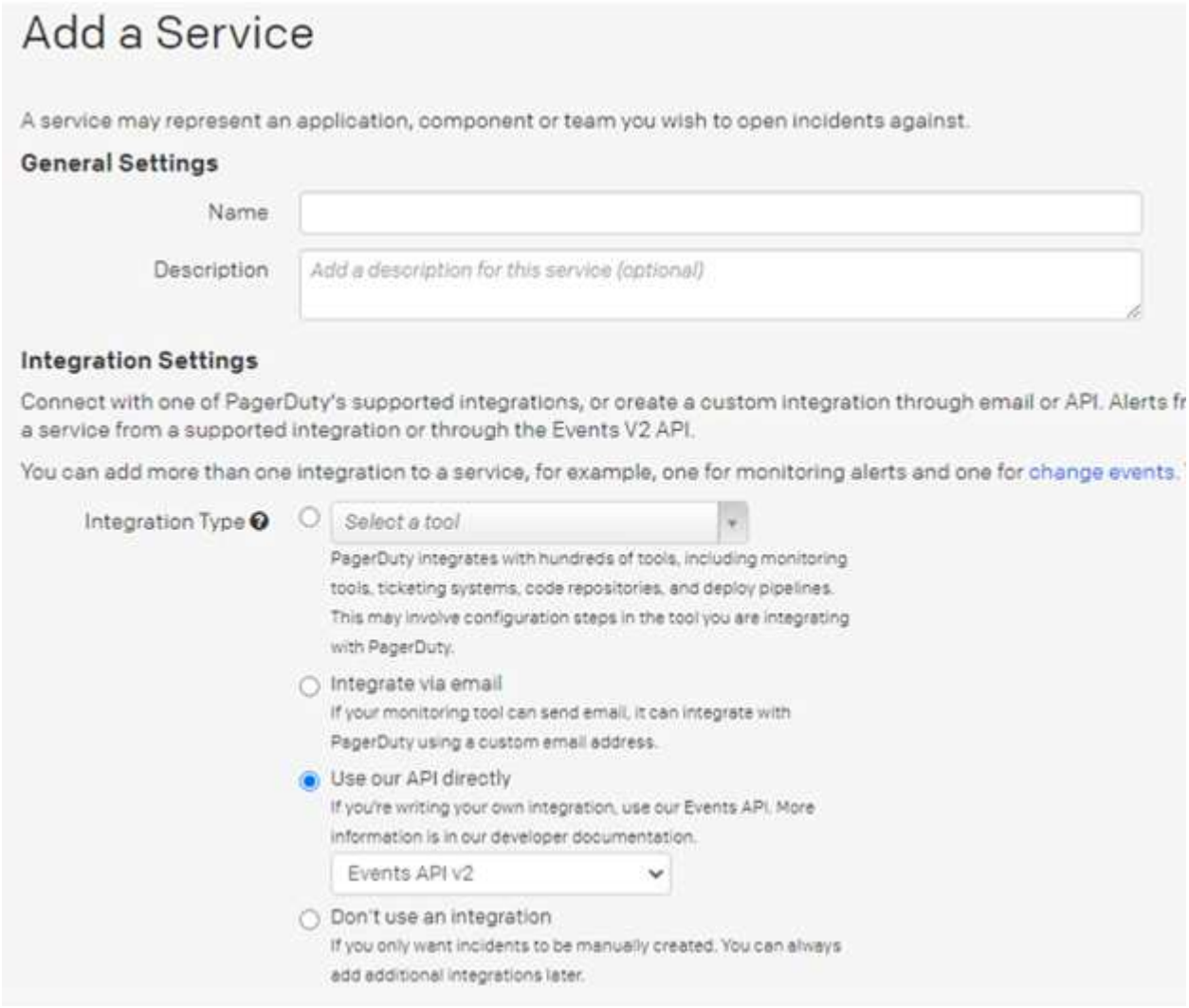
Ejemplo de webhook de seguridad de carga de trabajo para PagerDuty

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para PagerDuty.

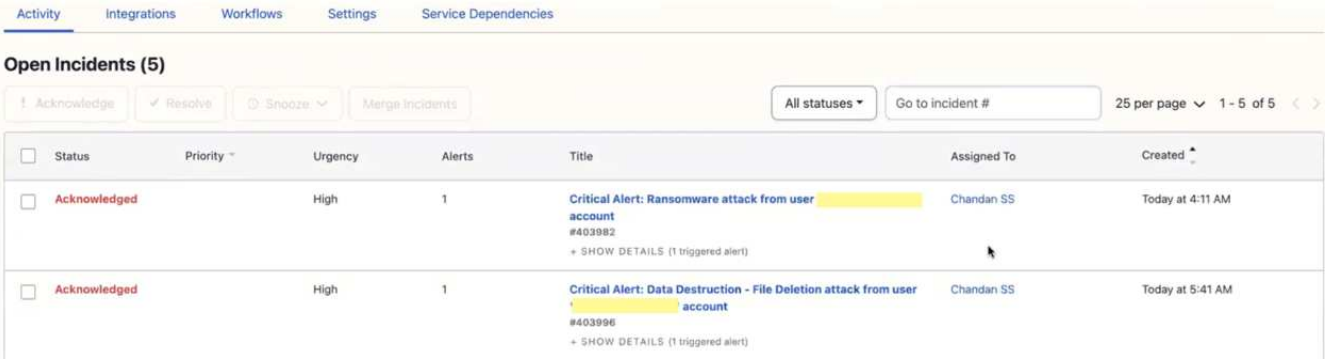
Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la"Documentación de PagerDuty" para obtener la información más actualizada.

Configuración de PagerDuty:

1. En PagerDuty, navegue a **Servicios > Directorio de servicios** y haga clic en el botón **+Nuevo servicio**.
2. Ingrese un *Nombre* y seleccione *Usar nuestra API directamente*. Seleccione *Agregar servicio*.

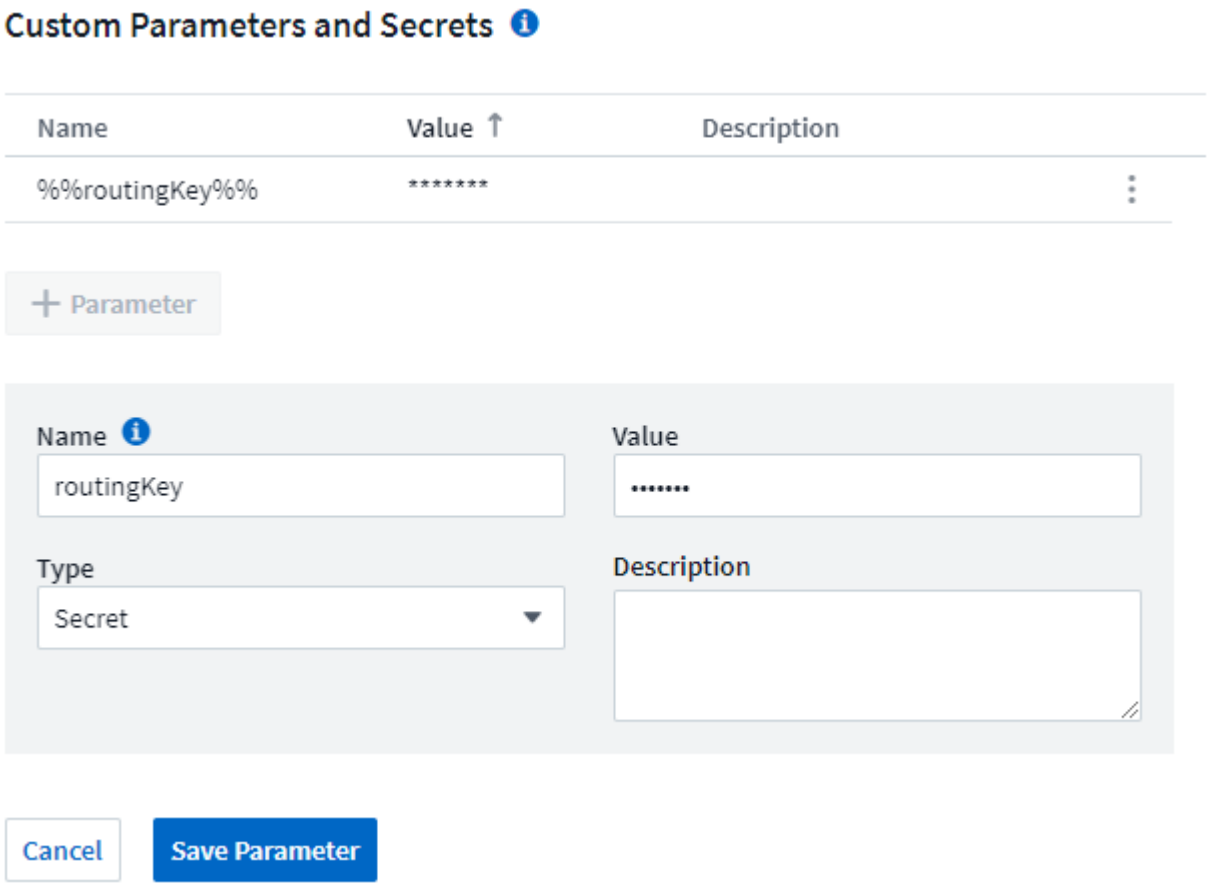


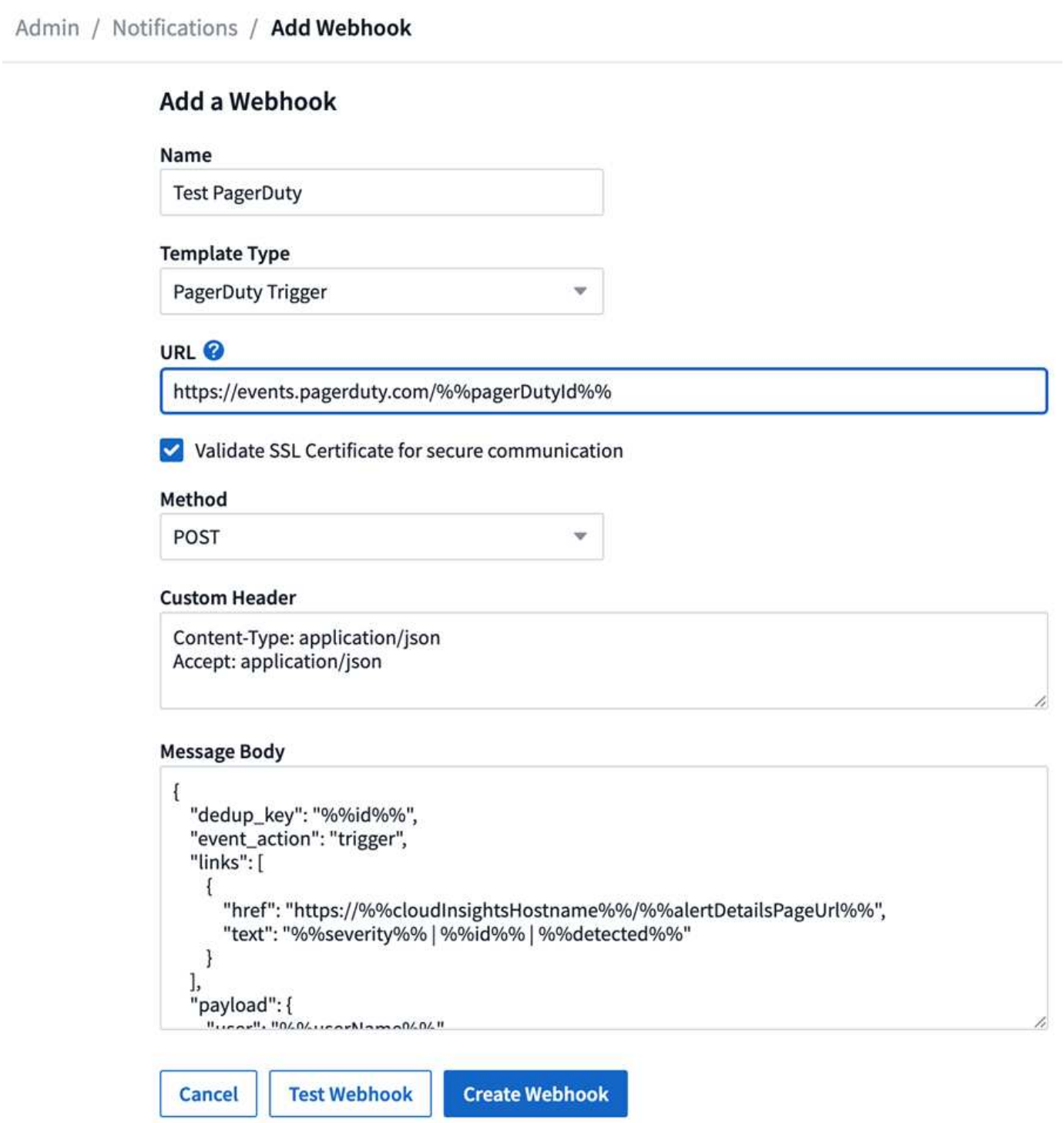
3. Seleccione la pestaña *Integraciones* para ver la **Clave de integración**. Necesitará esta clave cuando cree el webhook de seguridad de carga de trabajo a continuación.
4. Vaya a **Incidentes** o **Servicios** para ver las alertas.



Crear un webhook de PagerDuty para la seguridad de la carga de trabajo:

- Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Seleccione '+ Webhook' para crear un nuevo webhook.
- Dale al webhook un nombre significativo.
- En el menú desplegable *Tipo de plantilla*, seleccione *Activador PagerDuty*.
- Cree un parámetro secreto personalizado llamado *routingKey* y establezca el valor en la clave de integración de PagerDuty *Integration Key* creada anteriormente.

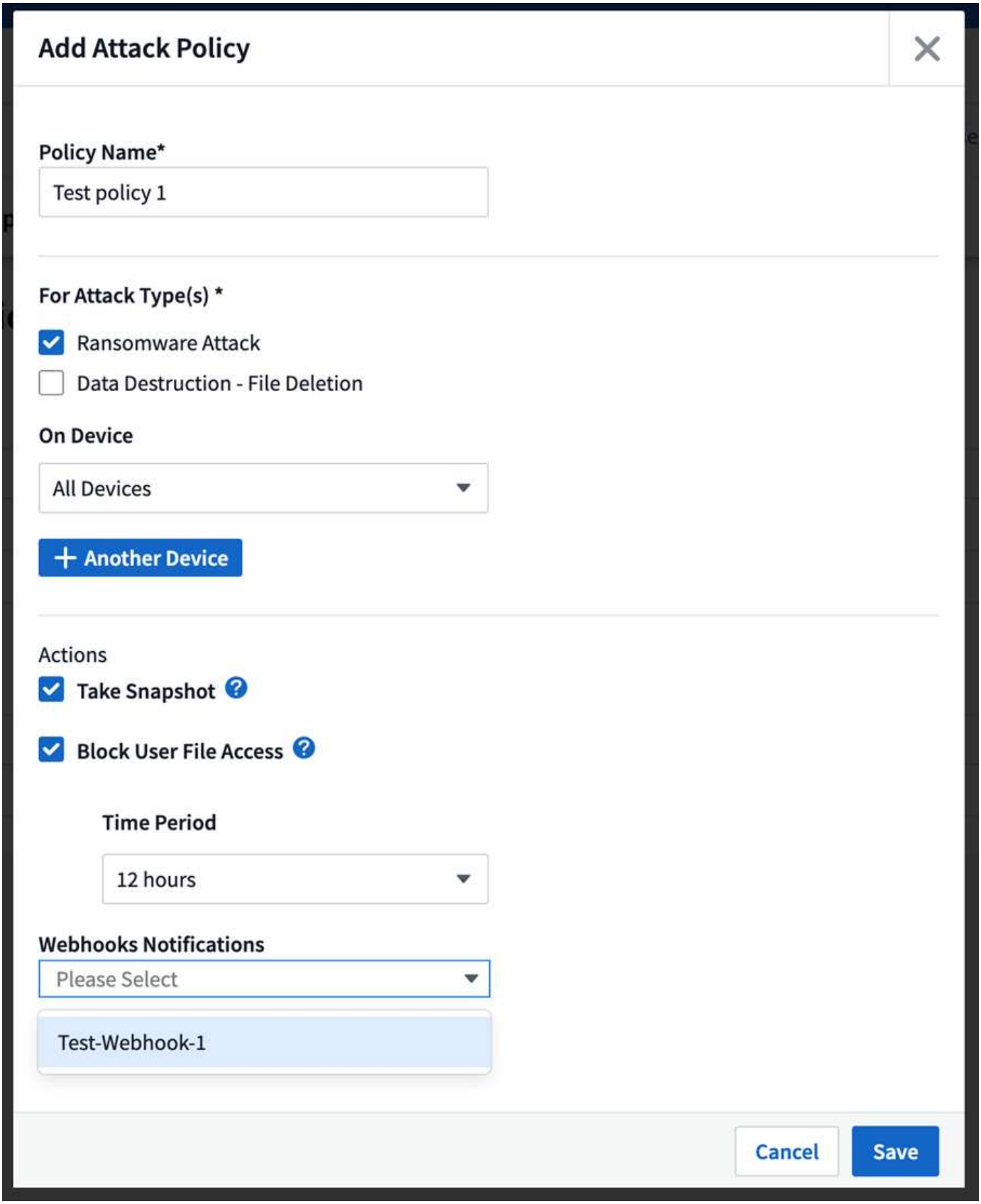




Notificaciones mediante webhook

- Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo* > *Políticas*. Seleccione *+Política de ataque* o *+Política de advertencia*.
- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de PagerDuty necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.



Ejemplo de webhook de seguridad de carga de trabajo para Slack

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Slack.

Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la documentación de Slack para obtener la información más actualizada.

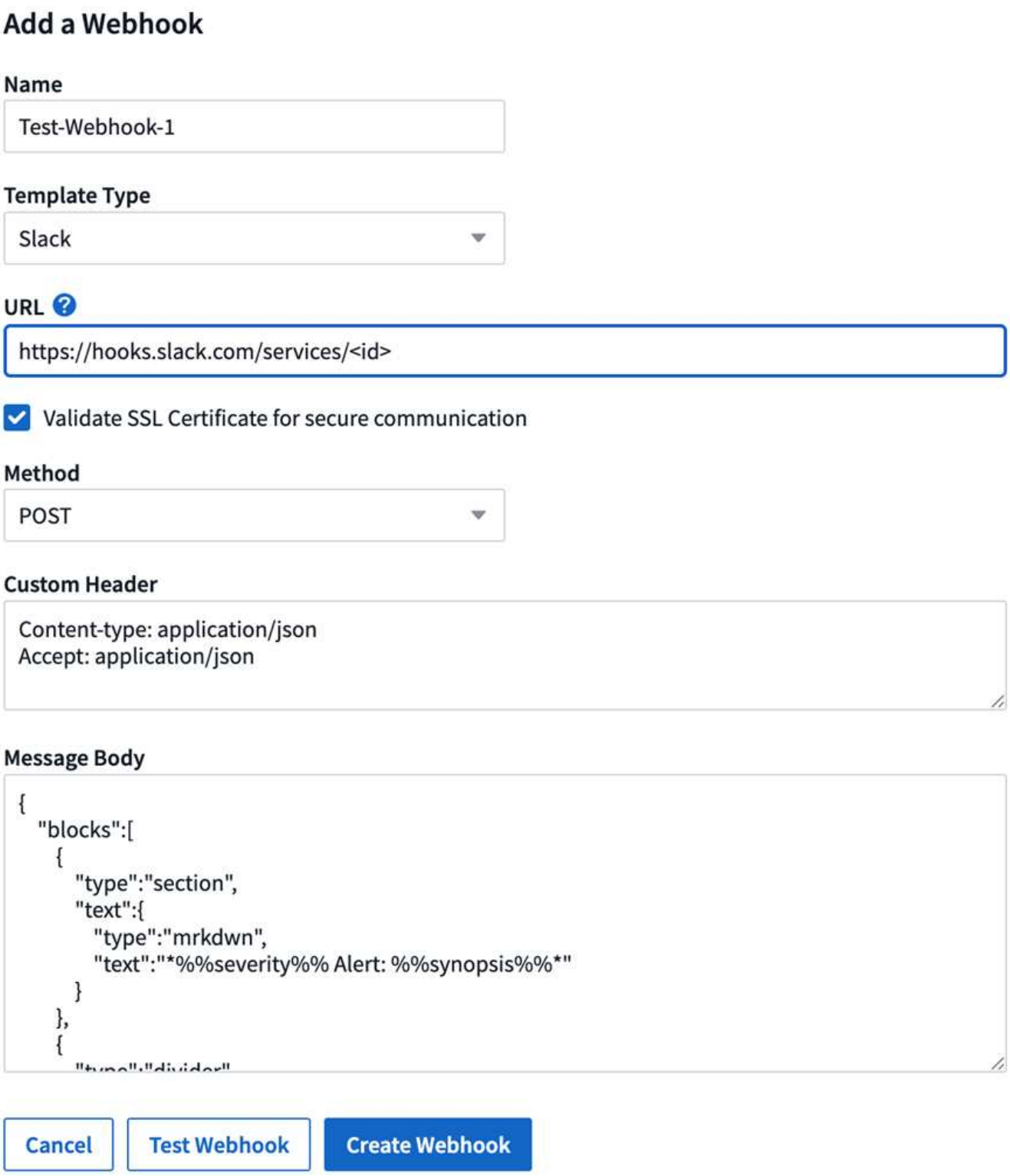
Ejemplo de holgura

- Ir a https://api.slack.com/apps y crea una nueva aplicación. Asígnele un nombre significativo y seleccione un espacio de trabajo.

- Vaya a Webhooks entrantes, haga clic en *Activar webhooks entrantes*, seleccione *Agregar nuevo webhook* y seleccione el canal en el que desea publicar.
- Copiar la URL del webhook. Esta URL se proporcionará al crear un webhook de seguridad de carga de trabajo.

Crear un webhook de Slack para la seguridad de la carga de trabajo

1. Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Seleccione + *Webhook* para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione *Slack*.
4. Pegue la URL copiada arriba.

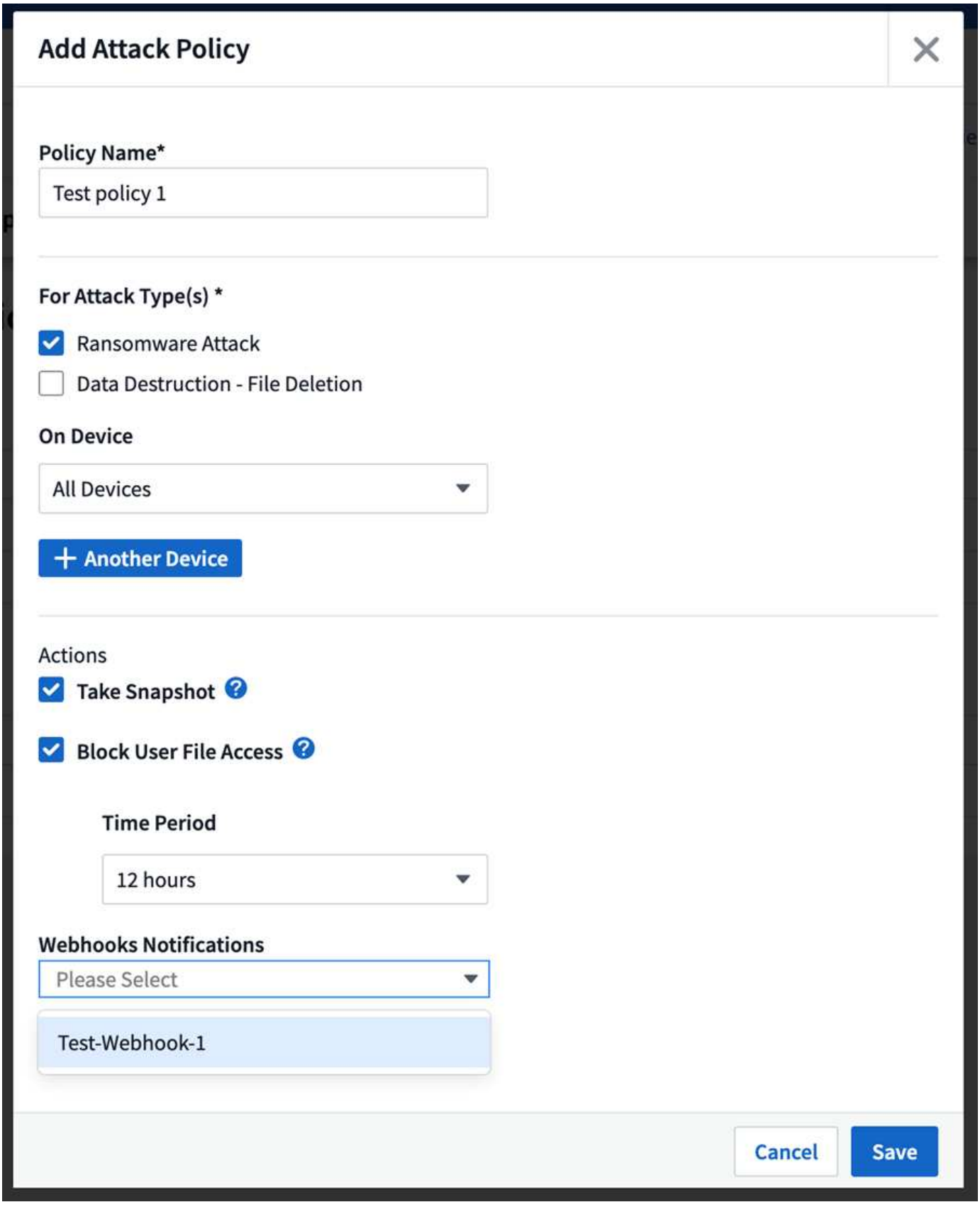


Notificaciones mediante webhook

- Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo* > *Políticas*. Haga clic en *+Política de ataque* o *+Política de advertencia*.
- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.

- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.



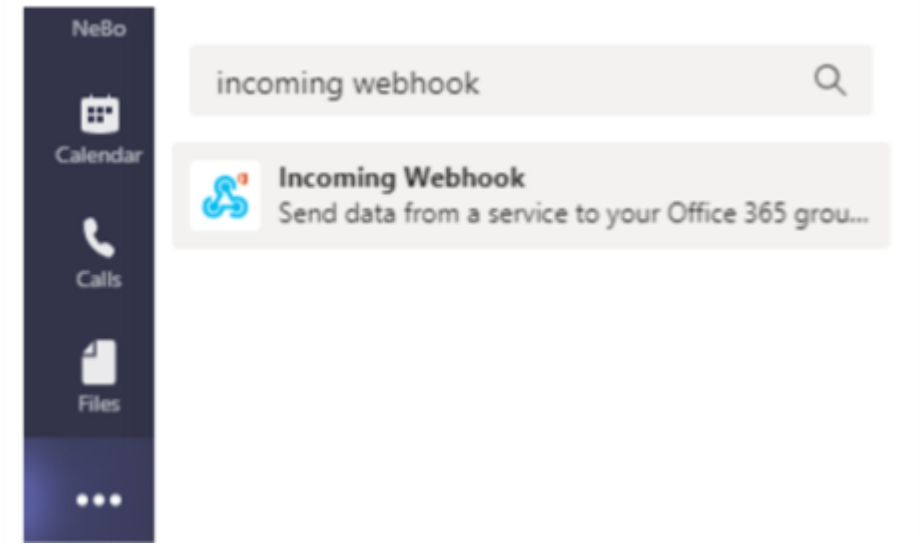
Ejemplo de webhook de seguridad de carga de trabajo para Microsoft Teams

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Teams.

Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la"Documentación de Teams" para obtener la información más actualizada.

Configuración de los equipos:

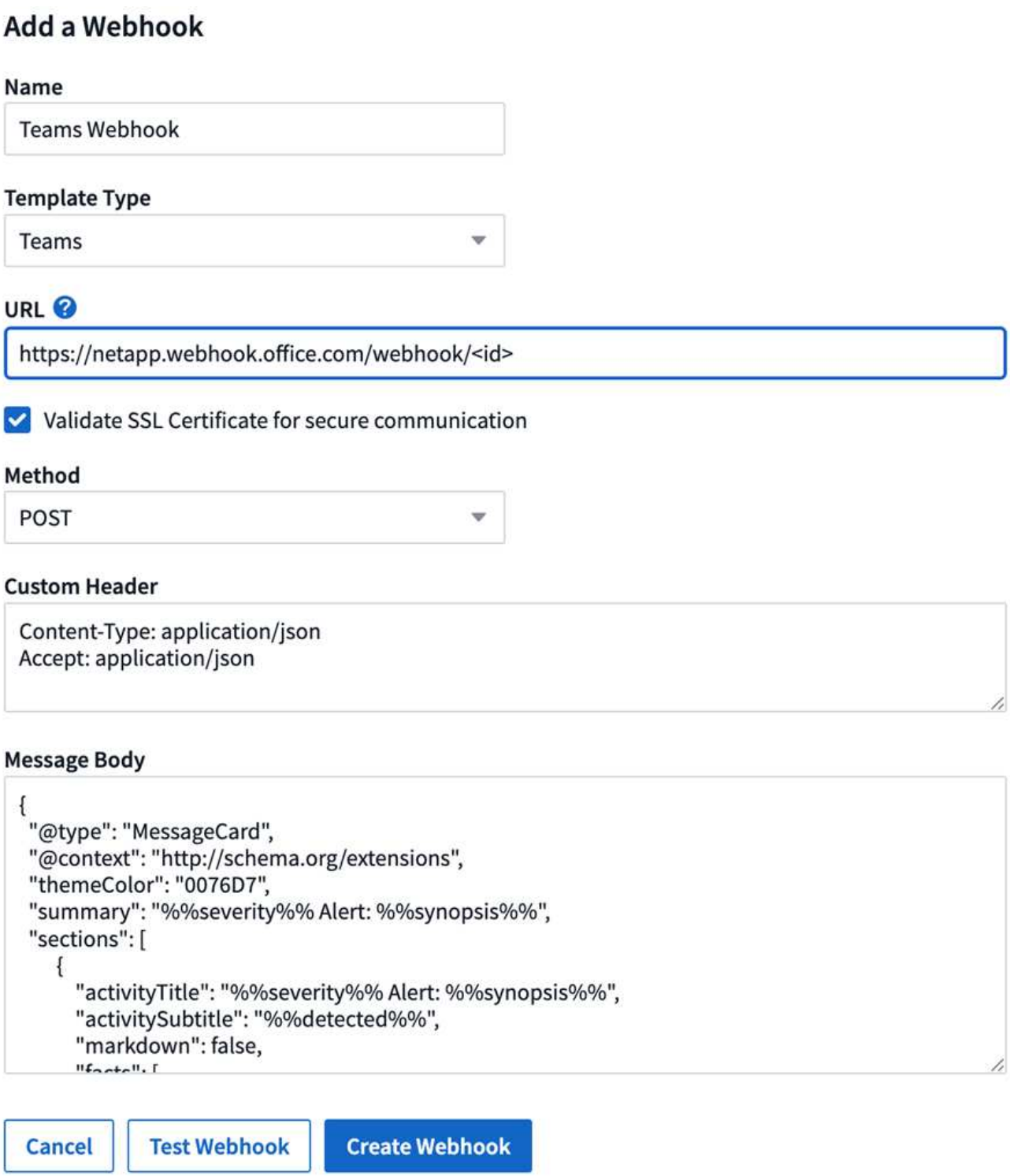
1. En Teams, seleccione el kebab y busque Webhook entrante.



2. Seleccione **Agregar a un equipo > Seleccionar un equipo > Configurar un conector**.
3. Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de seguridad de carga de trabajo.

Crear webhook de equipos de seguridad de carga de trabajo:

1. Vaya a Admin > Notificaciones y seleccione la pestaña *"Webhooks de seguridad de carga de trabajo*. Seleccione + *Webhook* para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione **Equipos**.



4. Pegue la URL de arriba en el campo *URL*.

Pasos para crear una notificación de Teams con la plantilla de tarjeta adaptable

1. Reemplaza el cuerpo del mensaje con la siguiente plantilla:

```
{
"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. Si usas Power Automate Flows, los parámetros de consulta en la URL están en formato codificado. Debes descodificar la URL antes de ingresarla.
3. Haz clic en "Probar Webhook" para asegurarte de que no hay errores.
4. Guarda el webhook.

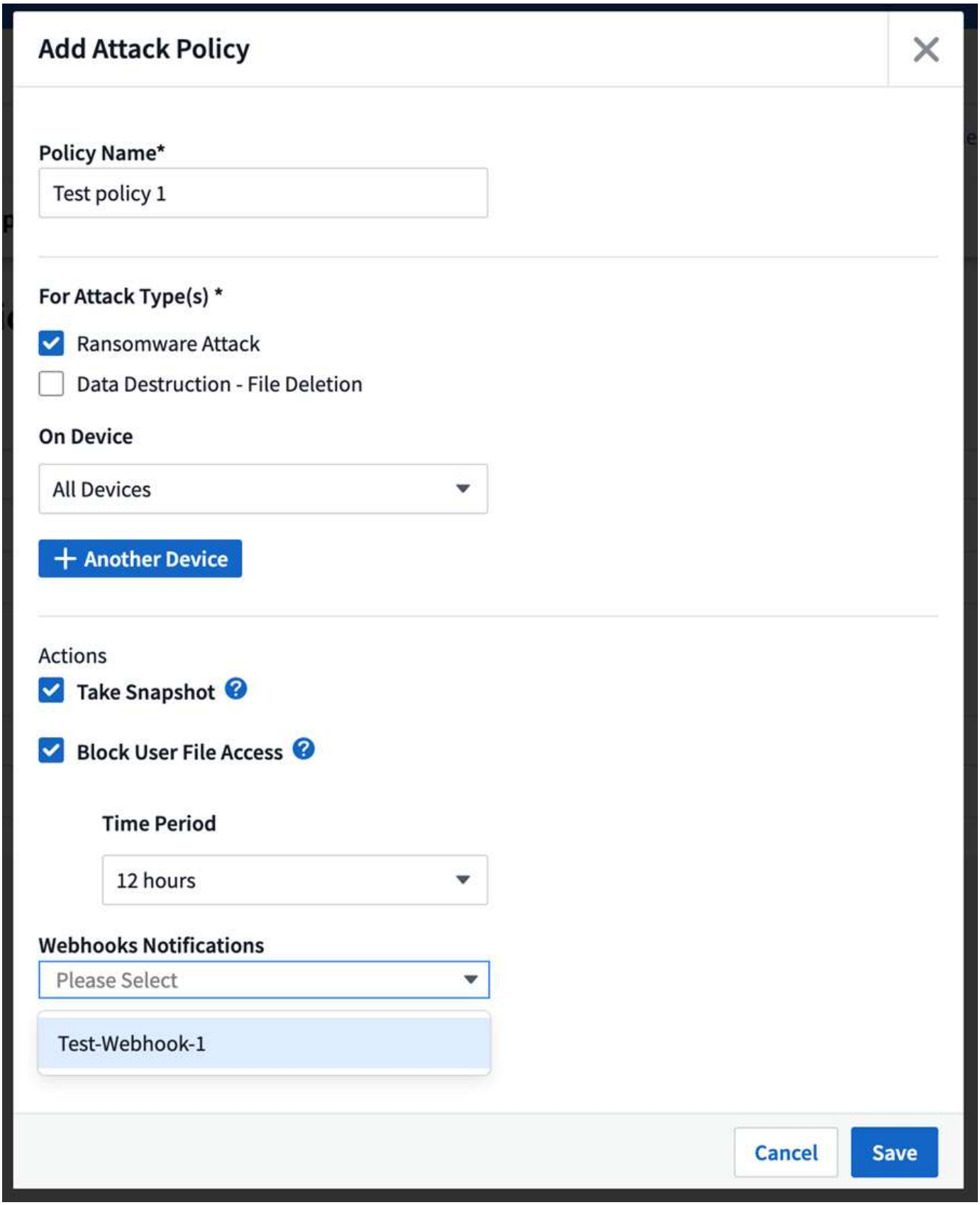
Notificaciones mediante webhook

Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo* > *Políticas*. Seleccione *+Política de ataque* o *+Política de advertencia*.

- Introduzca un nombre de política significativo.

- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de Teams necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.


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

Información de copyright

Información de la marca comercial