Notificações de webhook

Data Infrastructure Insights

NetApp
February 11, 2026

Índice

Notificações de webhook

Notificações de segurança de carga de trabalho usando webhooks

Os webhooks permitem que os usuários enviem notificações de alerta críticas ou de advertência para vários aplicativos usando um canal de webhook personalizado.

Muitos aplicativos comerciais oferecem suporte a webhooks como uma interface de entrada padrão, por exemplo: Slack, PagerDuty, Teams e Discord. Ao oferecer suporte a um canal webhook genérico e personalizável, o Workload Security pode oferecer suporte a muitos desses canais de entrega. Informações sobre como configurar os webhooks podem ser encontradas nos sites dos respectivos aplicativos. Por exemplo, o Slack fornece"este guia útil" .

Você pode criar vários canais de webhook, cada canal direcionado a uma finalidade diferente, aplicativos separados, destinatários diferentes, etc.

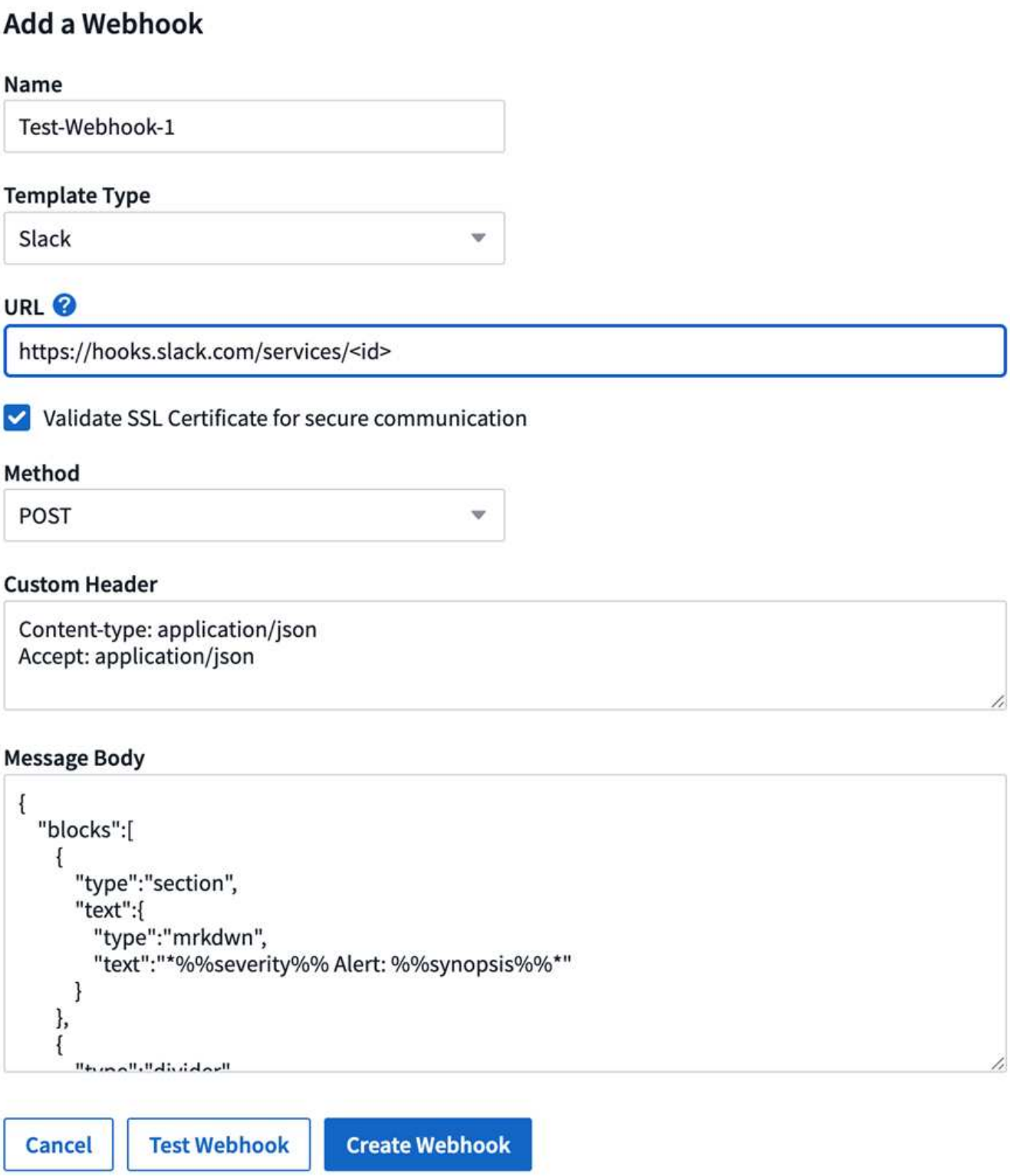
A instância do canal webhook é composta pelos seguintes elementos

Nome	Descrição
URL	URL de destino do webhook, incluindo o prefixo http:// ou https:// junto com os parâmetros de URL
Método	GET/POST - O padrão é POST
Cabeçalho personalizado	Especifique quaisquer cabeçalhos personalizados aqui
Corpo da mensagem	Coloque o corpo da sua mensagem aqui
Parâmetros de alerta padrão	Lista os parâmetros padrão para o webhook
Parâmetros e segredos personalizados	Parâmetros e segredos personalizados permitem que você adicione parâmetros exclusivos e elementos seguros, como senhas

Criando um webhook

Para criar um Webhook de segurança de carga de trabalho, vá para Admin > Notificações e selecione a aba “Webhooks de segurança de carga de trabalho”. A imagem a seguir mostra uma tela de exemplo de criação de webhook do Slack.

Observação: o usuário deve ser um *Administrador* do Workload Security para criar e gerenciar Webhooks do Workload Security.



- Insira as informações apropriadas para cada um dos campos e clique em "Salvar".
- Você também pode clicar no botão "Testar Webhook" para testar a conexão. Observe que isso enviará o "Corpo da Mensagem" (sem substituições) para a URL definida de acordo com o Método selecionado.
- Os webhooks do SWS compreendem uma série de parâmetros padrão. Além disso, você pode criar seus próprios parâmetros ou segredos personalizados.

Parâmetros: O que são e como usá-los?

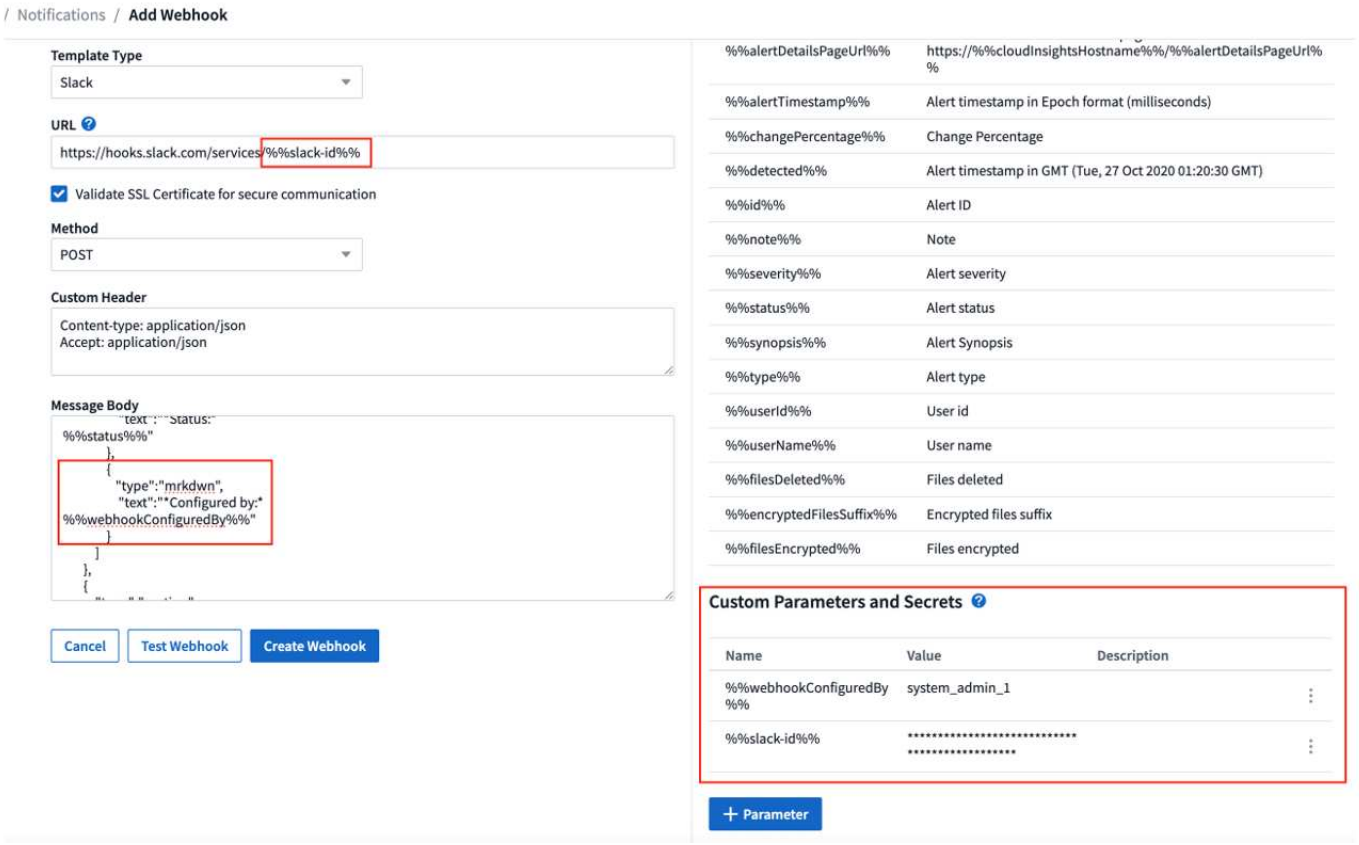
Parâmetros de alerta são valores dinâmicos preenchidos por alerta. Por exemplo, o parâmetro *%%severity%%* será substituído pelo tipo de gravidade do alerta.

Observe que as substituições não são realizadas ao clicar no botão "Testar Webhook"; o teste envia uma carga útil que mostra os espaços reservados do parâmetro (*%%<param-name>%%*), mas não os substitui por dados.

Parâmetros e segredos personalizados

Nesta seção, você pode adicionar quaisquer parâmetros personalizados e/ou segredos que desejar. Um parâmetro personalizado ou segredo pode estar no URL ou no corpo da mensagem. Os segredos permitem que o usuário configure um parâmetro personalizado seguro, como senha, apiKey etc.

A imagem de exemplo a seguir mostra como parâmetros personalizados são usados na criação de webhook.



Página da lista de webhooks de segurança de carga de trabalho

Na página da lista Webhooks, são exibidos os campos Nome, Criado por, Criado em, Status, Seguro e Último relatório. Observação: o valor da coluna 'status' continuará mudando com base no resultado do último gatilho do webhook. A seguir estão alguns exemplos de resultados de status.

Status	Descrição
OK	Notificação enviada com sucesso.
403	Proibido.

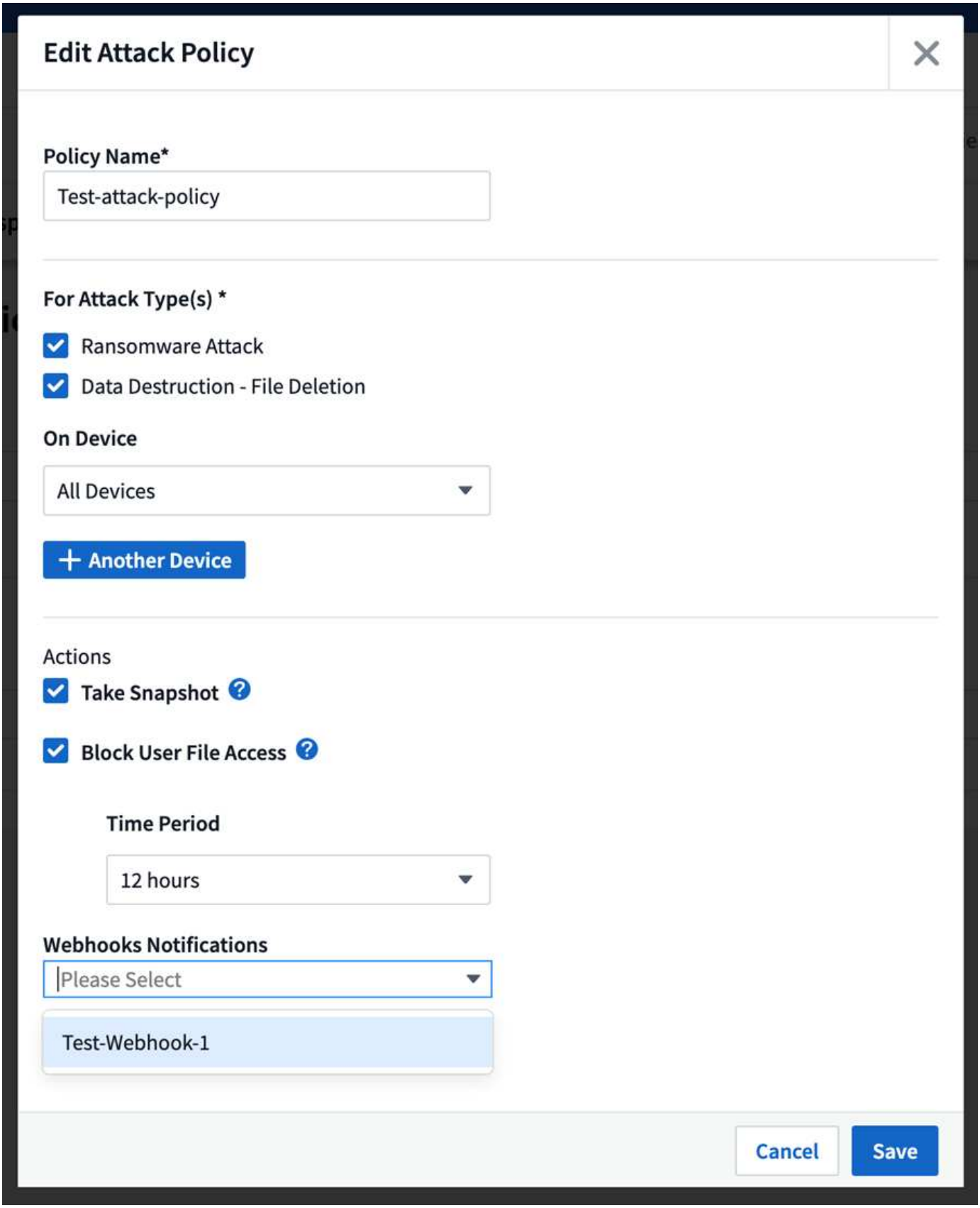
404	URL não encontrada.
400	Pedido ruim. Você poderá ver esse status se houver algum erro no corpo da mensagem, por exemplo: • JSON mal formatado. • Fornecendo valor inválido para chaves reservadas. Por exemplo, o PagerDuty aceita apenas crítico/aviso/erro/informação para “Gravidade”. Qualquer outro resultado pode render um status 400. • Erros de validação específicos do aplicativo. Por exemplo, o Slack permite no máximo 10 campos dentro de uma seção. Incluir mais de 10 pode resultar em um status 400.
410	O recurso não está mais disponível

A coluna “Último relatório” indica o horário em que o webhook foi acionado pela última vez.

Na página de listagem de webhooks, os usuários também podem editar/duplicar/excluir webhooks.

Configurar notificação de Webhook na política de alerta

Para adicionar uma notificação de webhook a uma política de alerta, acesse -Segurança de carga de trabalho > Políticas- e selecione uma política existente ou adicione uma nova política. Na seção *Ações* > menu suspenso *Notificações de webhook*, selecione os webhooks necessários.



As notificações do webhook estão vinculadas às políticas. Quando o ataque (RW/DD/WARN) acontecer, a ação configurada (Tirar snapshot/bloqueio de usuário) será tomada e então a notificação de webhook associada será acionada.

Observação: as notificações por e-mail são independentes de políticas e serão acionadas normalmente.

- Se uma política for pausada, as notificações do webhook não serão acionadas.
- Vários webhooks podem ser anexados a uma única política, mas é recomendável anexar no máximo 5 webhooks a uma política.

Exemplos de webhook de segurança de carga de trabalho

Webhooks para"Folga"

Webhooks para"PagerDuty" Webhooks para"Equipes" Webhooks para"Discórdia"

Exemplo de webhook de segurança de carga de trabalho para Discord

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Discord.

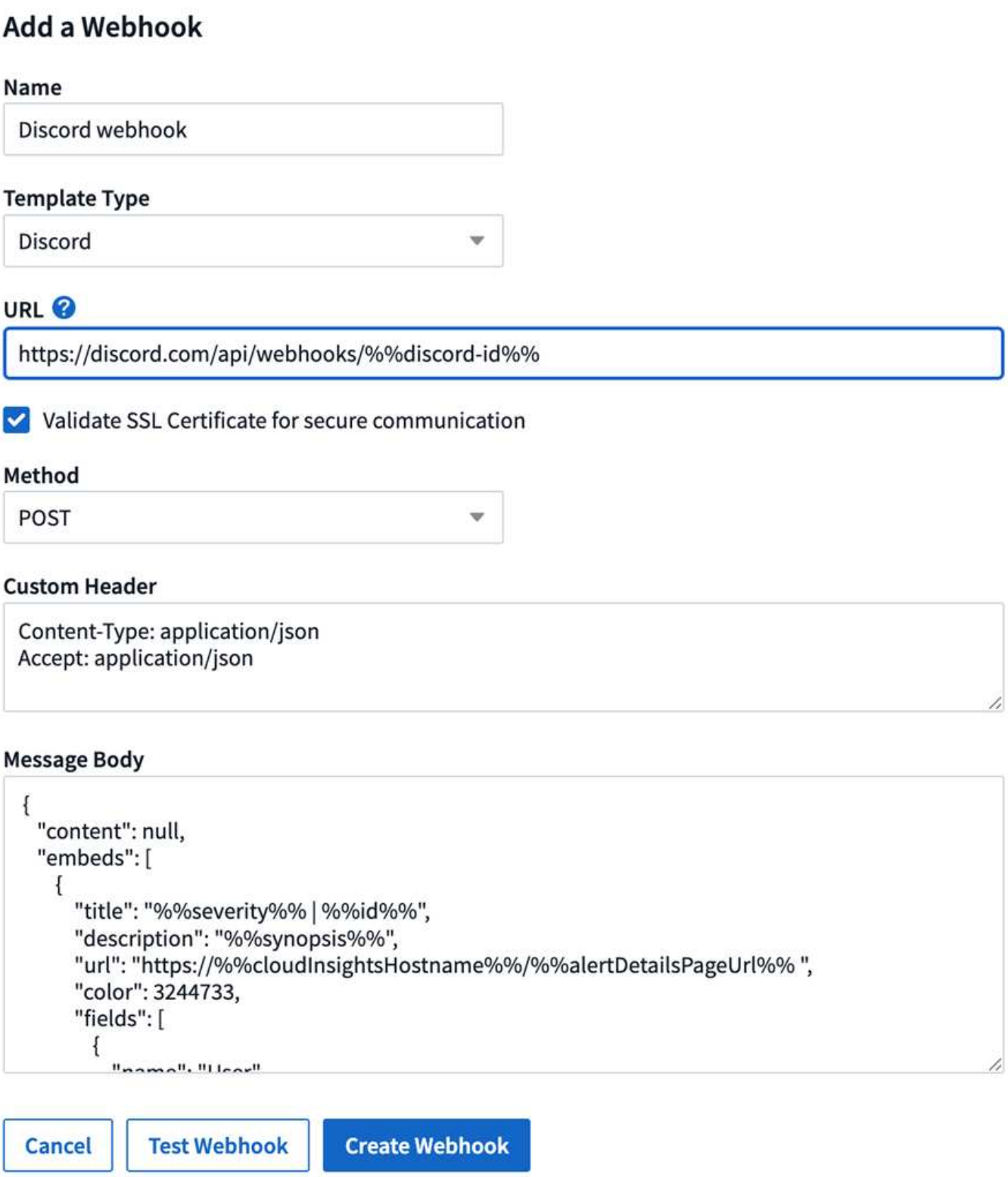
Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o"Documentação do Discord" para obter as informações mais atualizadas.

Configuração do Discord:

- No Discord, selecione o Servidor, em Canais de Texto, selecione Editar Canal (ícone de engrenagem)
- Selecione **Integrações > Exibir Webhooks** e clique em **Novo Webhook**
- Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Workload Security.

Criar Webhook de Segurança de Carga de Trabalho:

1. Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Clique em "+ Webhook" para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione **Discord**.
4. Cole a URL do Discord acima no campo *URL*.



Para testar o webhook, substitua temporariamente o valor da URL no corpo da mensagem por qualquer URL válida (como *https://netapp.com*) e clique no botão *Testar Webhook*. O Discord exige que uma URL válida seja fornecida para que a funcionalidade Test Webhook funcione.

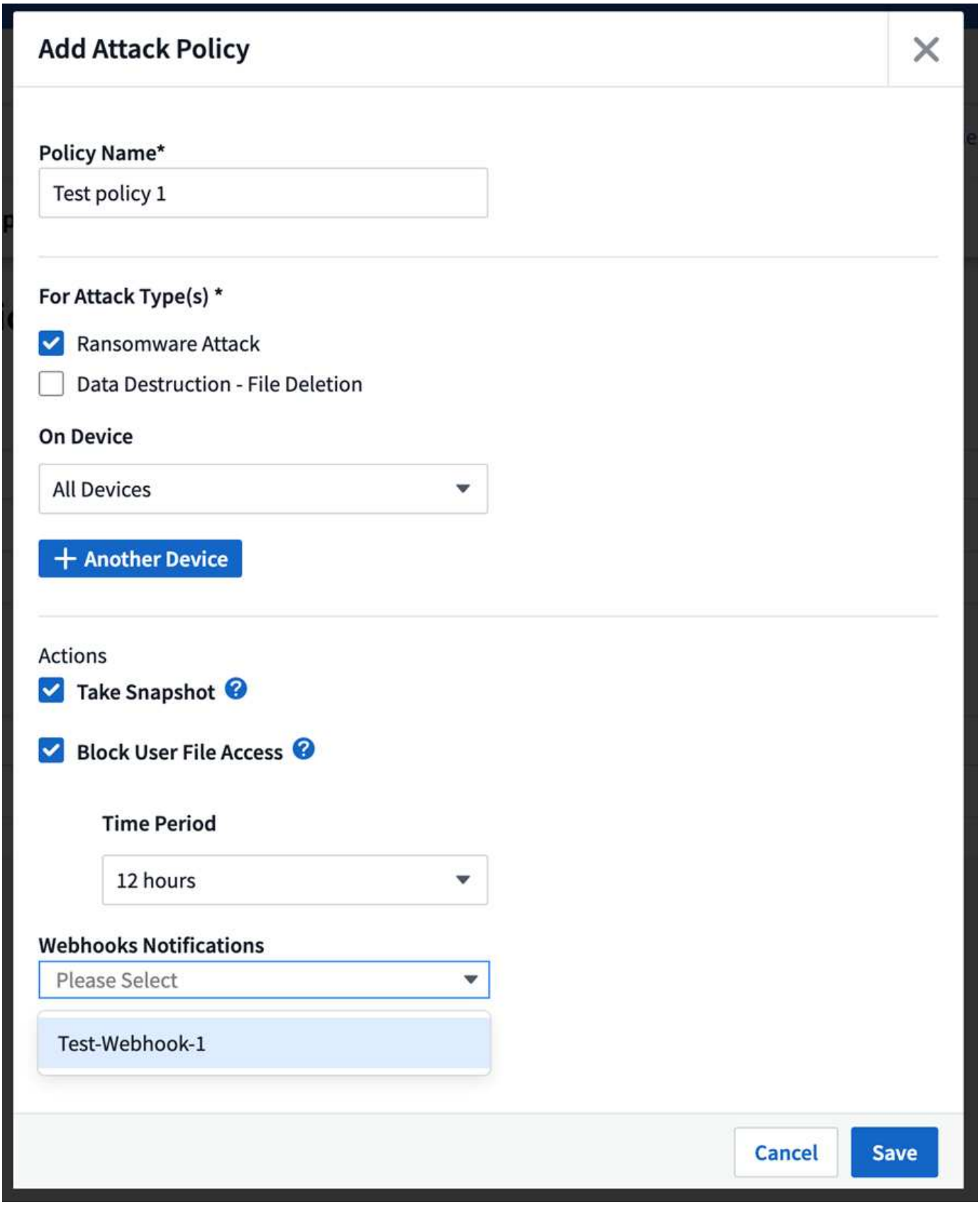
Não se esqueça de redefinir o corpo da mensagem quando o teste for concluído.

Notificações via Webhook

Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho* > *Políticas*. Clique em *+Política de Ataque* ou *+Política de Aviso*.

- Insira um nome de política significativo.
- Selecione o(s) Tipo(s) de Ataque necessário(s), os Dispositivos aos quais a política deve ser anexada e as Ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do Discord necessários e salve.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.


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

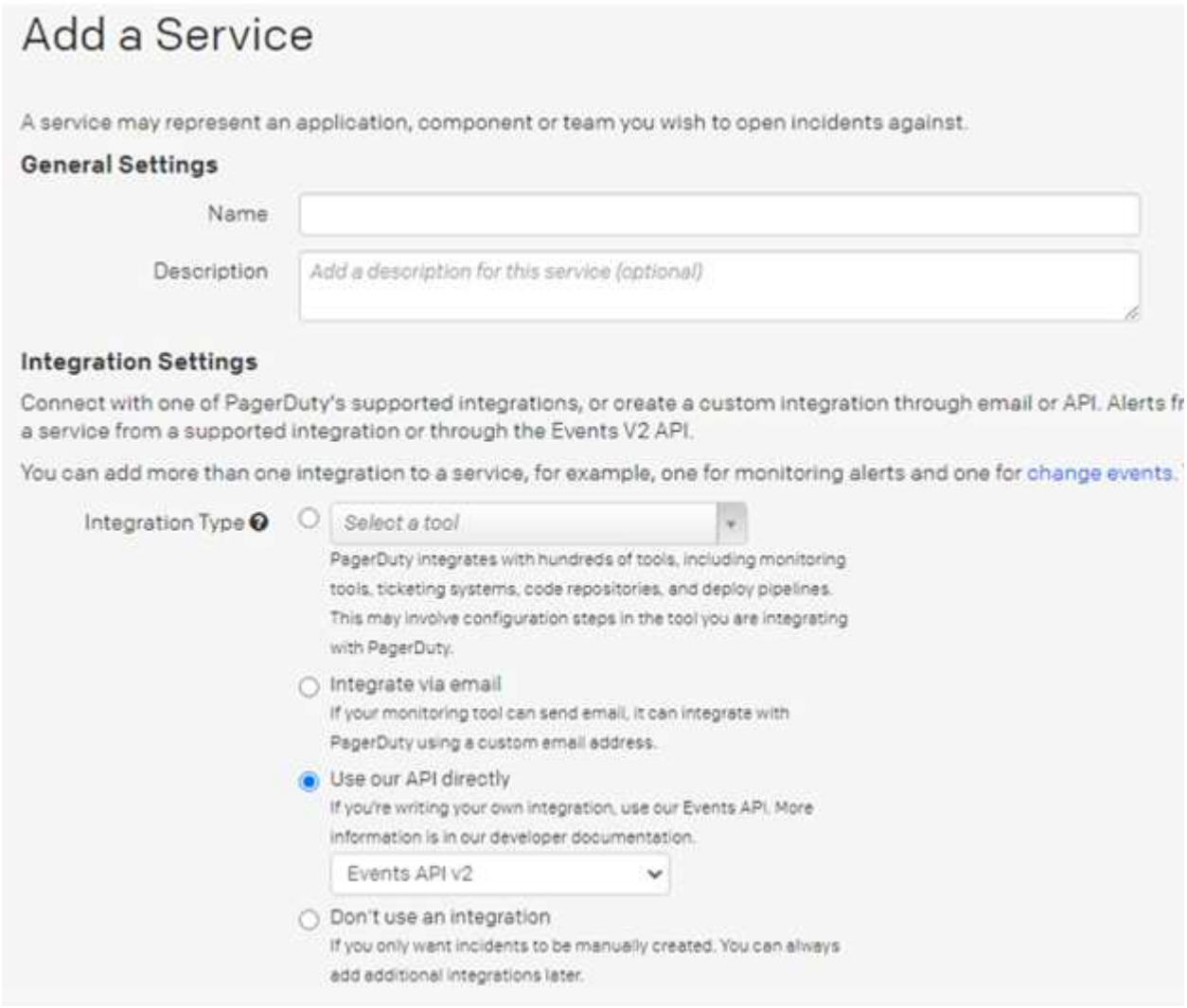
Exemplo de webhook de segurança de carga de trabalho para PagerDuty

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o PagerDuty.

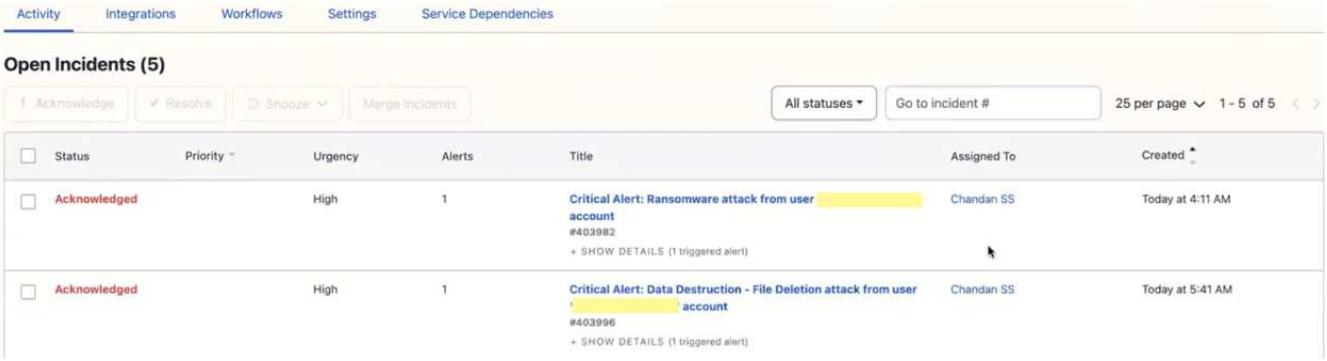
Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o"Documentação do PagerDuty" para obter as informações mais atualizadas.

Configuração do PagerDuty:

1. No PagerDuty, navegue até **Serviços > Diretório de serviços** e clique no botão **+Novo serviço**.
2. Digite um *Nome* e selecione *Usar nossa API diretamente*. Selecione *Adicionar serviço*.

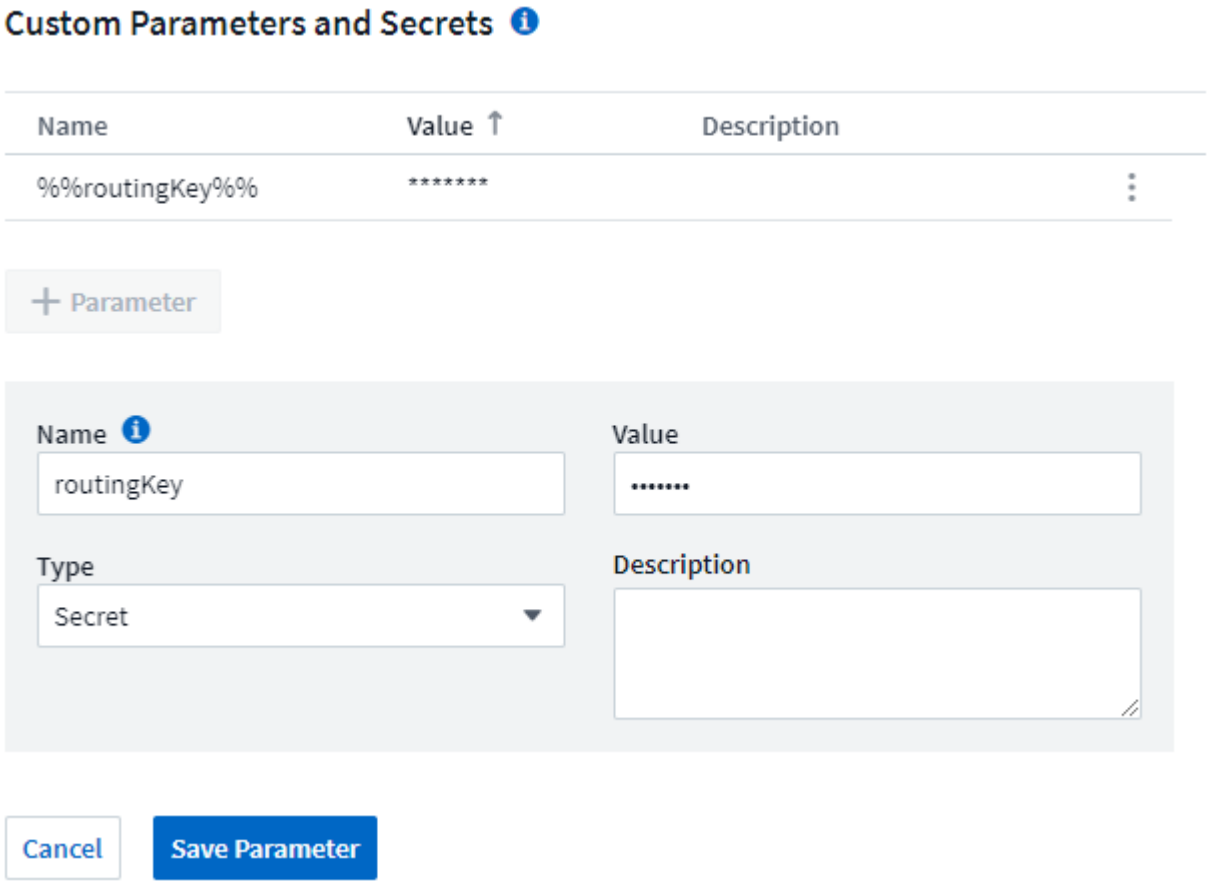


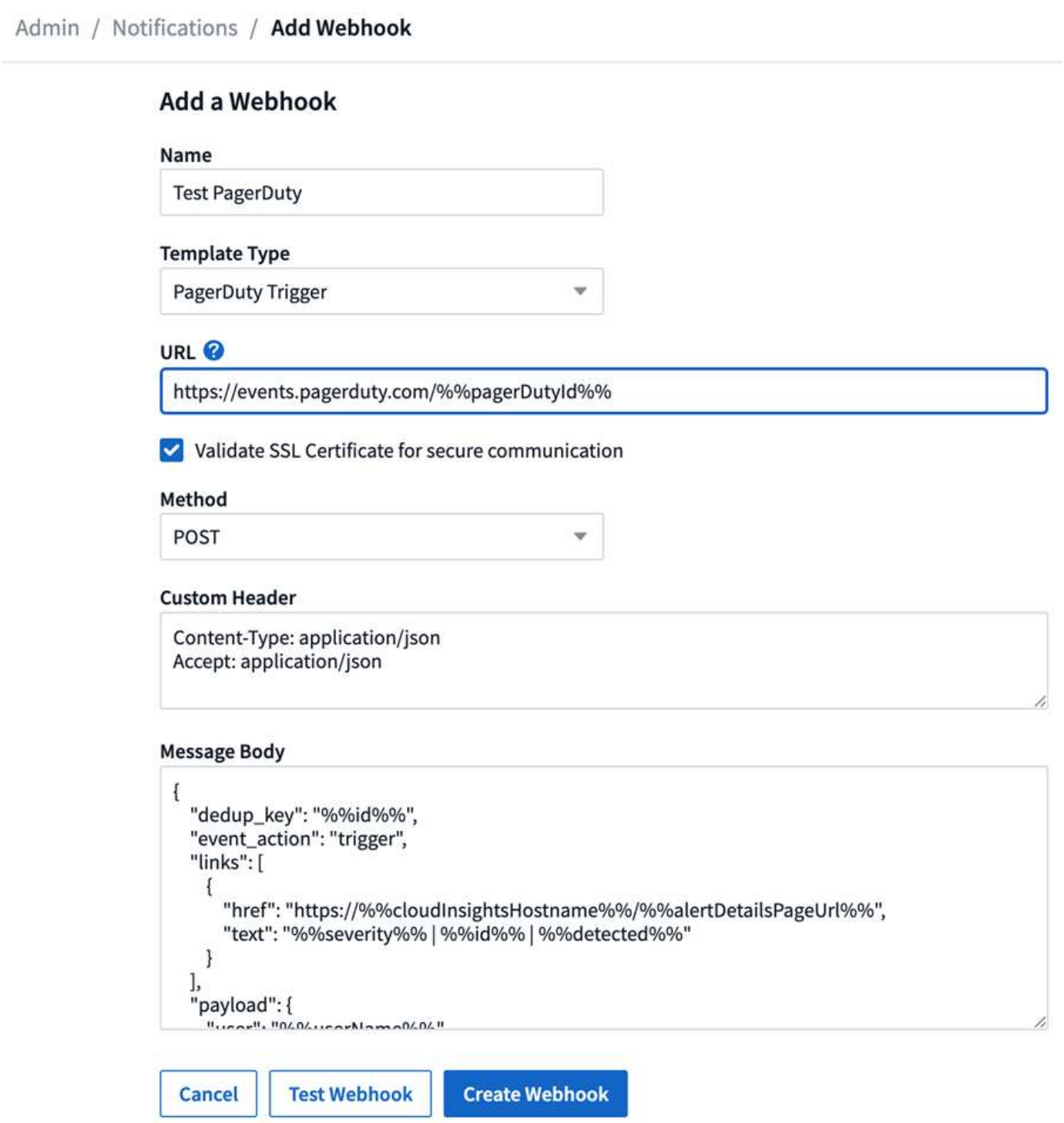
3. Selecione a aba *Integrações* para ver a **Chave de Integração**. Você precisará dessa chave ao criar o webhook do Workload Security abaixo.
4. Acesse **Incidentes** ou **Serviços** para visualizar Alertas.



Criar Webhook do PagerDuty de Segurança de Carga de Trabalho:

- Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Selecione '+ Webhook' para criar um novo webhook.
- Dê ao webhook um nome significativo.
- No menu suspenso *Tipo de modelo*, selecione *Gatilho do PagerDuty*.
- Crie um segredo de parâmetro personalizado chamado *routingKey* e defina o valor como a *Chave de Integração* do PagerDuty criada acima.

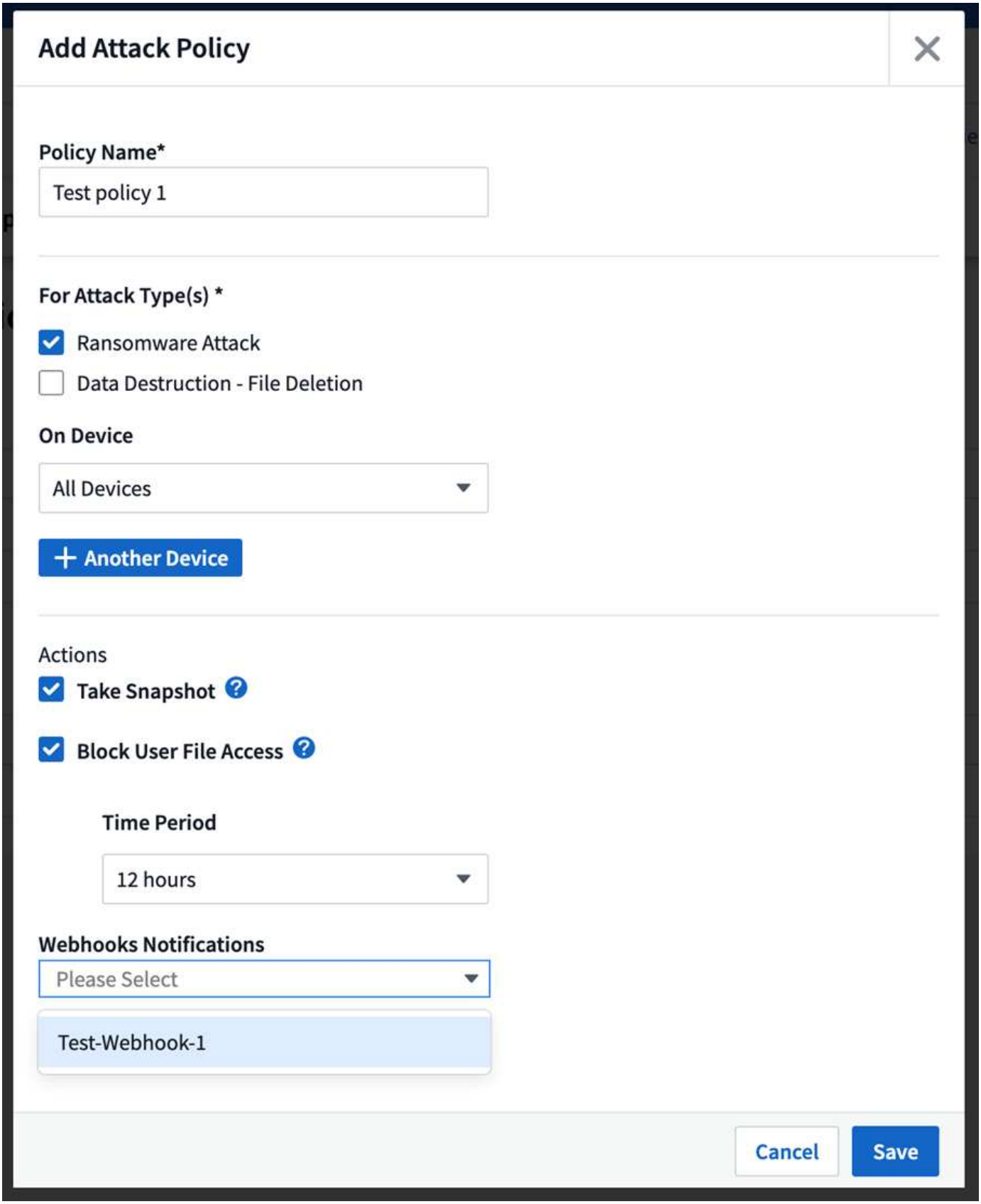




Notificações via Webhook

- Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho* > *Políticas*. Selecione *+Política de Ataque* ou *+Política de Aviso*.
- Insira um nome de política significativo.
- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do PagerDuty necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



Exemplo de webhook de segurança de carga de trabalho para Slack

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Slack.

Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte a documentação do Slack para obter as informações mais atualizadas.

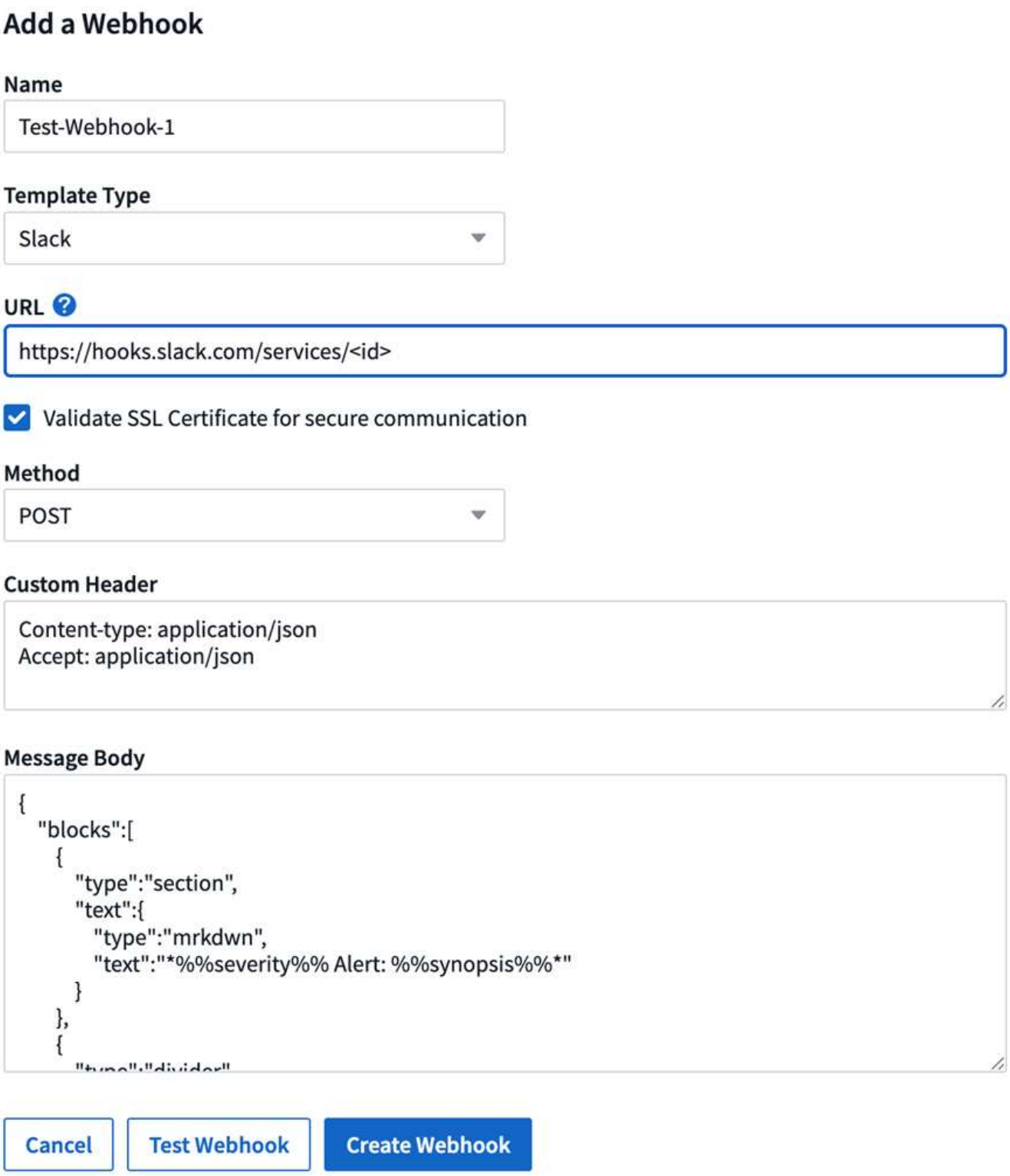
Exemplo de folga

- Vá para https://api.slack.com/apps e crie um novo aplicativo. Dê um nome significativo e selecione um espaço de trabalho.

- Vá para Webhooks de entrada, clique em *Ativar Webhooks de entrada*, selecione *Adicionar novo Webhook* e selecione o canal no qual deseja postar.
- Copie o URL do Webhook. Esta URL será fornecida ao criar um webhook de segurança de carga de trabalho.

Criar Webhook do Slack para Segurança de Carga de Trabalho

1. Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Selecione + *Webhook* para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione *Slack*.
4. Cole a URL copiada acima.

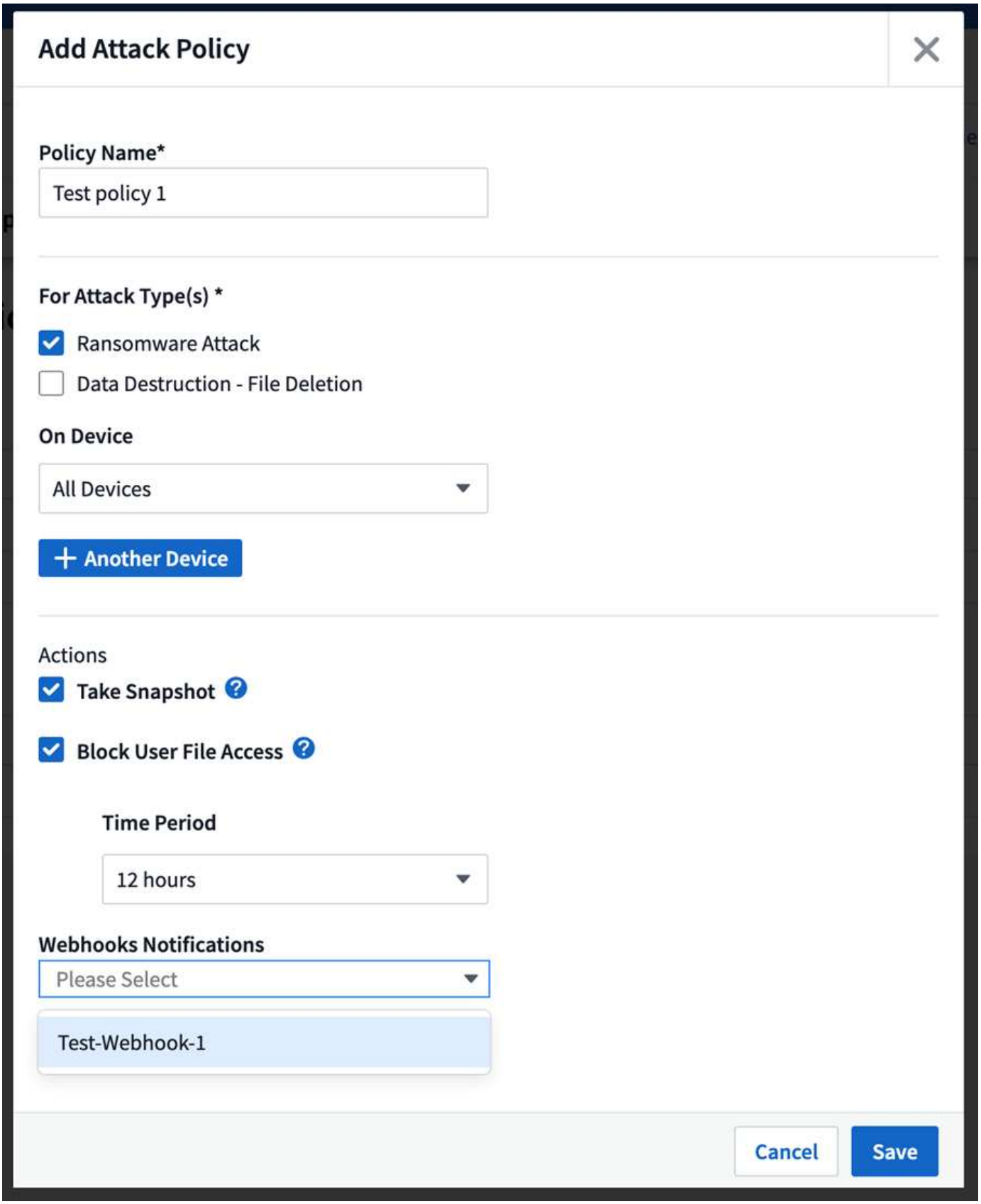


Notificações via webhook

- Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho* > *Políticas*. Clique em *+Política de Ataque* ou *+Política de Aviso*.
- Insira um nome de política significativo.
- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.

- No menu suspenso *Notificações de webhooks*, selecione os webhooks necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



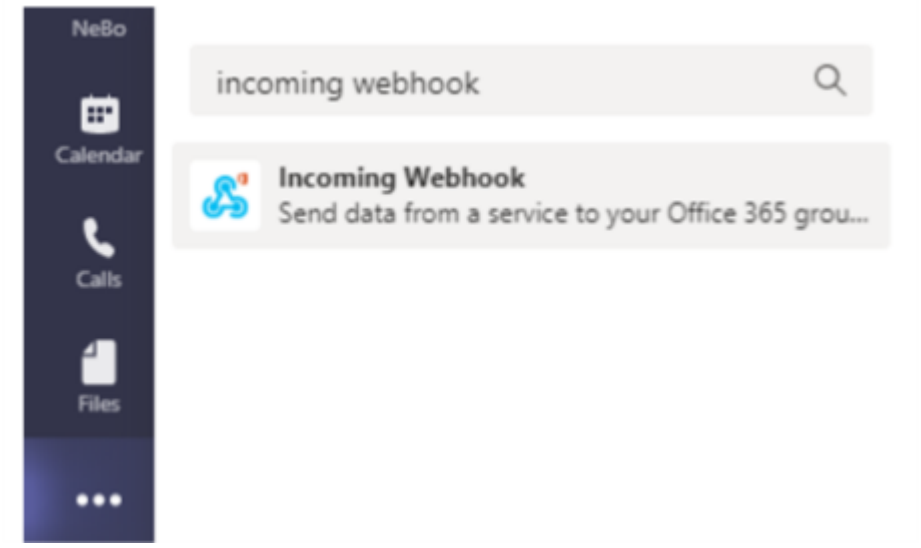
Exemplo de webhook de segurança de carga de trabalho para Microsoft Teams

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Teams.

Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o"Documentação das equipes" para obter as informações mais atualizadas.

Configuração das equipes:

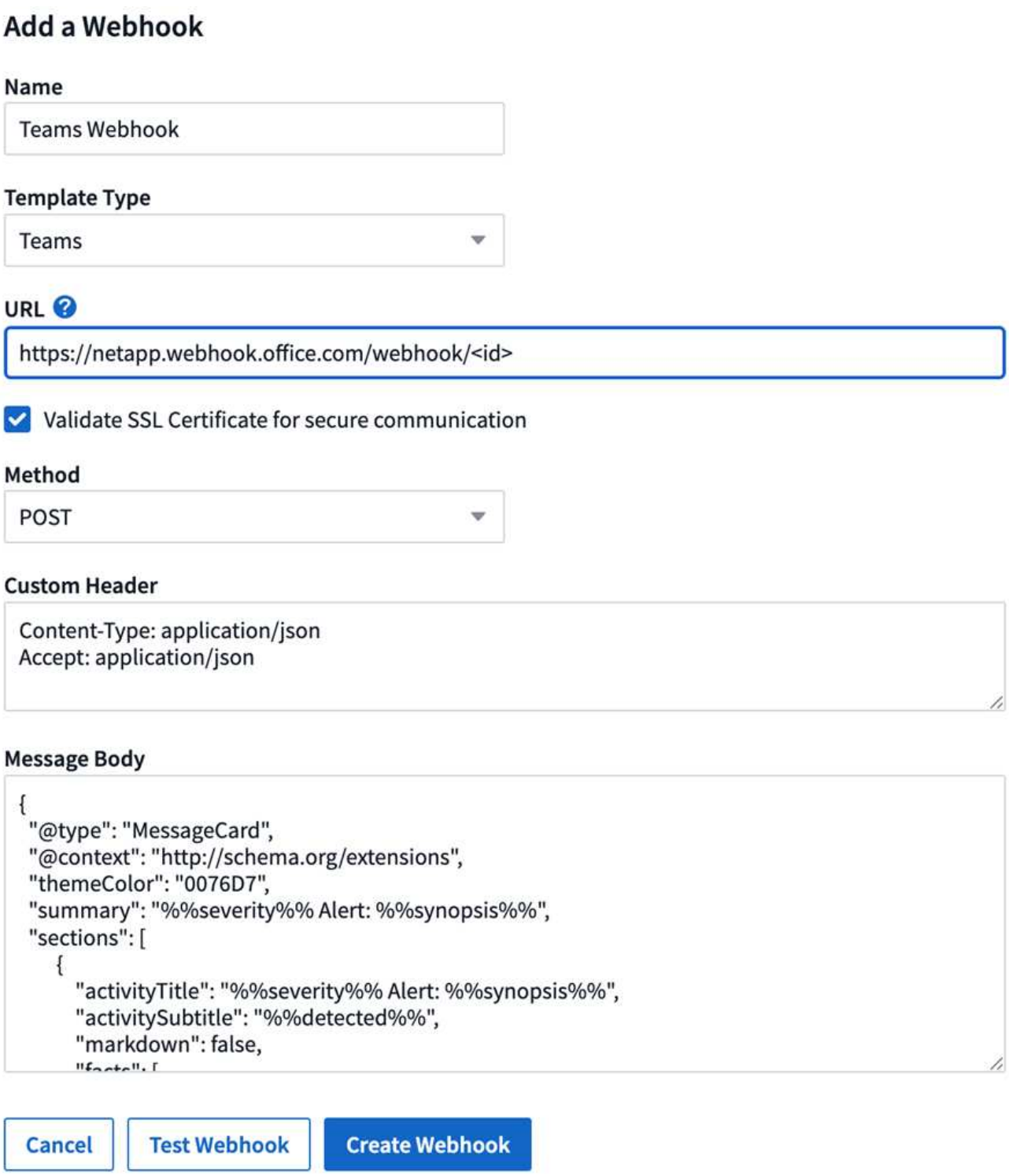
1. No Teams, selecione o kebab e pesquise por Webhook de entrada.



2. Selecione **Adicionar a uma equipe > Selecionar uma equipe > Configurar um conector**.
3. Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Workload Security.

Criar Webhook de Equipes de Segurança de Carga de Trabalho:

1. Navegue até Admin > Notificações e selecione a aba *"Workload Security Webhooks*. Selecione + *Webhook* para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione **Equipes**.



4. Cole a URL acima no campo *URL*.

Passos para criar uma notificação do Teams com o modelo de Adaptive Card

1. Substitua o corpo da mensagem pelo seguinte modelo:

```
{
"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. Se você estiver usando Power Automate Flows, os parâmetros de consulta na URL estarão em formato codificado. Você deve decodificar a URL antes de inserir.
3. Clique em "Test Webhook" para garantir que não haja erros.
4. Salve o webhook.

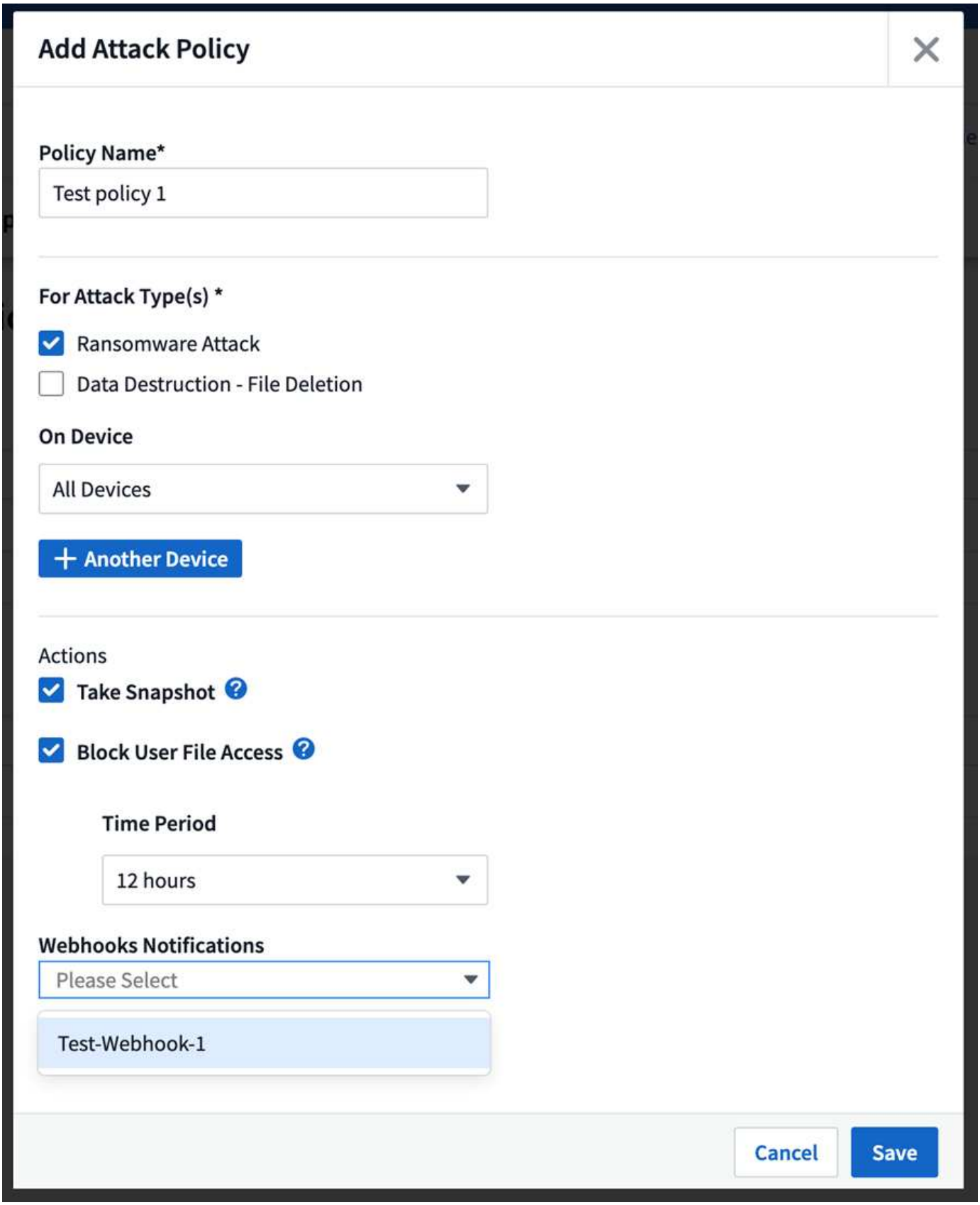
Notificações via Webhook

Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho > Políticas*. Selecione *+Política de Ataque* ou *+Política de Aviso*.

- Insira um nome de política significativo.

- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do Teams necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.


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

Informações sobre direitos autorais

Informações sobre marcas comerciais