Webhook 通知

Data Infrastructure Insights

NetApp
February 03, 2026

目录

Webhook 通知

使用 webhook 的工作负载安全通知

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送关键或警告警报通知。

许多商业应用程序支持 webhook 作为标准输入接口，例如：Slack、PagerDuty、Teams 和 Discord。通过支持通用、可定制的 webhook 通道，Workload Security 可以支持许多这样的交付通道。有关配置 webhook 的信息可以在相应应用程序的网站上找到。例如，Slack 提供"这个有用的指南"。

您可以创建多个 webhook 通道，每个通道针对不同的目的、单独的应用程序、不同的收件人等。

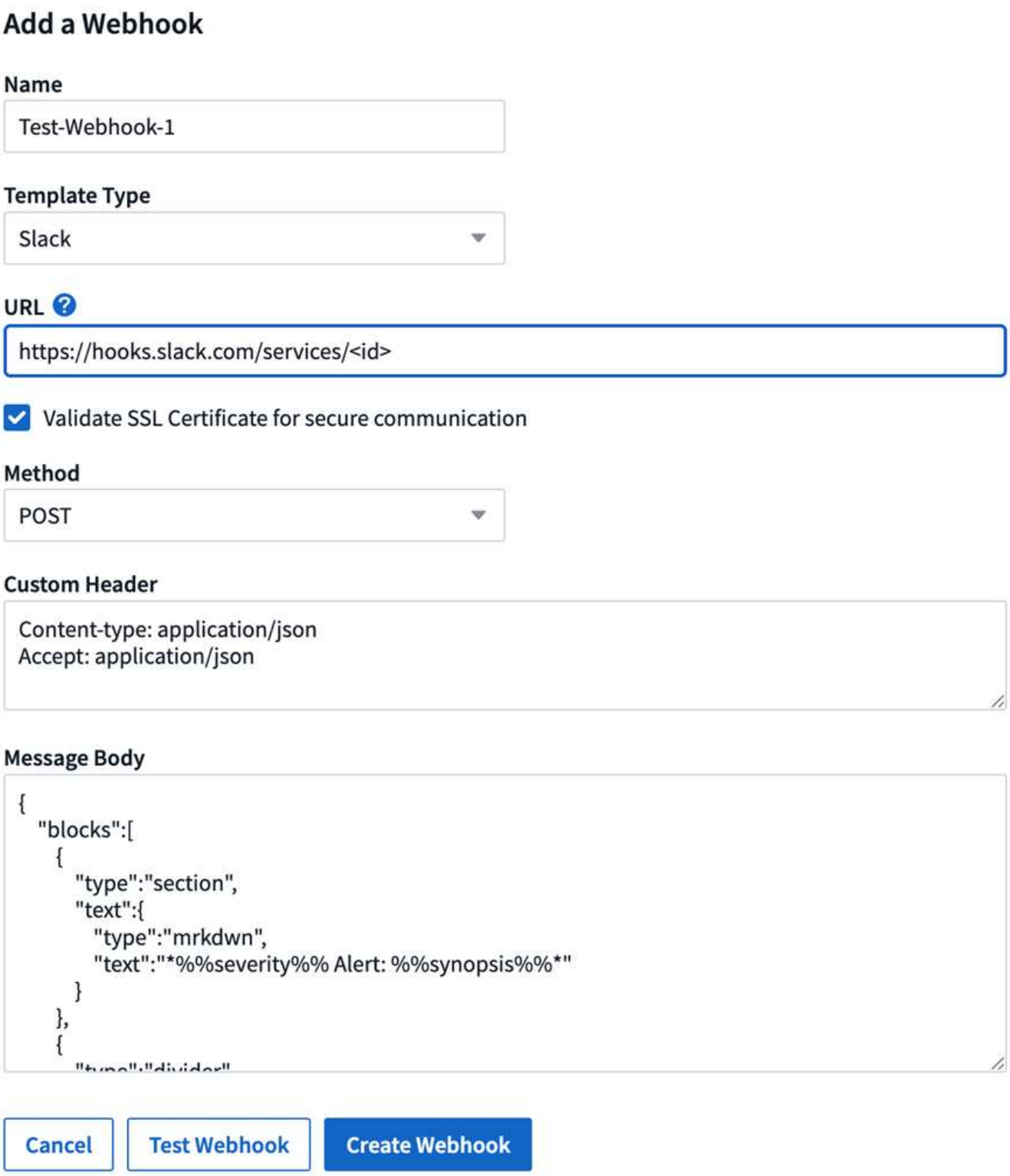
Webhook 通道实例由以下元素组成

名称	描述
URL	Webhook 目标 URL，包括 http:// 或 https:// 前缀以及 URL 参数
方法	GET/POST - 默认为 POST
自定义标题	在此处指定任何自定义标题
消息正文	在此处填写您的邮件正文
默认警报参数	列出 webhook 的默认参数
自定义参数和机密	自定义参数和秘密允许您添加唯一参数和安全元素，例如密码

创建 webhook

要创建工作负载安全 Webhook，请转到管理 > 通知并选择“工作负载安全 Webhook”选项卡。下图显示了 Slack webhook 创建屏幕的示例。

注意：用户必须是工作负载安全_管理员_才能创建和管理工作负载安全 Webhook。



- 在每个字段中输入适当的信息，然后单击“保存”。
- 您也可以点击“测试 Webhook”按钮来测试连接。请注意，这将根据所选方法将“消息正文”（不带替换）发送到定义的 URL。
- SWS webhook 包含许多默认参数。此外，您还可以创建自己的自定义参数或秘密。

参数：它们是什么以及如何使用它们?

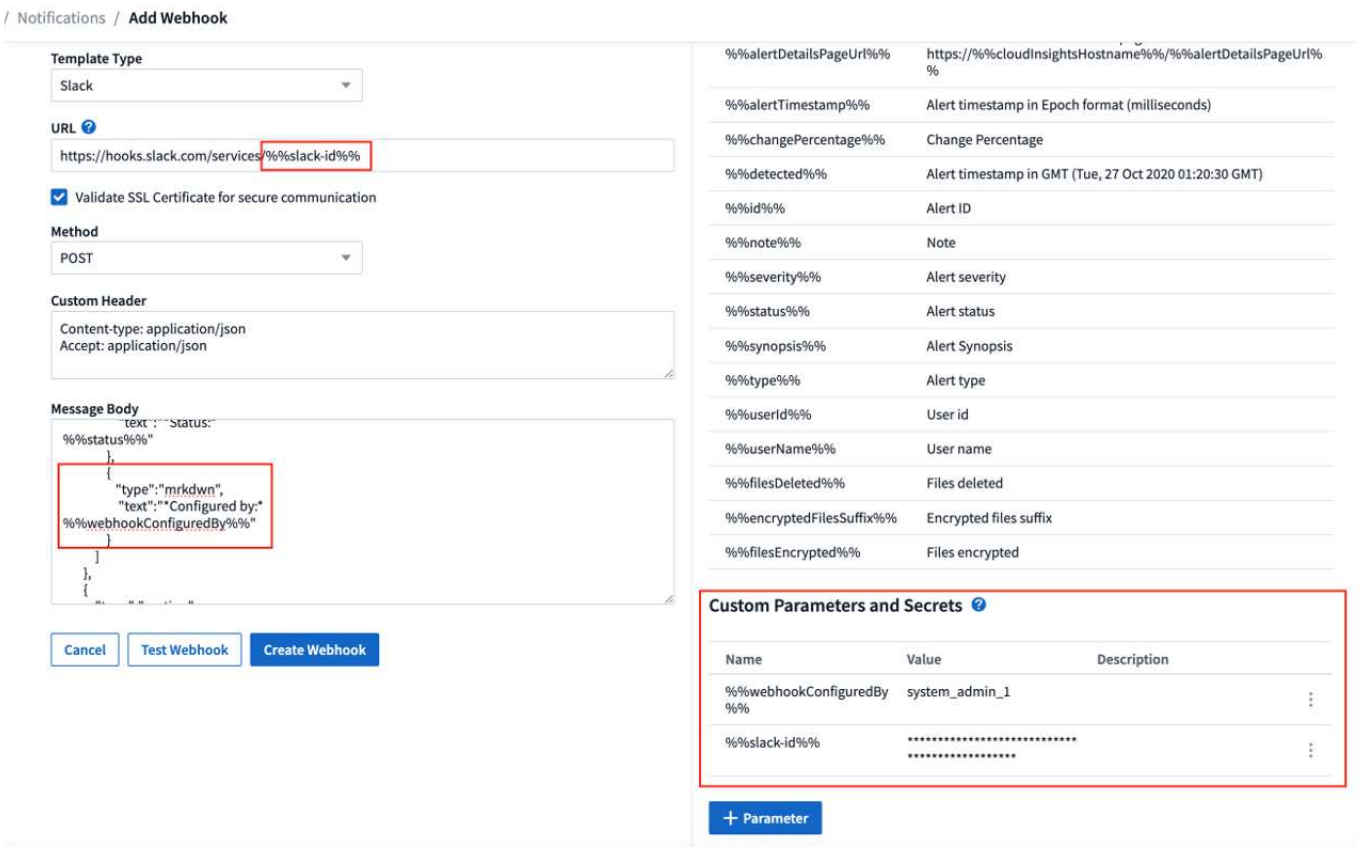
警报参数是每个警报填充的动态值。例如，*%%severity%%* 参数将被替换为警报的严重性类型。

请注意，单击“测试 Webhook”按钮时不会执行替换；测试会发送一个有效负载，显示参数的占位符（*%%<param-name>%%*），但不会用数据替换它们。

自定义参数和机密

在本节中，您可以添加任何您想要的自定义参数和/或秘密。自定义参数或秘密可以位于 URL 或消息正文中。秘密允许用户配置安全的自定义参数，如密码、apiKey 等。

下面的示例图展示了如何在 webhook 创建中使用自定义参数。



工作负载安全 **Webhook** 列表页面

Webhooks 列表页面显示名称、创建者、创建日期、状态、安全和上次报告字段。注意：'status' 列的值将根据最后一个 webhook 触发结果不断变化。以下是状态结果的示例。

状态	描述
确定	通知已成功发送。
403	禁止。
404	未找到 URL。

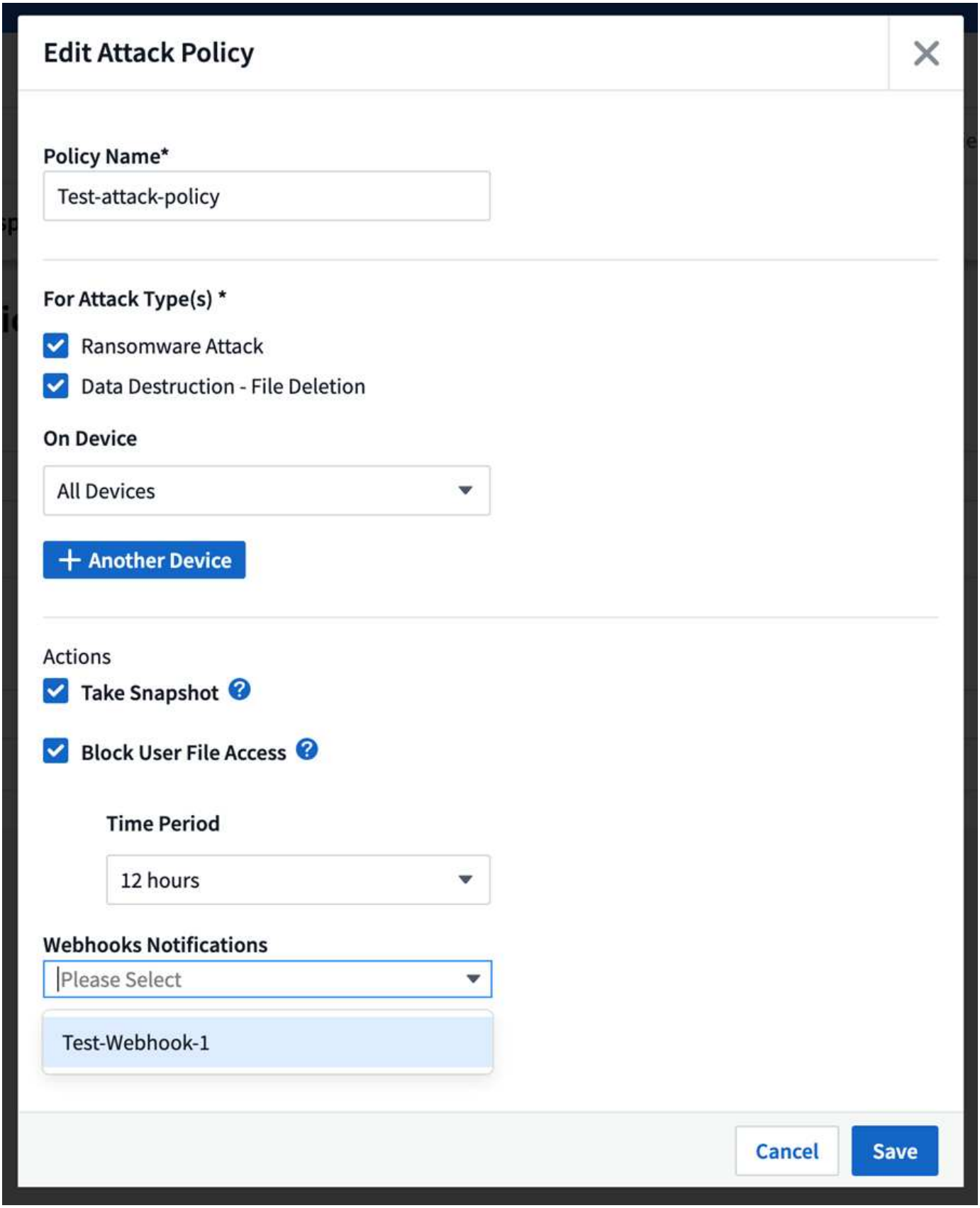
400	错误的请求。如果消息正文中存在任何错误，您可能会看到此状态，例如： • json 格式错误。 • 为保留键提供无效值。例如，PagerDuty 仅接受“严重性”为严重/警告/错误/信息。任何其他结果都可能产生 400 状态。 • 应用程序特定的验证错误。例如，Slack 允许一个部分内最多有 10 个字段。包含超过 10 个可能会导致 400 状态。
410	资源不再可用

“上次报告”列表示 webhook 上次触发的时间。

从 webhook 列表页面，用户还可以编辑/复制/删除 webhook。

在警报策略中配置 **Webhook** 通知

要将 webhook 通知添加到警报策略，请转到“工作负载安全”>“策略”，然后选择现有策略或添加新策略。在“操作”部分 > “Webhook 通知”下拉菜单中，选择所需的 webhook。



Webhook 通知与策略相关。当攻击（RW/DD/WARN）发生时，将采取配置的操作（拍摄快照/用户阻止），然后触发相关的 webhook 通知。

注意：电子邮件通知与策略无关，它们将照常触发。

- 如果策略暂停，则不会触发 webhook 通知。
- 可以将多个 webhook 附加到单个策略，但建议将不超过 5 个 webhook 附加到策略。

工作负载安全 **Webhook** 示例

Webhook 适用于"松弛"

Webhook 适用于"PagerDuty"Webhook 适用于"团队"Webhook 适用于"不和谐"

Discord 的工作负载安全 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供了为 Discord 设置 webhook 的示例。

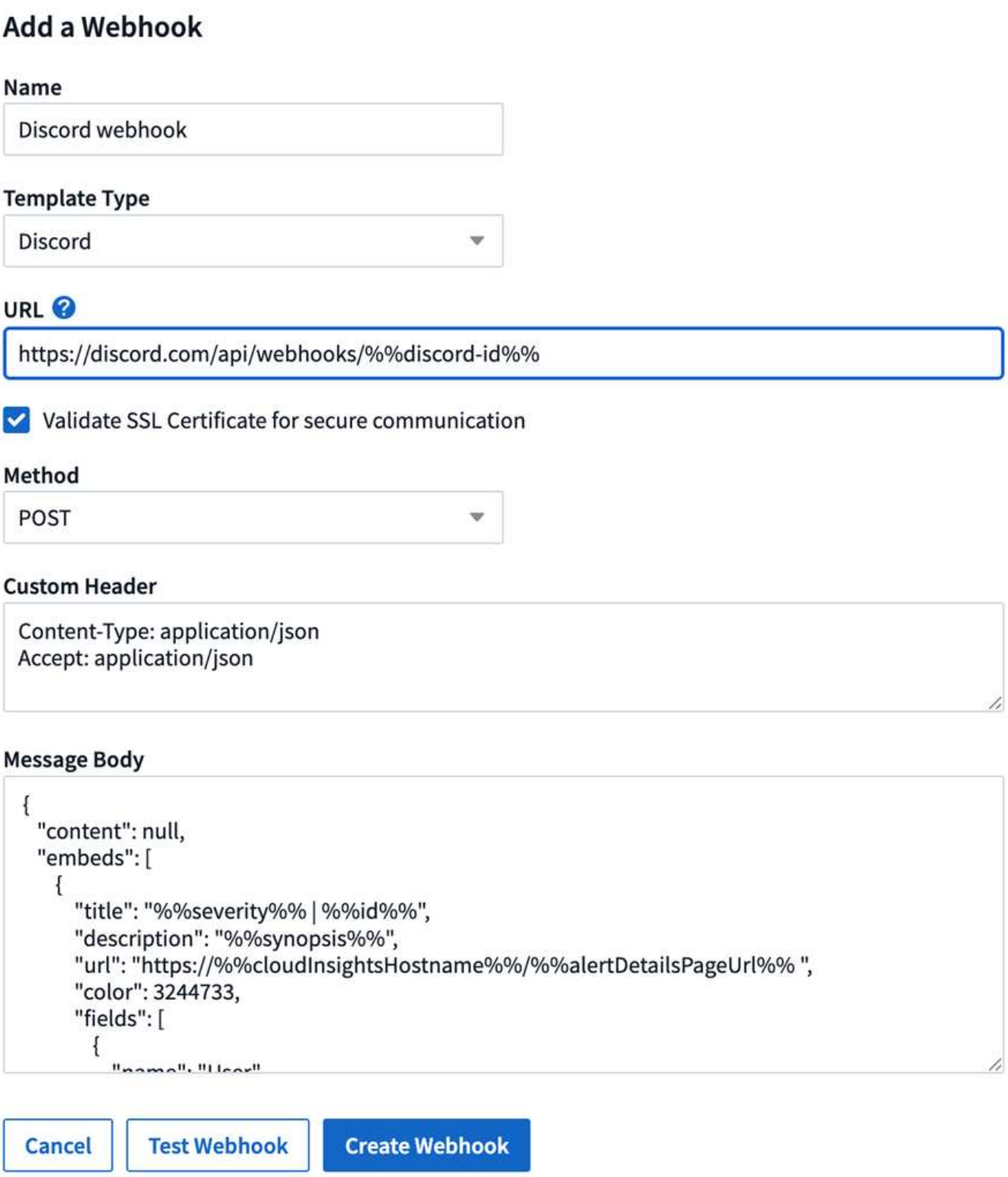
本页引用第三方说明，这些说明可能会有所变更。请参阅"Discord 文档"以获取最新信息。

Discord 设置：

- 在 Discord 中，选择服务器，在文本频道下，选择编辑频道（齿轮图标）
- 选择“集成”>“查看 Webhook”，然后单击“新建 Webhook”
- 复制 Webhook URL。您需要将其粘贴到 Workload Security webhook 配置中。

创建工作负载安全 Webhook：

1. 导航到“管理”>“通知”，然后选择“*Workload Security Webhooks*”选项卡。单击“+ Webhook”创建一个新的 webhook。
2. 为 webhook 赋予一个有意义的名称。
3. 在“模板类型”下拉菜单中，选择“Discord”。
4. 将上面的 Discord URL 粘贴到 *URL* 字段中。



为了测试 webhook，请暂时将消息正文中的 URL 值替换为任何有效的 URL（例如 *https://netapp.com*），然后单击 测试 *Webhook* 按钮。 Discord 要求提供有效的 URL 才能使测试 Webhook 功能正常工作。

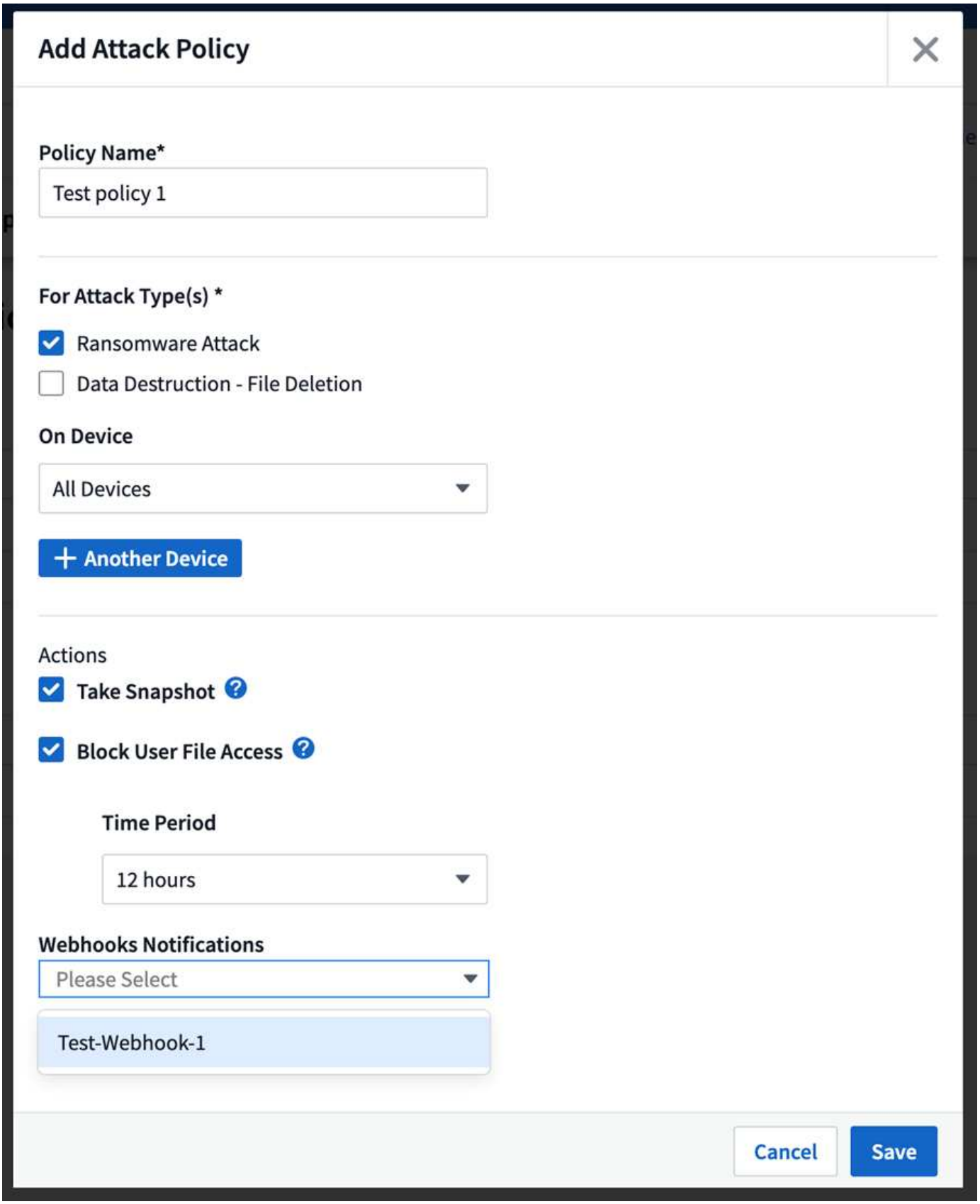
测试完成后，请务必将消息正文重新设置。

通过 **Webhook** 发送通知

要通过 webhook 通知事件，请导航至_工作负载安全 > 策略_。单击“+攻击策略”或“+警告策略”。

- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。
- 在“Webhooks Notifications”下拉菜单下，选择所需的 Discord webhook 并保存。

注意：还可以通过编辑将 Webhook 附加到现有策略。



PagerDuty 的工作负载安全 Webhook 示例

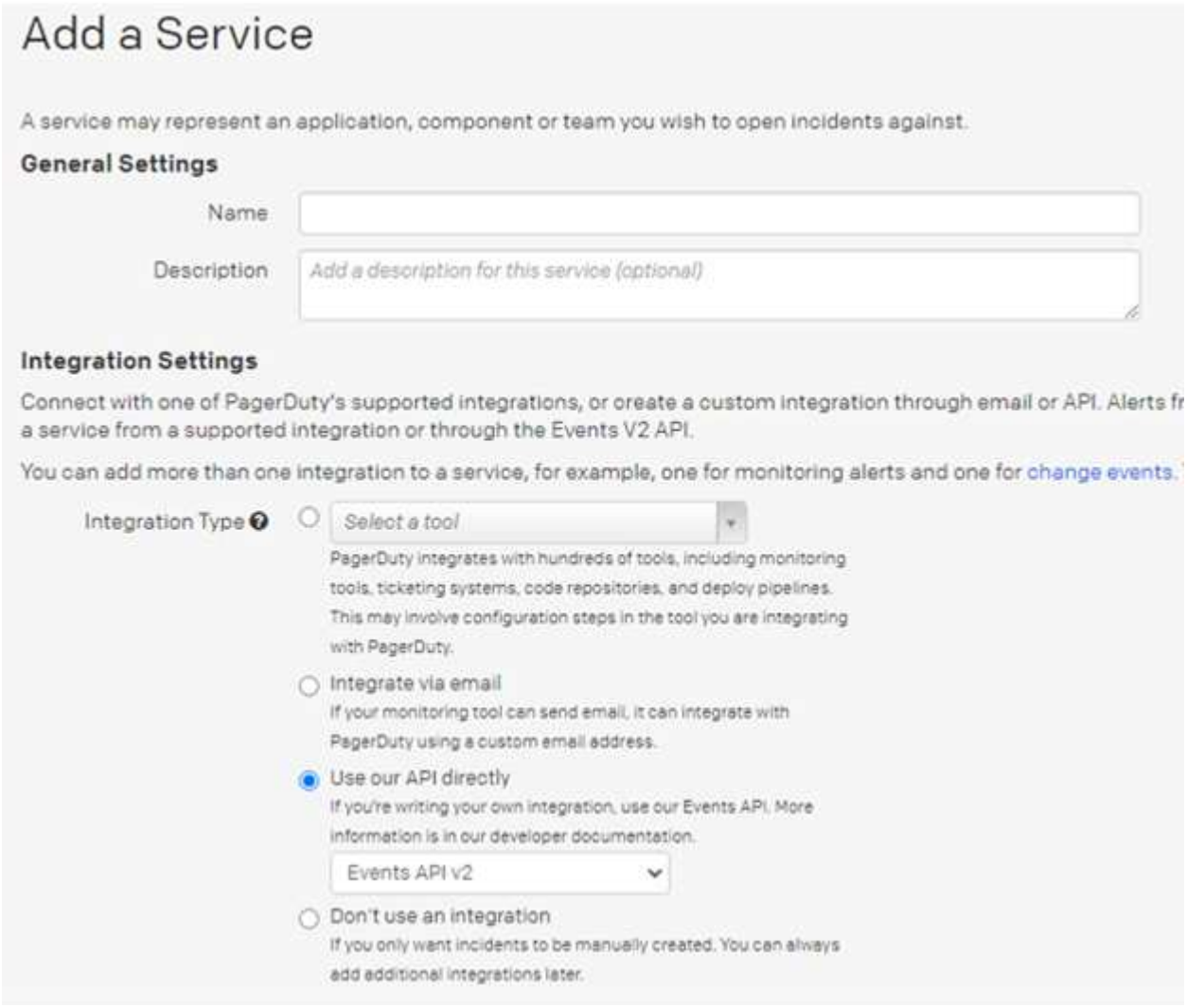
Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页面提

供了为 PagerDuty 设置 webhook 的示例。

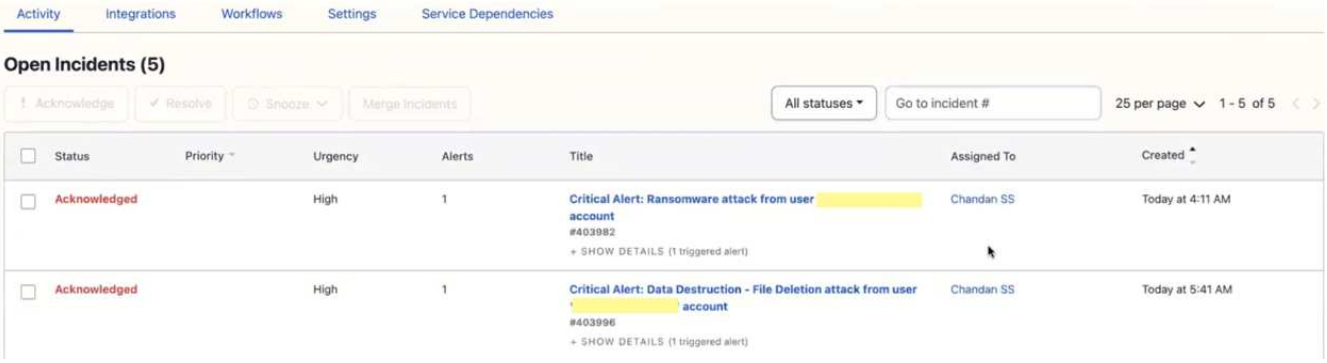
本页引用第三方说明，可能会有变更。请参阅"PagerDuty 文档"以获取最新信息。

PagerDuty 设置：

1. 在 PagerDuty 中，导航到 服务 > 服务目录 并单击 +新服务 按钮。
2. 输入_名称_并选择_直接使用我们的 API_。选择“添加服务”。

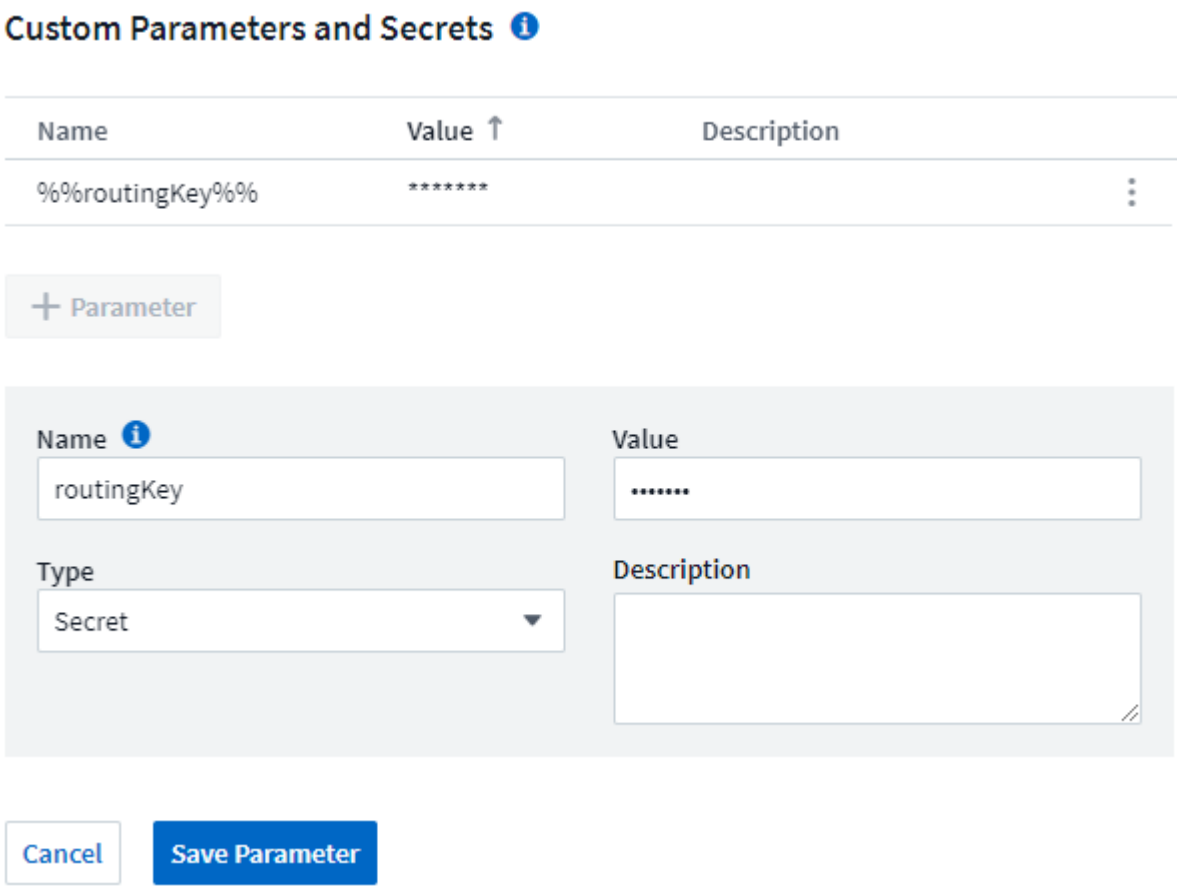


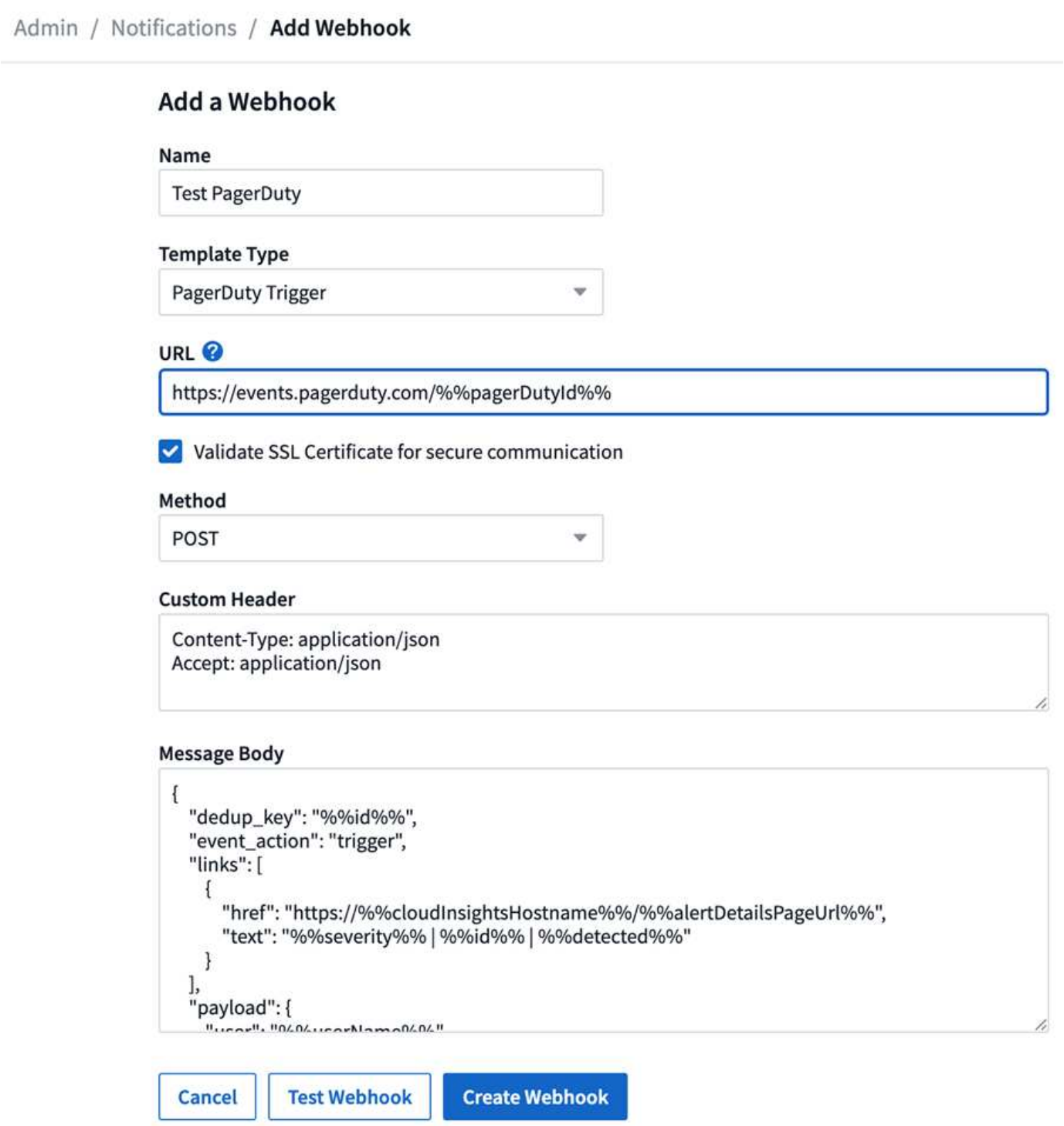
3. 选择“Integrations”选项卡来查看“Integration Key”。当您创建下面的工作负载安全 webhook 时，您将需要此密钥。
4. 前往*事件*或*服务*查看警报。



创建工作负载安全 **PagerDuty Webhook**：

- 导航到“管理”>“通知”，然后选择“*Workload Security Webhooks*”选项卡。选择“+ Webhook”来创建一个新的webhook。
- 为 webhook 赋予一个有意义的名称。
- 在“模板类型”下拉菜单中，选择“PagerDuty 触发器”。
- 创建一个名为_routingKey_的自定义参数密钥，并将其值设置为上面创建的PagerDuty_Integration Key_。

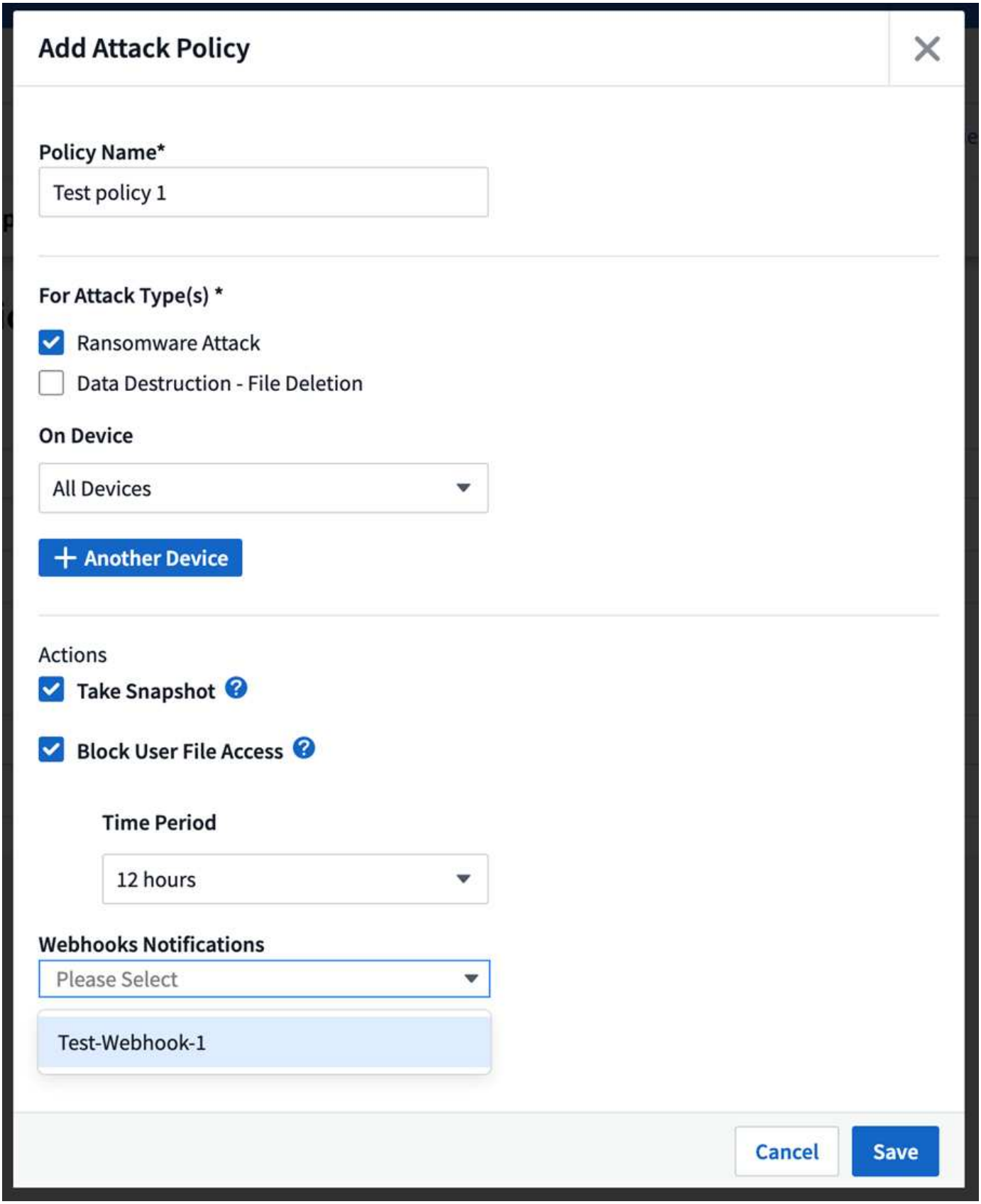




通过 **Webhook** 发送通知

- 要通过 webhook 通知事件，请导航至_工作负载安全 > 策略_。选择“+攻击策略”或“+警告策略”。
- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。
- 在“Webhooks Notifications”下拉菜单下，选择所需的 PagerDuty webhook。保存策略。

注意：还可以通过编辑将 Webhook 附加到现有策略。



Slack 的工作负载安全 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供

了为 Slack 设置 webhook 的示例。

本页引用第三方说明，可能会有变更。请参阅 Slack 文档以获取最新信息。

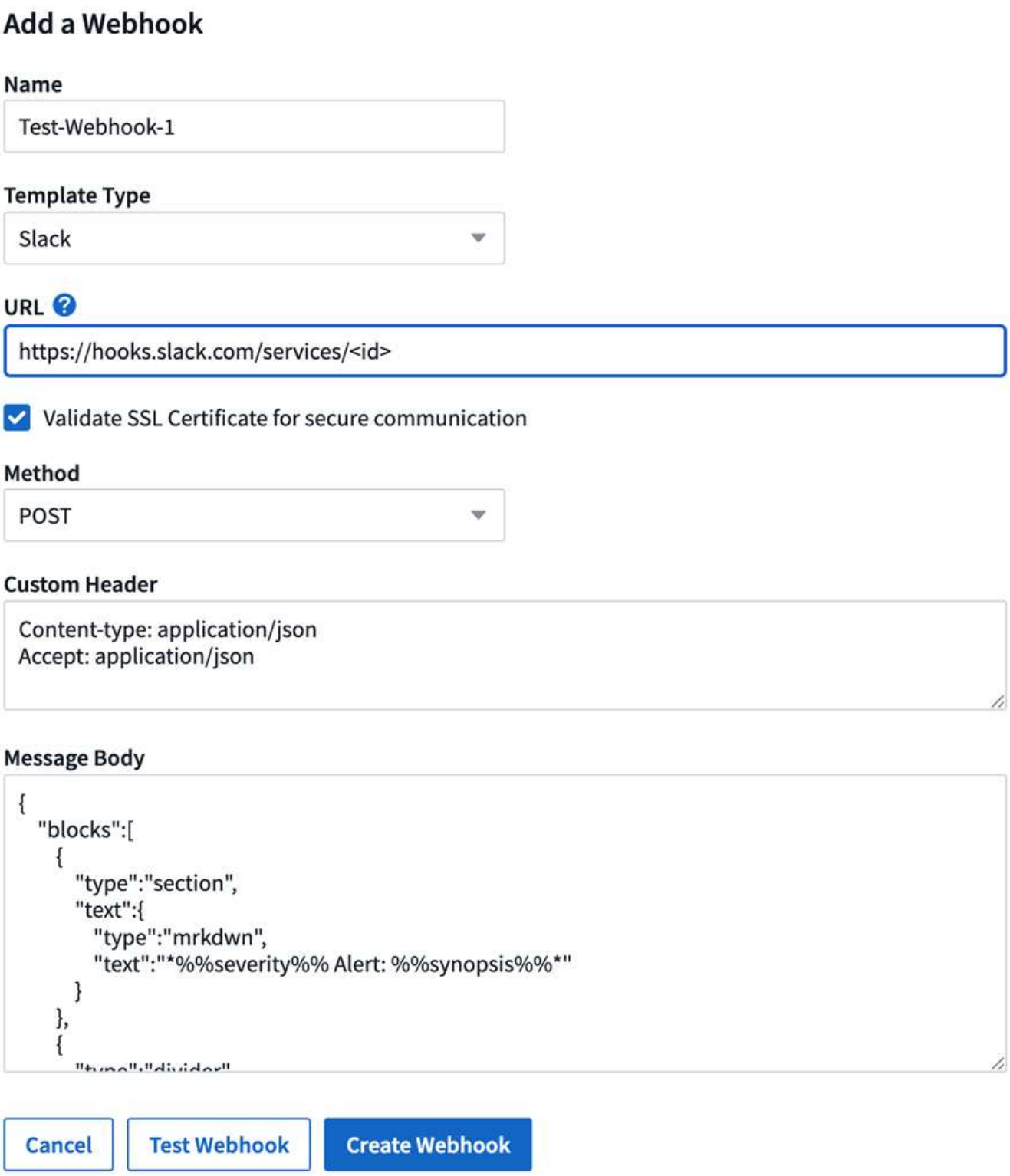
Slack 示例

- 前往 https://api.slack.com/apps并创建一个新的应用程序。给它一个有意义的名字并选择一个工作区。

- 转到传入 Webhook，单击_激活传入 Webhook_，选择_添加新 Webhook_，然后选择要发布的频道。
- 复制 Webhook URL。创建工作负载安全 webhook 时将提供此 URL。

创建工作负载安全 **Slack Webhook**

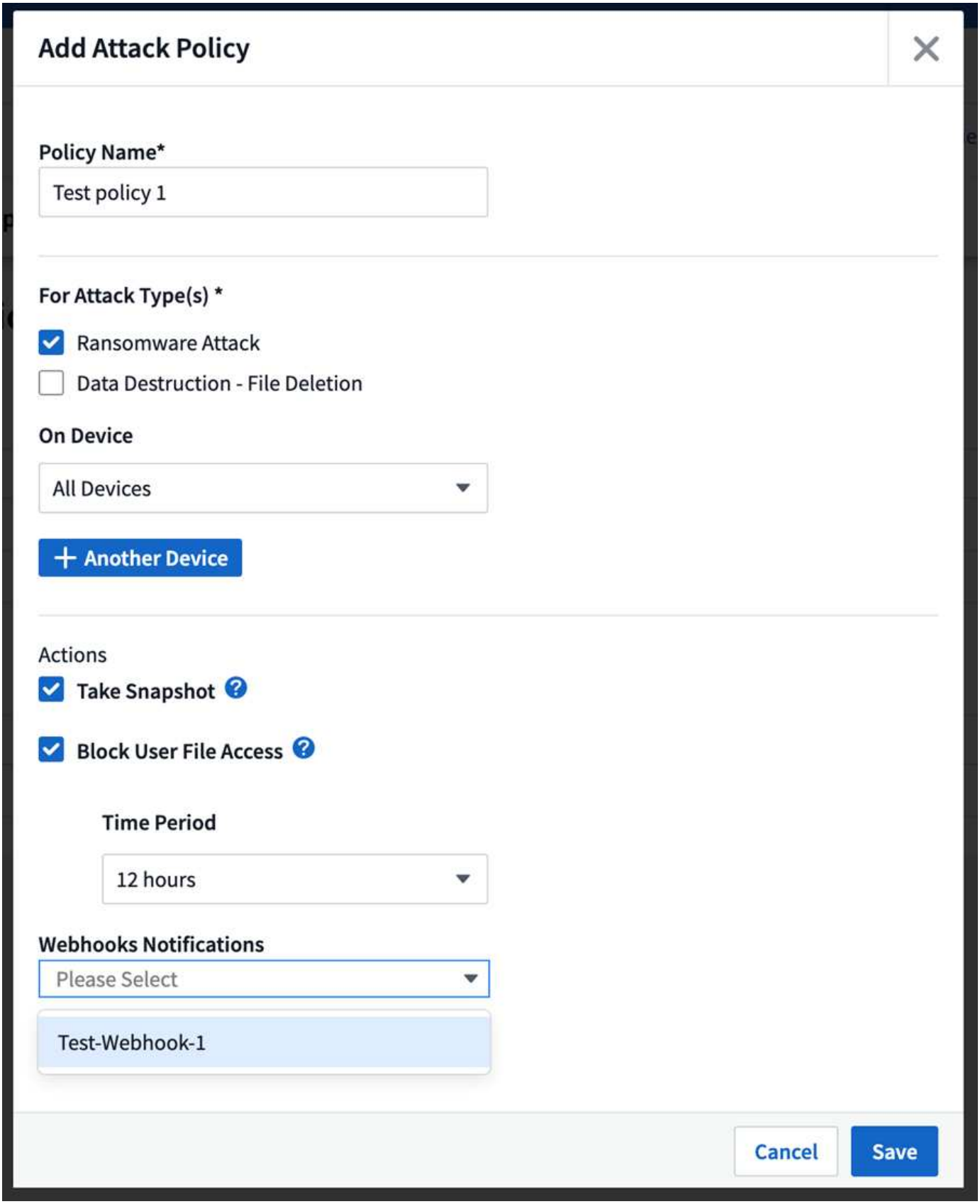
1. 导航到“管理”>“通知”，然后选择“*Workload Security Webhooks*”选项卡。选择 + *Webhook* 来创建一个新的 webhook。
2. 为 webhook 赋予一个有意义的名称。
3. 在“模板类型”下拉菜单中，选择“Slack”。
4. 粘贴从上面复制的 URL。



通过 **webhook** 发送通知

- 要通过 webhook 通知事件，请导航至_工作负载安全 > 策略_。单击“+攻击策略”或“+警告策略”。
- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。
- 在“Webhooks Notifications”下拉菜单下，选择所需的 webhook。保存策略。

注意：还可以通过编辑将 Webhook 附加到现有策略。



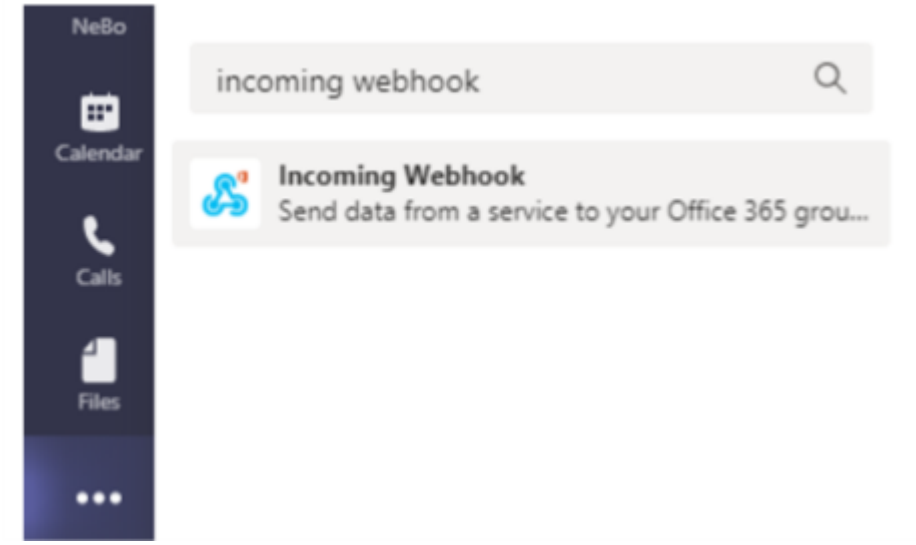
Microsoft Teams 的工作负载安全 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供了为 Teams 设置 webhook 的示例。

本页引用第三方说明，可能会有变更。请参阅"团队文档"以获取最新信息。

团队设置：

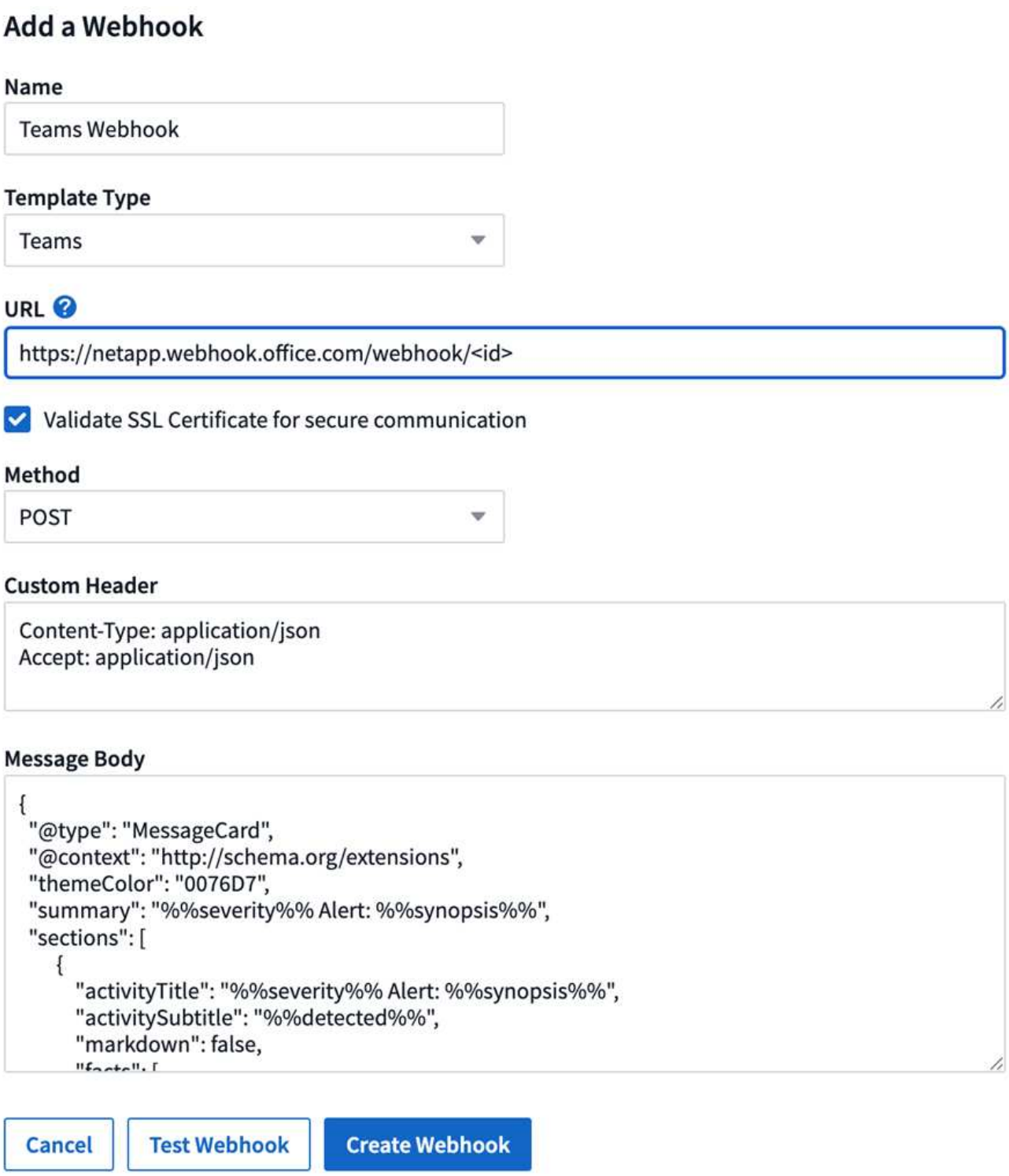
1. 在 Teams 中，选择 kebab，然后搜索 Incoming Webhook。



2. 选择*添加到团队>选择团队>设置连接器*。
3. 复制 Webhook URL。您需要将其粘贴到 Workload Security webhook 配置中。

创建工作负载安全团队 Webhook：

1. 导航到“管理”>“通知”，然后选择“工作负载安全 Webhooks”选项卡。选择 + *Webhook* 来创建一个新的 webhook。
2. 为 webhook 赋予一个有意义的名称。
3. 在“模板类型”下拉菜单中，选择“团队”。



4. 将上面的 URL 粘贴到 *URL* 字段中。

通过 **Webhook** 发送通知

要通过 webhook 通知事件，请导航至_工作负载安全 > 策略_。选择“+攻击策略”或“+警告策略”。

- 输入一个有意义的策略名称。
- 选择所需的攻击类型、应附加策略的设备以及所需的操作。

- 在“Webhooks Notifications”下拉菜单下，选择所需的 Teams webhook。保存策略。

注意：还可以通过编辑将 Webhook 附加到现有策略。