웹훅 알림

Data Infrastructure Insights

NetApp
February 11, 2026

목차

웹훅 알림

웹후크를 사용한 워크로드 보안 알림

웹후크를 사용하면 사용자는 사용자 정의된 웹후크 채널을 사용하여 다양한 애플리케이션에 중요하거나 경고 알림 메시지를 보낼 수 있습니다.

Slack, PagerDuty, Teams, Discord 등 많은 상업용 애플리케이션은 표준 입력 인터페이스로 웹훅을 지원합니다. Workload Security는 일반적이고 사용자 정의 가능한 웹훅 채널을 지원함으로써 이러한 다양한 전달 채널을 지원할 수 있습니다. 웹후크 구성에 대한 정보는 해당 애플리케이션 웹사이트에서 확인할 수 있습니다. 예를 들어 Slack은 다음을 제공합니다."이 유용한 가이드" .

여러 개의 웹훅 채널을 만들 수 있으며, 각 채널은 다른 목적, 별도의 애플리케이션, 다른 수신자 등을 대상으로 합니다.

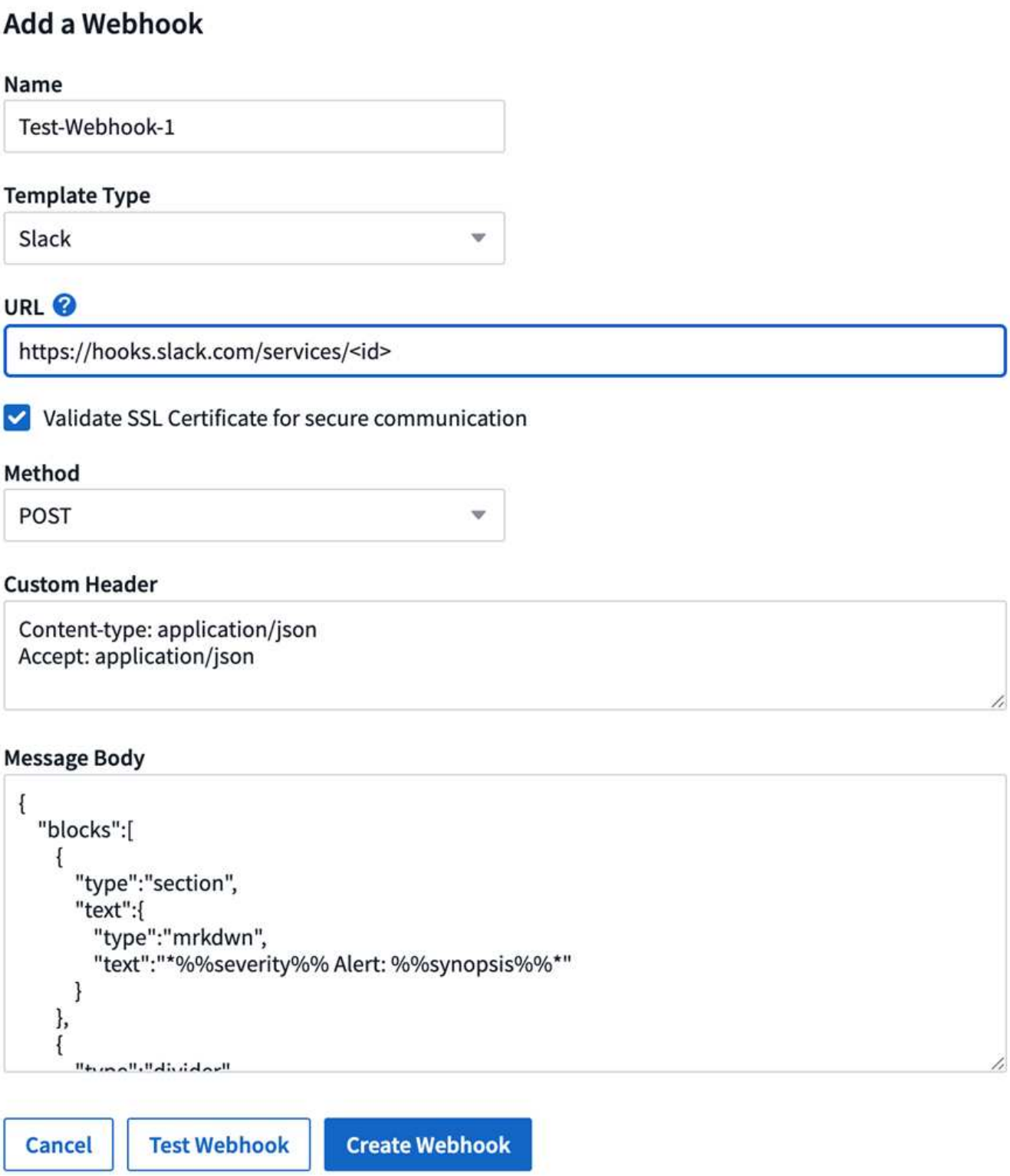
웹훅 채널 인스턴스는 다음 요소로 구성됩니다.

이름	설명
URL	URL 매개변수와 함께 http:// 또는 https:// 접두사를 포함한 웹훅 대상 URL
방법	GET/POST - 기본값은 POST입니다.
사용자 정의 헤더	여기에 사용자 정의 헤더를 지정하세요
메시지 본문	여기에 메시지 본문을 입력하세요
기본 알림 매개변수	웹훅의 기본 매개변수를 나열합니다.
사용자 정의 매개변수 및 비밀	사용자 정의 매개변수 및 비밀을 사용하면 비밀번호와 같은 고유한 매개변수 및 보안 요소를 추가할 수 있습니다.

웹훅 만들기

워크로드 보안 웹훅을 생성하려면 관리 > 알림으로 이동하여 "워크로드 보안 웹훅" 탭을 선택하세요. 다음 이미지는 Slack 웹훅 생성 화면의 샘플을 보여줍니다.

참고: Workload Security Webhook을 생성하고 관리하려면 사용자는 Workload Security _Admin_이어야 합니다.



- 각 필드에 적절한 정보를 입력하고 "저장"을 클릭하세요.
- "웹훅 테스트" 버튼을 클릭하여 연결을 테스트할 수도 있습니다. 이렇게 하면 선택된 방법에 따라 정의된 URL로 "메시지 본문"(대체 없음)이 전송됩니다.
- SWS 웹훅은 여러 개의 기본 매개변수로 구성됩니다. 또한, 사용자 정의 매개변수나 비밀번호를 직접 만들 수도 있습니다.

매개변수: 매개변수란 무엇이고 어떻게 사용하나요?

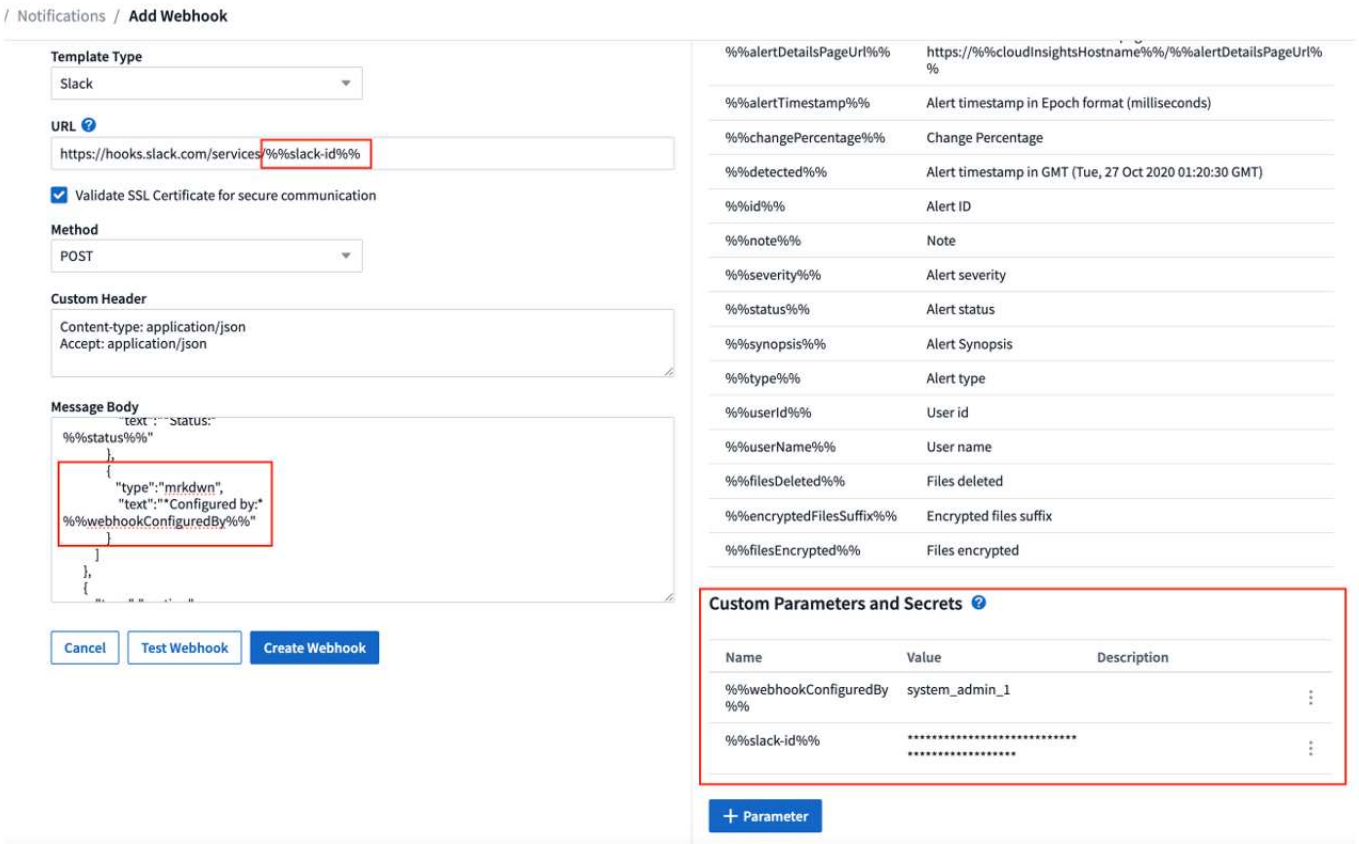
알림 매개변수는 알림마다 채워지는 동적 값입니다. 예를 들어, *%%severity%%* 매개변수는 경고의 심각도 유형으로 대체됩니다.

"웹후크 테스트" 버튼을 클릭해도 대체가 수행되지 않는다는 점에 유의하세요. 테스트는 매개변수의 플레이스홀더(*%%<param-name>%%*)를 보여주는 페이로드를 전송하지만 이를 데이터로 바꾸지는 않습니다.

사용자 정의 매개변수 및 비밀

이 섹션에서는 원하는 사용자 정의 매개변수 및/또는 비밀번호를 추가할 수 있습니다. 사용자 정의 매개변수나 비밀번호는 URL이나 메시지 본문에 포함될 수 있습니다. 비밀을 사용하면 사용자가 비밀번호, API 키 등과 같은 안전한 사용자 정의 매개변수를 구성할 수 있습니다.

다음 샘플 이미지는 사용자 정의 매개변수가 웹훅 생성에 어떻게 사용되는지 보여줍니다.



워크로드 보안 웹훅 목록 페이지

웹후크 목록 페이지에는 이름, 생성자, 생성일, 상태, 보안 및 마지막 보고 필드가 표시됩니다. 참고: '상태' 열의 값은 마지막 웹훅 트리거 결과에 따라 계속 변경됩니다. 다음은 상태 결과의 예입니다.

상태	설명
OK	알림이 성공적으로 전송되었습니다.
403	금지됨.
404	URL을 찾을 수 없습니다.

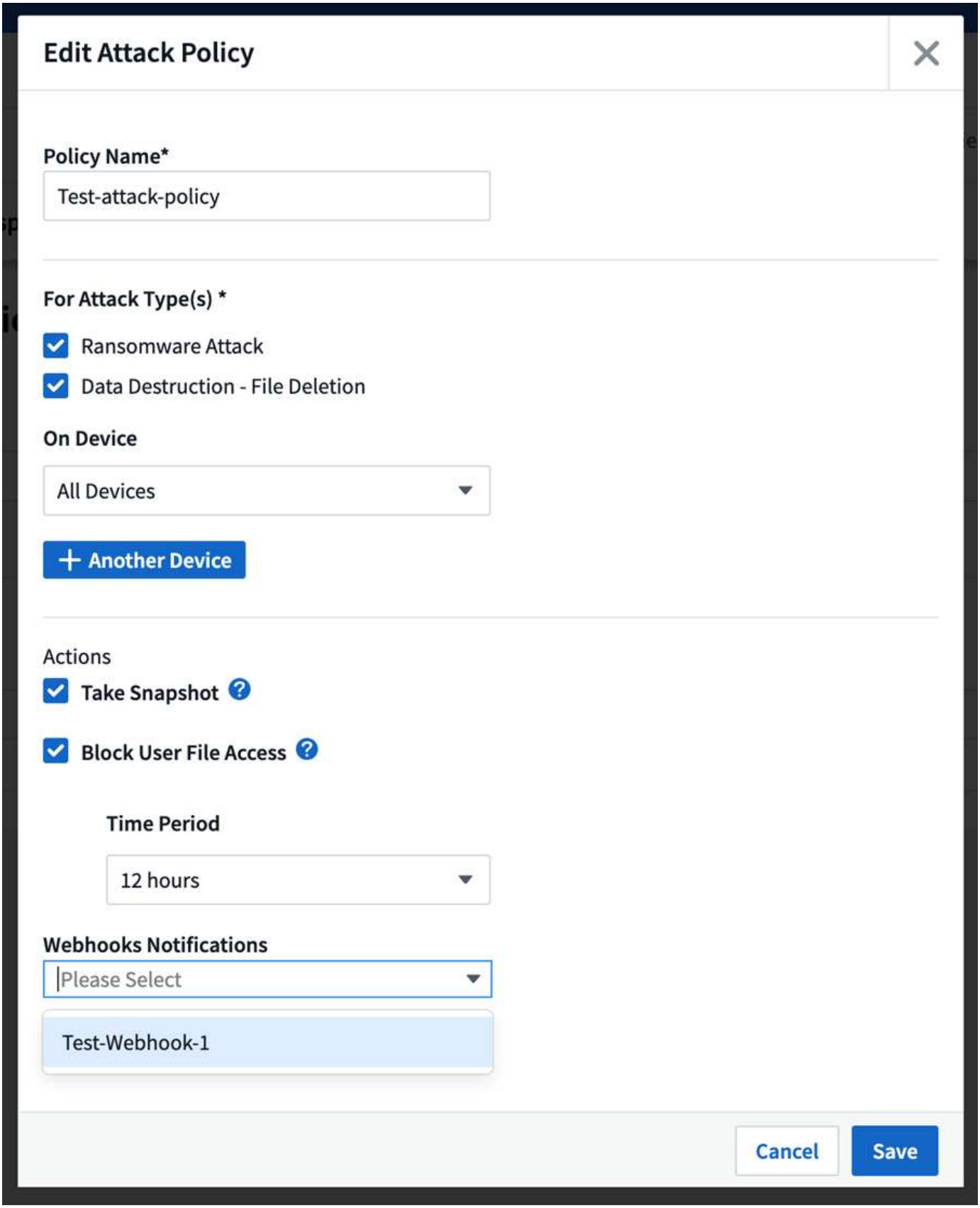
400	잘못된 요청입니다. 메시지 본문에 다음과 같은 오류가 있는 경우 이 상태가 표시될 수 있습니다. • 형식이 잘못된 JSON입니다. • 예약된 키에 잘못된 값을 제공했습니다. 예를 들어, PagerDuty는 "심각도"에 대해 중요/경고/오류/정보만 허용합니다. 다른 결과는 400 상태를 나타낼 수 있습니다. • 애플리케이션별 검증 오류. 예를 들어, Slack은 섹션 내에 최대 10개의 필드를 허용합니다. 10개 이상을 포함하면 400 상태가 될 수 있습니다.
410	더 이상 리소스를 사용할 수 없습니다.

"마지막 보고" 열은 웹훅이 마지막으로 트리거된 시간을 나타냅니다.

웹후크 목록 페이지에서 사용자는 웹후크를 편집/복제/삭제할 수도 있습니다.

알림 정책에서 **Webhook** 알림 구성

알림 정책에 웹훅 알림을 추가하려면 -워크로드 보안 > 정책-으로 이동하여 기존 정책을 선택하거나 새 정책을 추가합니다. 작업 섹션 > 웹훅 알림 드롭다운에서 필요한 웹훅을 선택합니다.



웹훅 알림은 정책에 연결됩니다. 공격(RW/DD/WARN)이 발생하면 구성된 작업(스냅샷 촬영/사용자 차단)이 수행되고 관련 웹훅 알림이 트리거됩니다.

참고: 이메일 알림은 정책과 무관하며 평소와 같이 트리거됩니다.

- 정책이 일시 중지되면 웹후크 알림이 트리거되지 않습니다.
- 하나의 정책에 여러 개의 웹훅을 첨부할 수 있지만 정책에 5개 이상의 웹훅을 첨부하지 않는 것이 좋습니다.

워크로드 보안 웹훅 예제

웹후크"느슨하게"

웹후크"페이저듀티" 웹후크"팀" 웹후크"불화"

Discord를 위한 워크로드 보안 웹훅 예시

웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을 보낼 수 있습니다. 이 페이지에서는 Discord에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

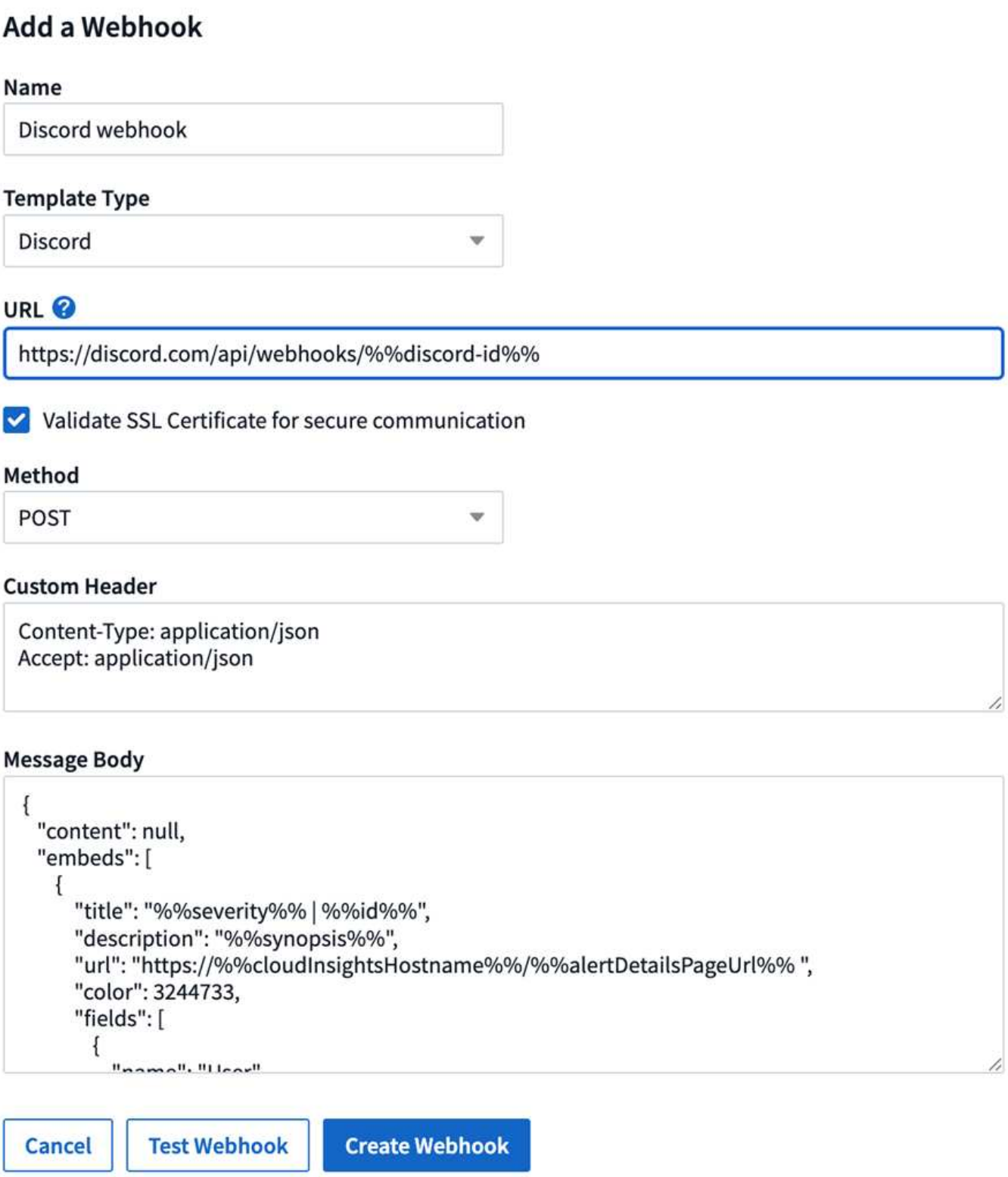
이 페이지는 제3자 지침을 참조하며, 해당 지침은 변경될 수 있습니다. 를 참조하세요"Discord 문서" 최신 정보를 확인하세요.

Discord 설정:

- Discord에서 서버를 선택하고 텍스트 채널 아래에서 채널 편집(기어 아이콘)을 선택합니다.
- *통합 > 웹훅 보기*를 선택하고 *새 웹훅*을 클릭합니다.
- Webhook URL을 복사합니다. 이것을 Workload Security 웹훅 구성에 붙여넣어야 합니다.

워크로드 보안 웹훅 생성:

1. 관리 > 알림으로 이동하여 워크로드 보안 웹훅 탭을 선택합니다. 새로운 웹훅을 만들려면 '+ 웹훅'을 클릭하세요.
2. 웹훅에 의미 있는 이름을 지정하세요.
3. 템플릿 유형 드롭다운에서 *Discord*를 선택합니다.
4. 위의 Discord URL을 *URL* 필드에 붙여넣습니다.



웹훅을 테스트하려면 메시지 본문의 URL 값을 유효한 URL(예: https://netapp.com)로 임시로 바꾼 다음 웹훅 테스트 버튼을 클릭합니다. Discord에서는 Test Webhook 기능이 작동하려면 유효한 URL을 제공해야 합니다.

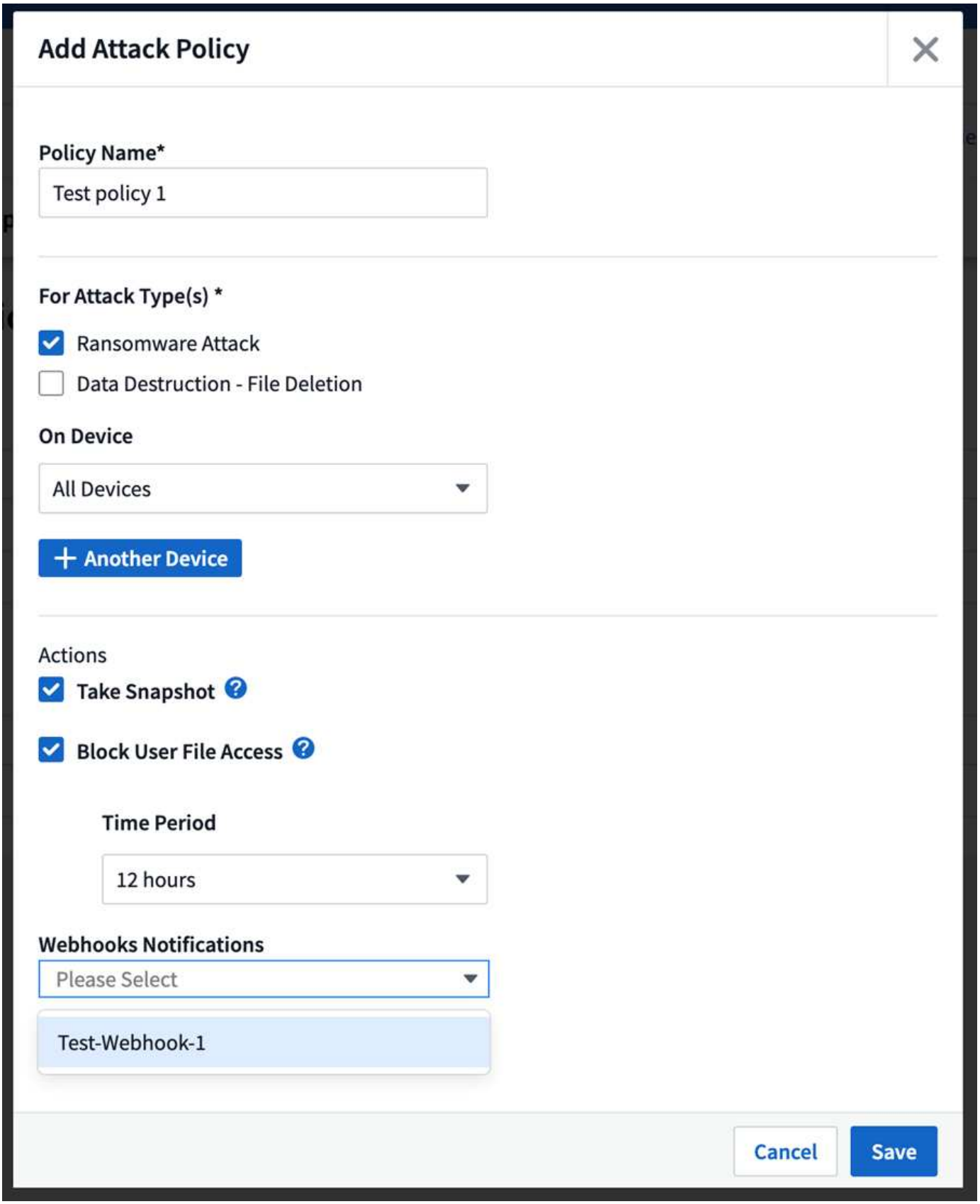
테스트가 완료되면 메시지 본문을 원래대로 설정하세요.

Webhook을 통한 알림

웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 클릭하세요.

- 의미 있는 정책 이름을 입력하세요.
- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.
- 웹훅 알림 드롭다운에서 필요한 Discord 웹훅을 선택하고 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.



PagerDuty를 위한 워크로드 보안 웹훅 예제

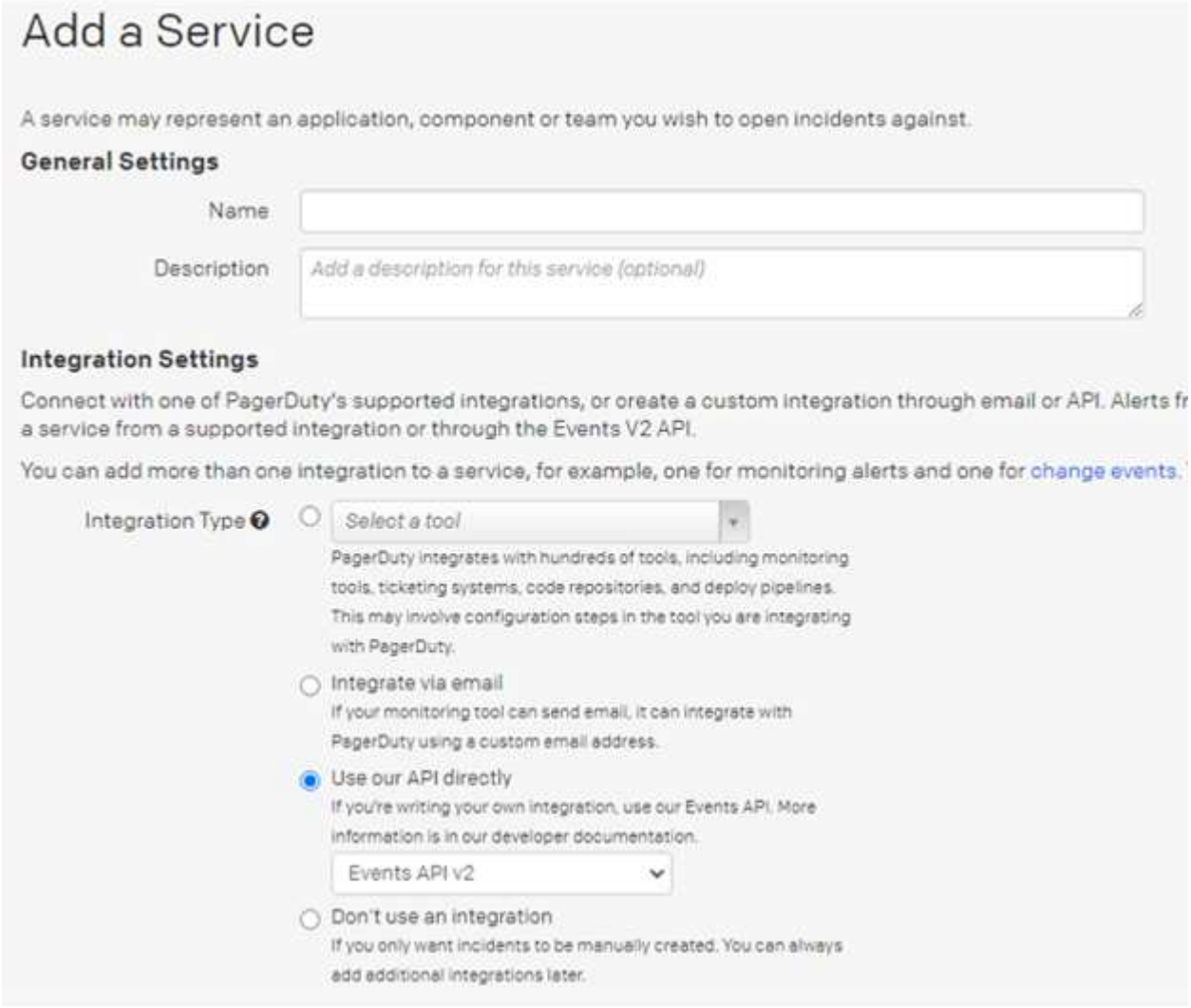
웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을

보낼 수 있습니다. 이 페이지에서는 PagerDuty에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

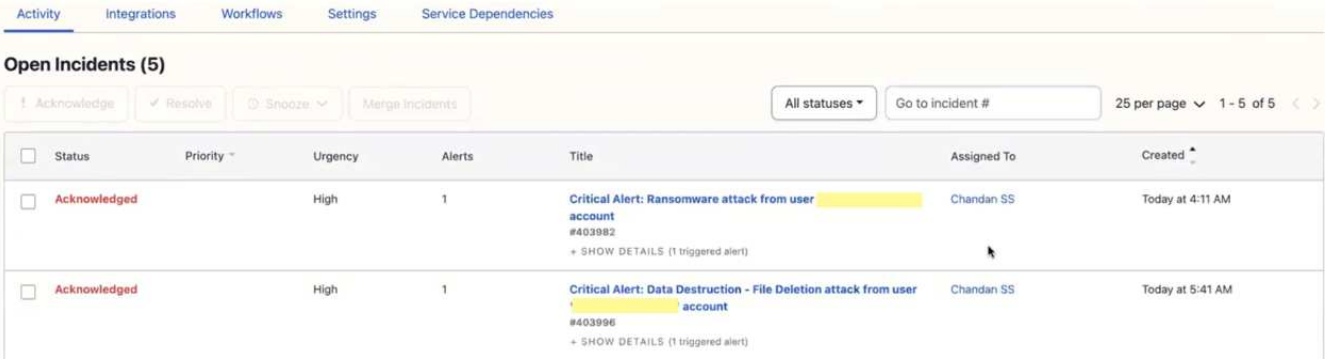
이 페이지는 변경될 수 있는 제3자 지침을 참조합니다. 를 참조하세요"PagerDuty 문서" 최신 정보를 확인하세요.

PagerDuty 설정:

1. PagerDuty에서 서비스 > 서비스 디렉터리*로 이동한 다음 *+새 서비스 버튼을 클릭합니다.
2. _이름_을 입력하고 _API를 직접 사용_을 선택하세요. _서비스 추가_를 선택하세요.

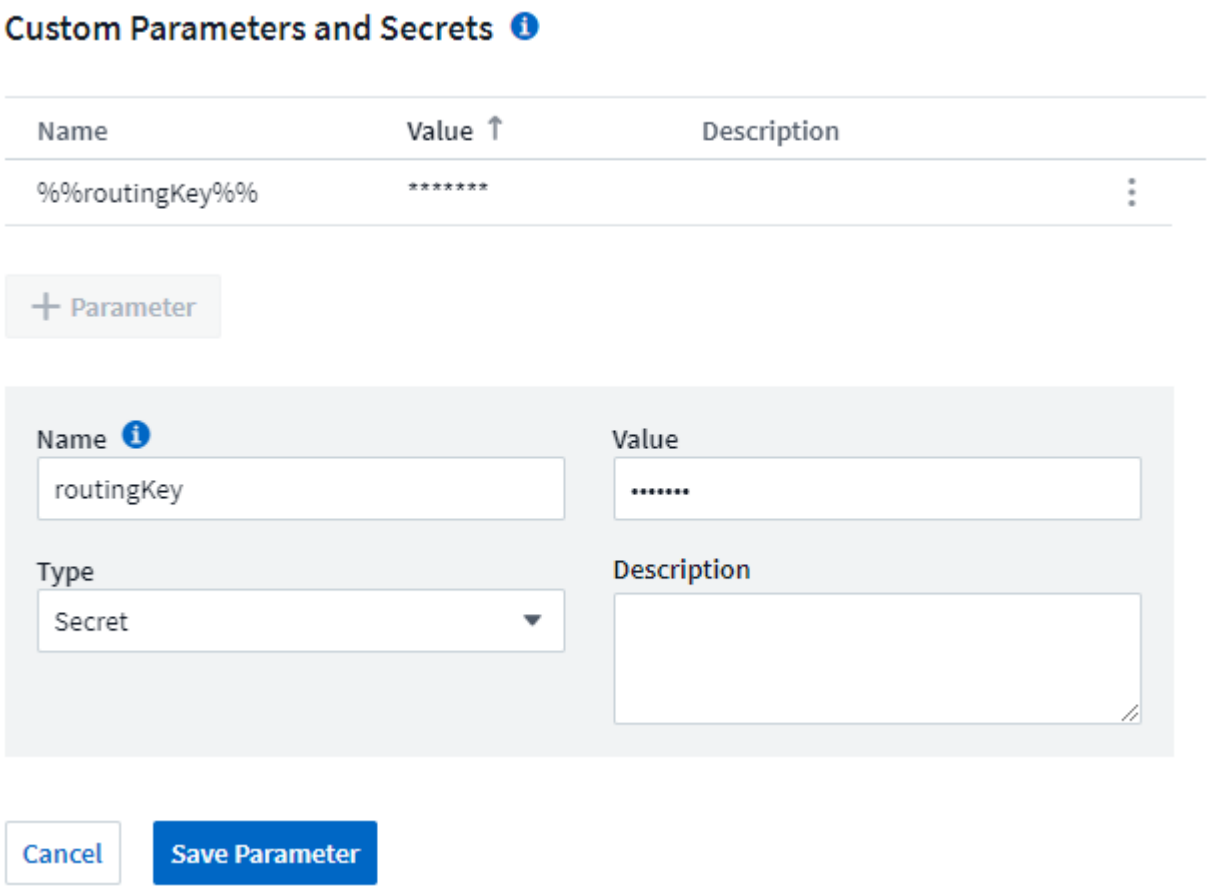


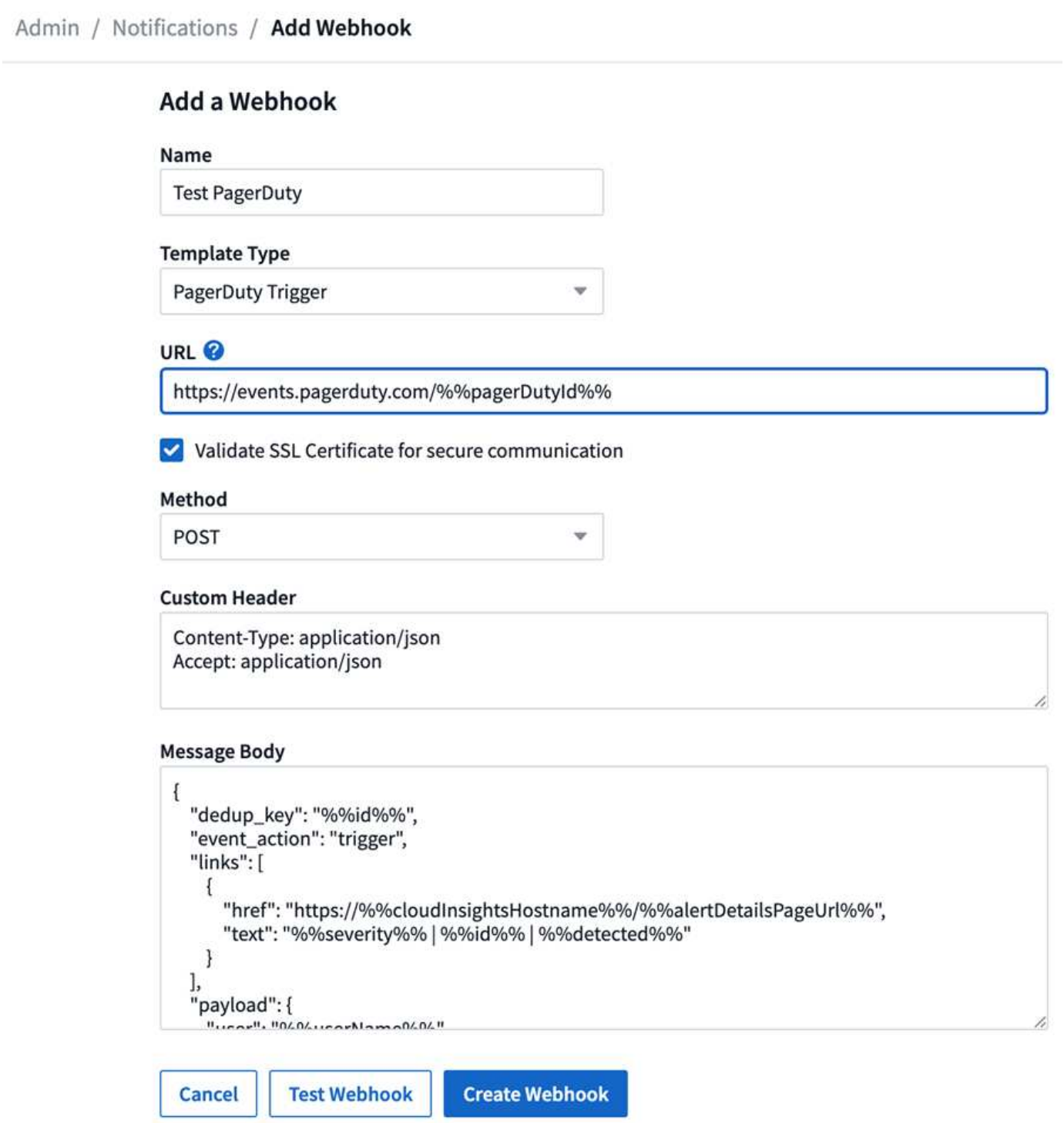
3. 통합 탭을 선택하여 *통합 키*를 확인하세요. 아래의 워크로드 보안 웹후크를 생성할 때 이 키가 필요합니다.
4. 알림을 보려면 사건 또는 *서비스*로 이동하세요.



워크로드 보안 **PagerDuty** 웹훅 생성:

- 관리 > 알림으로 이동하여 워크로드 보안 웹훅 탭을 선택합니다. 새로운 웹훅을 만들려면 '+ 웹훅'을 선택하세요.
- 웹훅에 의미 있는 이름을 지정하세요.
- 템플릿 유형 드롭다운에서 _PagerDuty Trigger_를 선택합니다.
- _routingKey_라는 사용자 지정 매개변수 비밀번호를 만들고 값을 위에서 만든 PagerDuty _Integration Key_로 설정합니다.

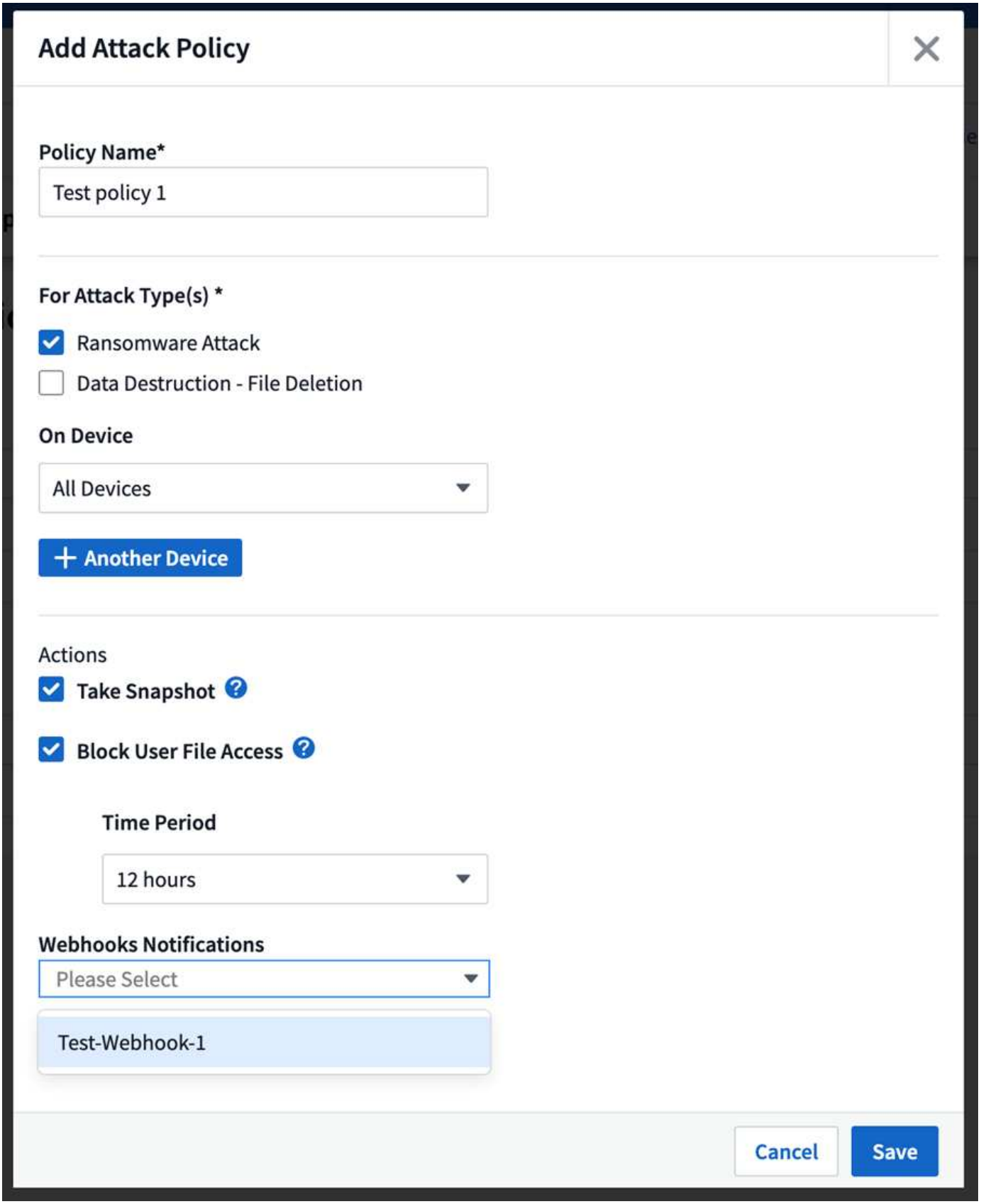




Webhook을 통한 알림

- 웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 선택하세요.
- 의미 있는 정책 이름을 입력하세요.
- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.
- 웹훅 알림 드롭다운에서 필요한 PagerDuty 웹훅을 선택합니다. 정책을 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.



Slack을 위한 워크로드 보안 웹훅 예시

웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을 보낼 수 있습니다. 이 페이지에서는 Slack에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

이 페이지는 변경될 수 있는 제3자 지침을 참조합니다. 최신 정보는 Slack 문서를 참조하세요.

슬랙 예시

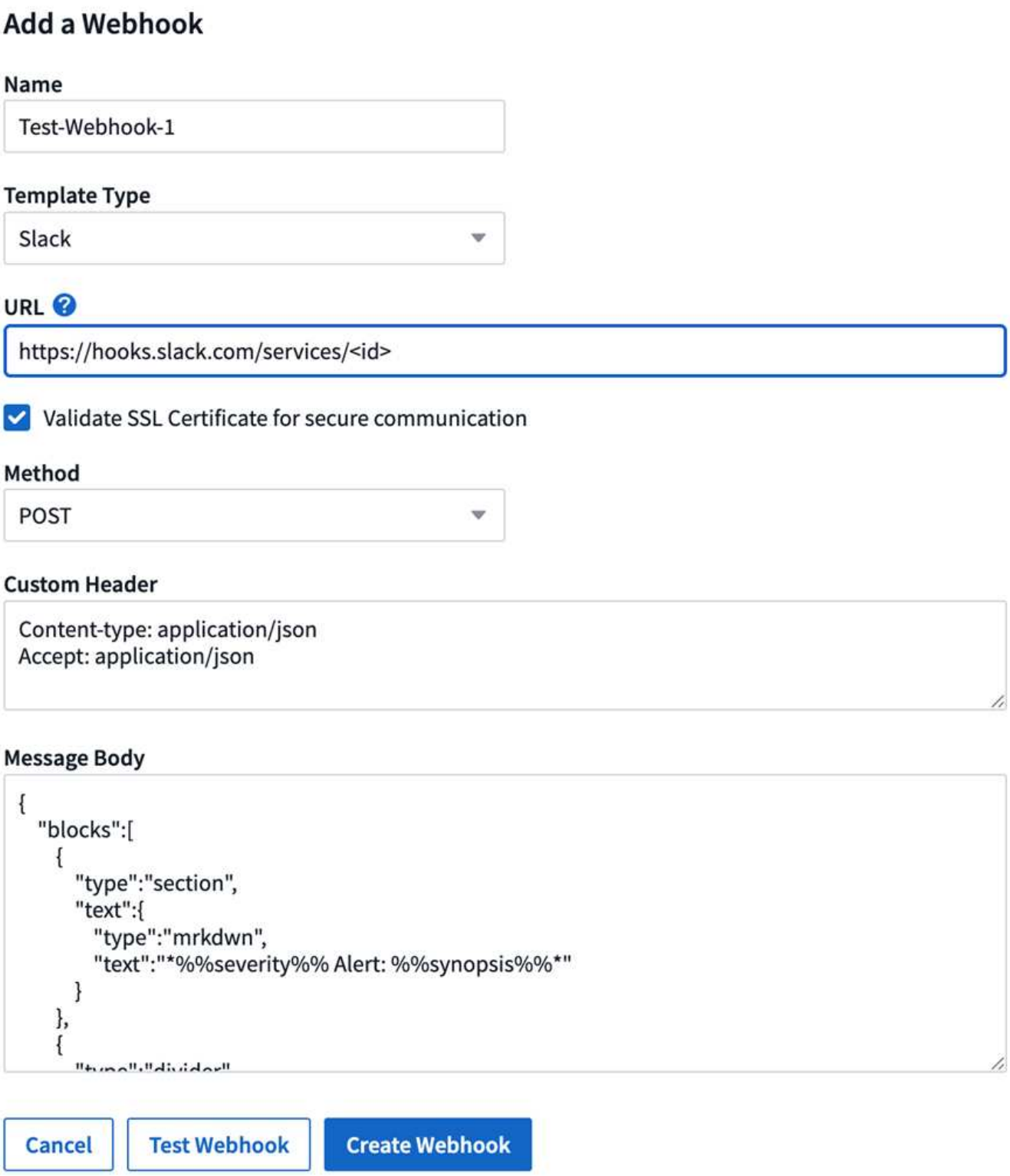
- 로 가다 https://api.slack.com/apps 새로운 앱을 만드세요. 의미 있는 이름을 지정하고 작업 공간을 선택하세요.

- 수신 웹훅으로 이동하여 _수신 웹훅 활성화_를 클릭하고 _새 웹훅 추가_를 선택한 다음 게시할 채널을 선택합니다.

- Webhook URL을 복사합니다. 이 URL은 워크로드 보안 웹훅을 생성할 때 제공됩니다.

워크로드 보안 **Slack** 웹훅 만들기

1. 관리 > 알림으로 이동하여 워크로드 보안 웹훅 탭을 선택합니다. _+ Webhook_을 선택하여 새 웹훅을 만듭니다.
2. 웹훅에 의미 있는 이름을 지정하세요.
3. 템플릿 유형 드롭다운에서 _Slack_을 선택합니다.
4. 위에서 복사한 URL을 붙여넣으세요.

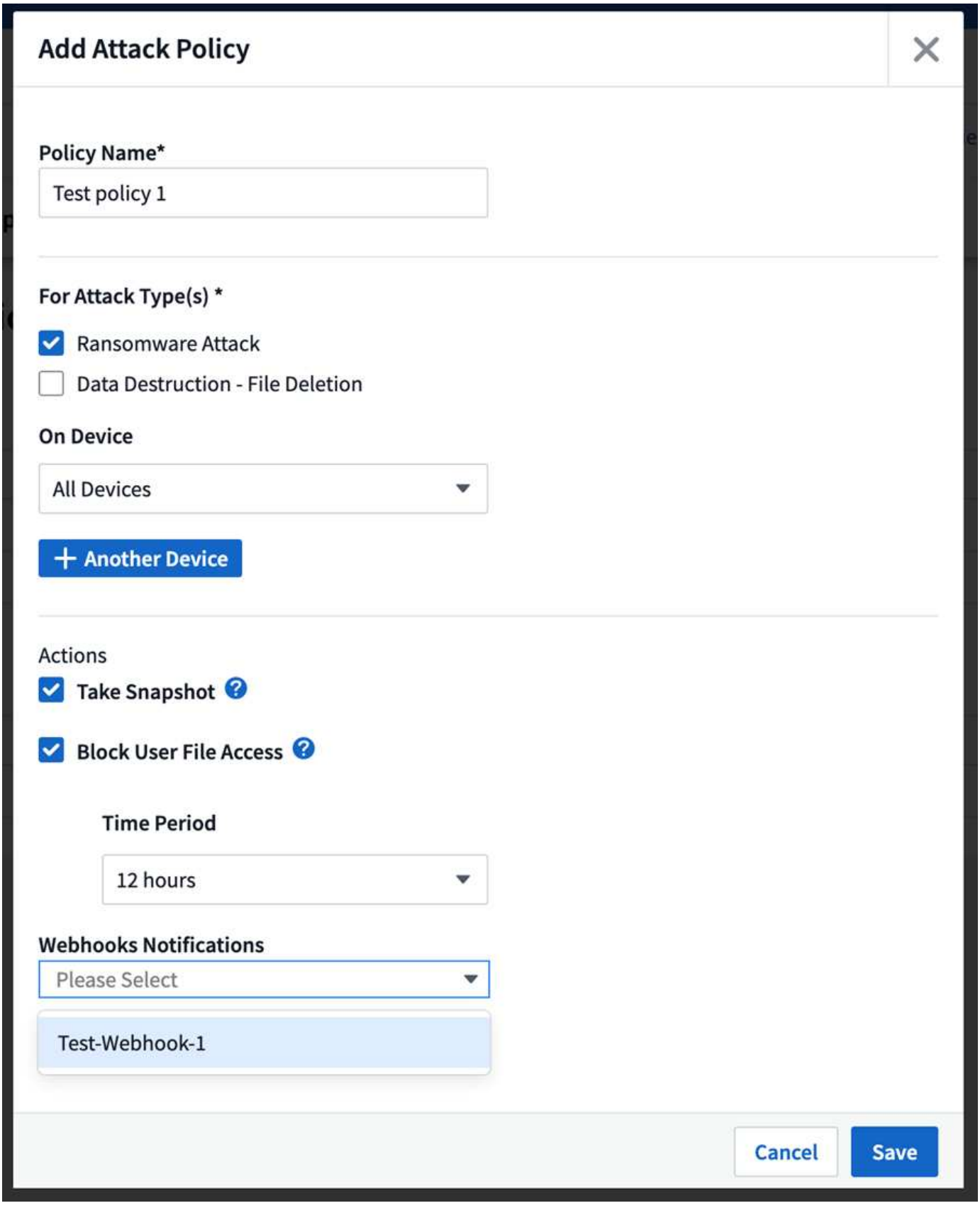


웹훅을 통한 알림

- 웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 클릭하세요.
- 의미 있는 정책 이름을 입력하세요.
- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.

- 웹후크 알림 드롭다운에서 필요한 웹후크를 선택합니다. 정책을 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.



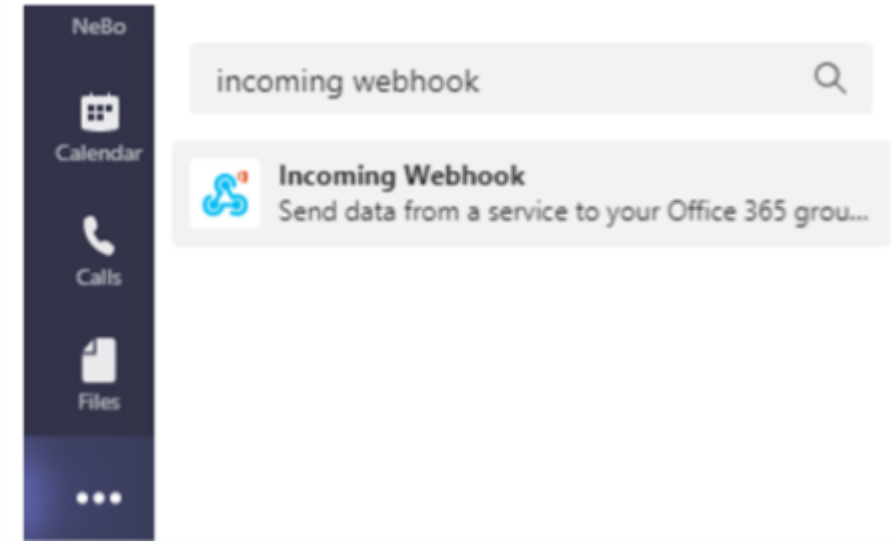
Microsoft Teams를 위한 워크로드 보안 웹훅 예시

웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을 보낼 수 있습니다. 이 페이지에서는 Teams에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

이 페이지는 변경될 수 있는 제3자 지침을 참조합니다. 를 참조하세요"팀 문서" 최신 정보를 확인하세요.

팀 설정:

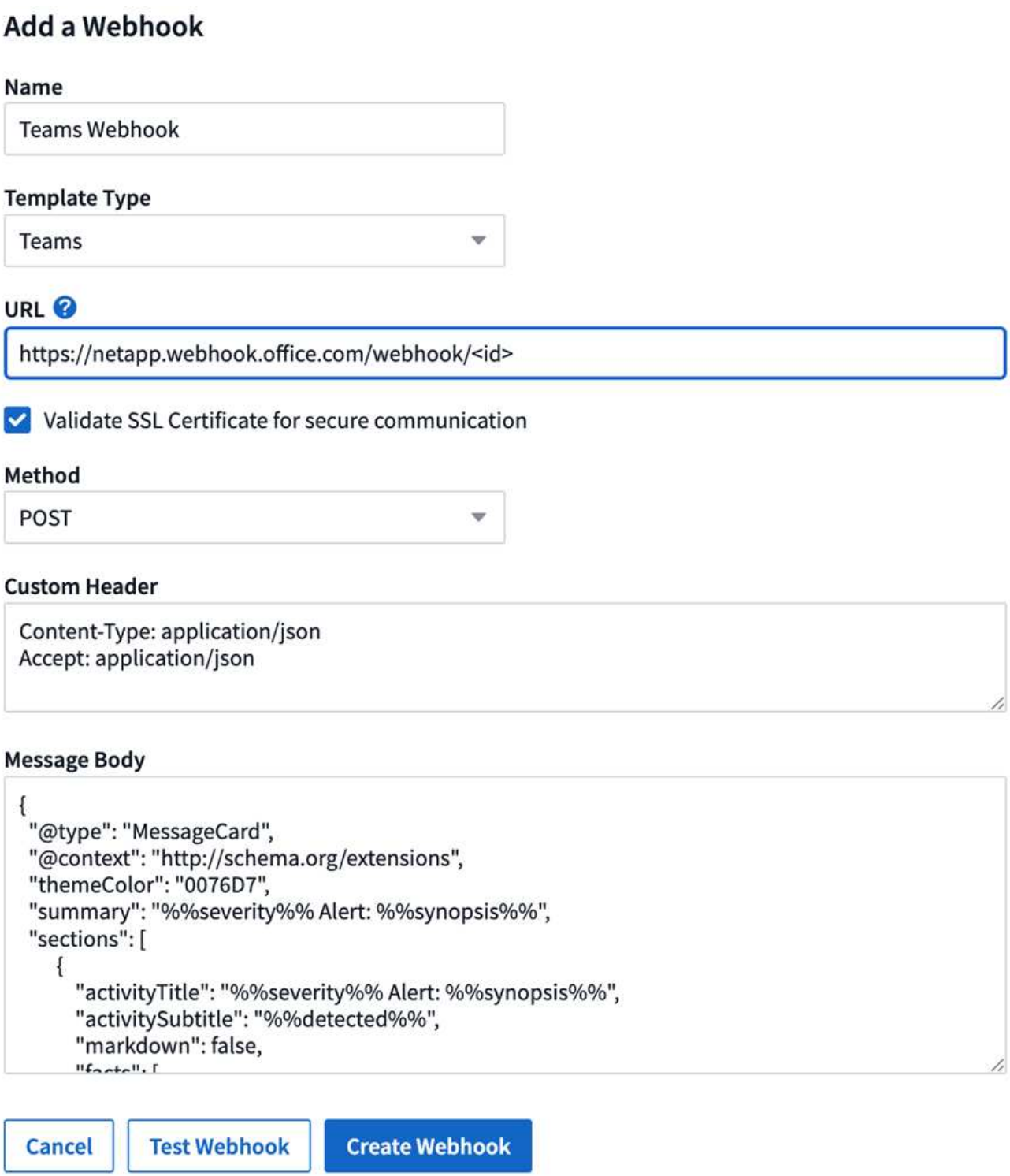
1. Teams에서 케밥을 선택하고 수신 웹훅을 검색합니다.



2. *팀에 추가 > 팀 선택 > 커넥터 설정*을 선택합니다.
3. Webhook URL을 복사합니다. 이것을 Workload Security 웹훅 구성에 붙여넣어야 합니다.

워크로드 보안 팀 웹훅 만들기:

1. 관리 > 알림으로 이동하여 “워크로드 보안 웹훅 탭을 선택합니다. _+ Webhook_을 선택하여 새 웹훅을 만듭니다.
2. 웹훅에 의미 있는 이름을 지정하세요.
3. 템플릿 유형 드롭다운에서 *팀*을 선택합니다.



4. 위의 URL을 *URL* 필드에 붙여넣으세요.

적응형 카드 템플릿을 사용하여 **Teams** 알림을 만드는 단계

1. 메시지 본문을 다음 템플릿으로 바꾸십시오.

```
{
"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. Power Automate Flows를 사용하는 경우 URL의 쿼리 매개변수는 인코딩된 형식입니다. 입력하기 전에 URL을 디코딩해야 합니다.
3. "Test Webhook"을 클릭하여 오류가 없는지 확인하십시오.
4. 웹훅을 저장합니다.

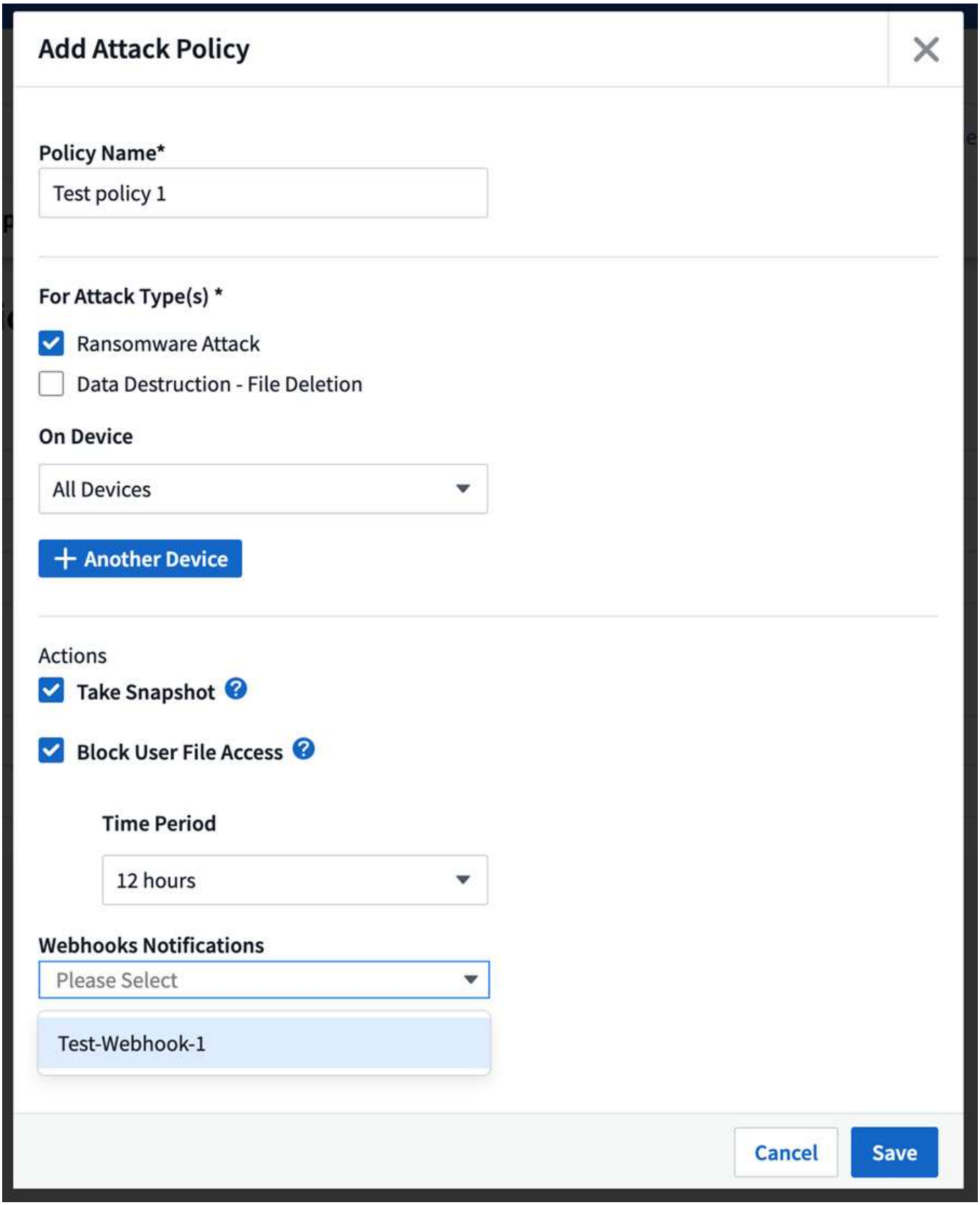
Webhook을 통한 알림

웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 선택하세요.

- 의미 있는 정책 이름을 입력하세요.

- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.
- 웹후크 알림 드롭다운에서 필요한 Teams 웹후크를 선택합니다. 정책을 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.


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