



웹훅 알림

Data Infrastructure Insights

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/data-infrastructure-insights/ws_notifications_using_webhooks.html on February 11, 2026. Always check docs.netapp.com for the latest.

목차

웹훅 알림	1
웹후크를 사용한 워크로드 보안 알림	1
웹훅 만들기	1
매개변수: 매개변수란 무엇이고 어떻게 사용하나요?	3
워크로드 보안 웹훅 목록 페이지	3
알림 정책에서 Webhook 알림 구성	4
Discord를 위한 워크로드 보안 웹훅 예시	6
Discord 설정:	6
워크로드 보안 웹훅 생성:	6
Webhook을 통한 알림	8
PagerDuty를 위한 워크로드 보안 웹훅 예제	9
PagerDuty 설정:	10
워크로드 보안 PagerDuty 웹훅 생성:	11
Webhook을 통한 알림	12
Slack을 위한 워크로드 보안 웹훅 예시	14
Microsoft Teams를 위한 워크로드 보안 웹훅 예시	18
팀 설정:	18
워크로드 보안 팀 웹훅 만들기:	18
Webhook을 통한 알림	21

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.

Add a Webhook

Name

Template Type

URL

Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-type: application/json
Accept: application/json
```

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "*%severity%% Alert: %%synopsis%%*"
      }
    },
    {
      "type": "divider"
    }
  ]
}
```

- 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.

/ Notifications / Add Webhook

Template Type: Slack

URL: `https://hooks.slack.com/services/%%slack-id%%`

Validate SSL Certificate for secure communication:

Method: POST

Custom Header:

```
Content-type: application/json
Accept: application/json
```

Message Body:

```
text: "Status: %%status%%"
},
{
  "type": "mrkdwn",
  "text": "Configured by: %%webhookConfiguredBy%%"
}
],
{
  "type": "mrkdwn",
  "text": "Configured by: %%webhookConfiguredBy%%"
}
]
```

Custom Parameters and Secrets:

Name	Value	Description
%%webhookConfiguredBy	system_admin_1	
%%slack-id%%	*****	

Cancel **Test Webhook** **Create Webhook**

워크로드 보안 웹훅 목록 페이지

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

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

400	<p>잘못된 요청입니다. 메시지 본문에 다음과 같은 오류가 있는 경우 이 상태가 표시될 수 있습니다.</p> <ul style="list-style-type: none"> • 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.

Edit Attack Policy



Policy Name*

For Attack Type(s) *

- Ransomware Attack
- Data Destruction - File Deletion

On Device

[+ Another Device](#)

Actions

- Take Snapshot [?](#)
- Block User File Access [?](#)

Time Period

Webhooks Notifications

Test-Webhook-1

[Cancel](#)[Save](#)

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 웹훅 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 "페이지듀티" 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:

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

Add a Webhook

Name

Template Type

URL ?

 Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-Type: application/json
Accept: application/json
```

Message Body

```
{
  "content": null,
  "embeds": [
    {
      "title": "%%severity%% | %%id%%",
      "description": "%%synopsis%%",
      "url": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%",
      "color": 3244733,
      "fields": [
        {
          "name": "%%",
          "value": "%%"
        }
      ]
    }
  ]
}
```

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.

Add Attack Policy



Policy Name*

For Attack Type(s) *

- Ransomware Attack
- Data Destruction - File Deletion

On Device

[+ Another Device](#)

Actions

- Take Snapshot [?](#)
- Block User File Access [?](#)

Time Period

Webhooks Notifications

Test-Webhook-1

[Cancel](#)[Save](#)

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 딕셔너리*로 이동한 다음 *+새 서비스 버튼을 클릭합니다.
2. _이름_을 입력하고 _API를 직접 사용_을 선택하세요. _서비스 추가_를 선택하세요.

Add a Service

A service may represent an application, component or team you wish to open incidents against.

General Settings

Name

Description

Add a description for this service (optional)

Integration Settings

Connect with one of PagerDuty's supported integrations, or create a custom integration through email or API. Alerts from a service from a supported integration or through the Events V2 API.

You can add more than one integration to a service, for example, one for monitoring alerts and one for [change events](#).

Integration Type



Select a tool



PagerDuty integrates with hundreds of tools, including monitoring tools, ticketing systems, code repositories, and deploy pipelines.

This may involve configuration steps in the tool you are integrating with PagerDuty.

Integrate via email

If your monitoring tool can send email, it can integrate with PagerDuty using a custom email address.

Use our API directly

If you're writing your own integration, use our Events API. More information is in our developer documentation.

Events API v2



Don't use an integration

If you only want incidents to be manually created. You can always add additional integrations later.

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.

Open Incidents (5)

					All statuses	Go to incident #	25 per page	1 - 5 of 5
Status	Priority	Urgency	Alerts	Title	Assigned To	Created		
<input type="checkbox"/> Acknowledged	High	1	1	Critical Alert: Ransomware attack from user [REDACTED] account #403982 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 4:11 AM		
<input type="checkbox"/> Acknowledged	High	1	1	Critical Alert: Data Destruction - File Deletion attack from user [REDACTED] account #403996 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 5:41 AM		

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.

Custom Parameters and Secrets 

Name	Value ↑	Description
%%routingKey%%	*****	***

 Parameter

Name 	Value
routingKey	*****
Type	Description
Secret	

Cancel
Save Parameter

Add a Webhook

Name

Test PagerDuty

Template Type

PagerDuty Trigger

URL 

https://events.pagerduty.com/%%pagerDutyId%%

 Validate SSL Certificate for secure communication

Method

POST

Custom Header

Content-Type: application/json
 Accept: application/json

Message Body

```
{
  "dedup_key": "%%id%%",
  "event_action": "trigger",
  "links": [
    {
      "href": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%",
      "text": "%%severity%% | %%id%% | %%detected%%"
    }
  ],
  "payload": {
    "user": "00000000000000000000"
  }
}
```

[Cancel](#)[Test Webhook](#)[Create Webhook](#)

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.

Add Attack Policy

Policy Name*

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**

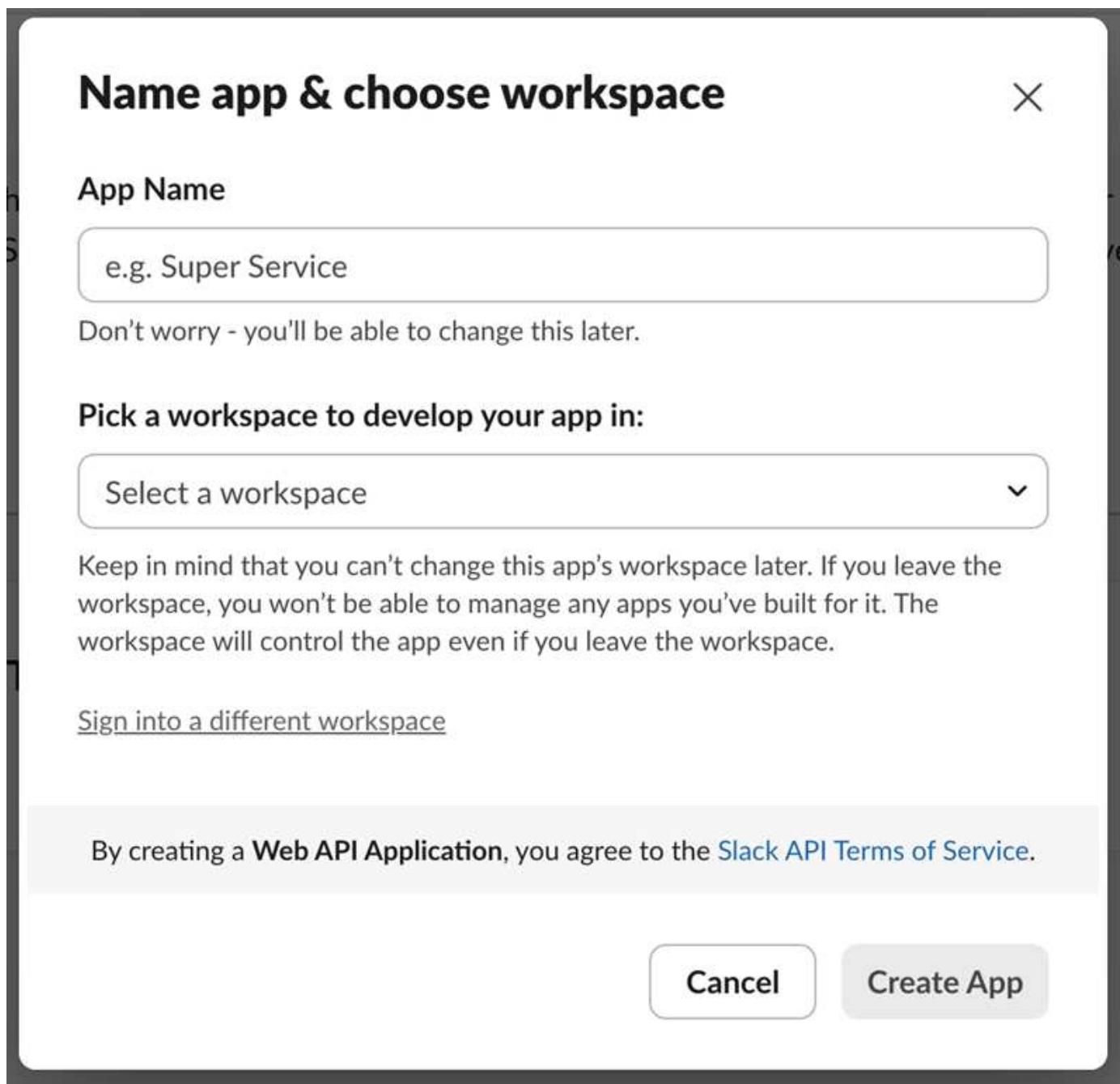
Slack을 위한 워크로드 보안 웹훅 예시

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.

Add a Webhook

Name

Template Type

URL

 Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-type: application/json
Accept: application/json
```

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "*%severity%% Alert: %%synopsis%%*"
      }
    },
    {
      "type": "divider"
    }
  ]
}
```

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.

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**

Microsoft Teams를 위한 워크로드 보안 웹훅 예시

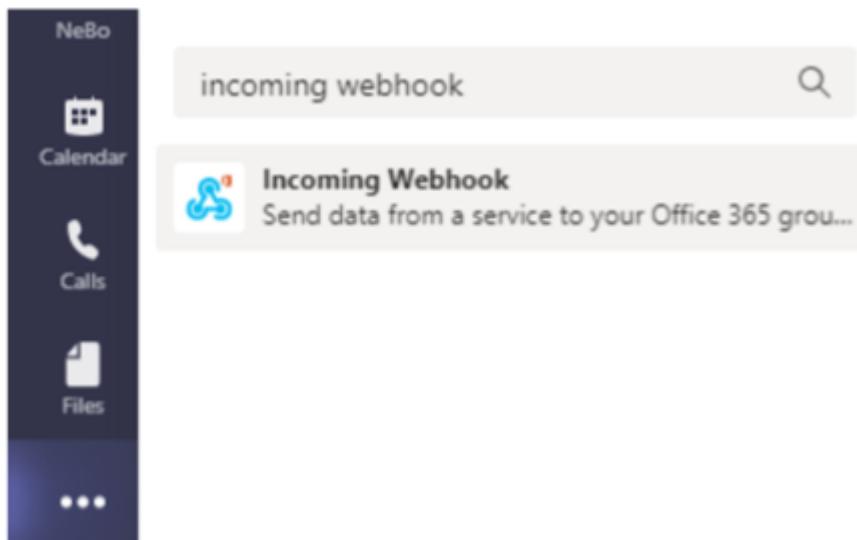
웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을 보낼 수 있습니다. 이 페이지에서는 Teams에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.



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.

Add a Webhook

Name

Template Type

URL

 Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-Type: application/json
Accept: application/json
```

Message Body

```
{
  "@type": "MessageCard",
  "@context": "http://schema.org/extensions",
  "themeColor": "0076D7",
  "summary": "%%severity%% Alert: %%synopsis%%",
  "sections": [
    {
      "activityTitle": "%%severity%% Alert: %%synopsis%%",
      "activitySubtitle": "%%detected%%",
      "markdown": false,
      "facts": [
        {
          "name": "Severity",
          "value": "%%severity%%"
        },
        {
          "name": "Detected At",
          "value": "%%detected%%"
        }
      ]
    }
  ]
}
```

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*

For Attack Type(s) *

- Ransomware Attack
- Data Destruction - File Deletion

On Device

[+ Another Device](#)

Actions

- Take Snapshot [?](#)
- Block User File Access [?](#)

Time Period

Webhooks Notifications

Test-Webhook-1

[Cancel](#)[Save](#)

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그레픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.