



Webhook-Benachrichtigungen

Data Infrastructure Insights

NetApp
February 11, 2026

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

Inhalt

Webhook-Benachrichtigungen	1
Workload-Sicherheitsbenachrichtigungen mithilfe von Webhooks	1
Erstellen eines Webhooks	1
Parameter: Was sind sie und wie werden sie verwendet?	3
Seite „Workload Security Webhooks – Liste“	3
Konfigurieren der Webhook-Benachrichtigung in der Warnrichtlinie	4
Workload Security Webhook-Beispiel für Discord	6
Discord-Setup:	6
Erstellen Sie einen Workload-Sicherheits-Webhook:	6
Benachrichtigungen per Webhook	8
Workload Security Webhook-Beispiel für PagerDuty	9
PagerDuty-Setup:	10
Erstellen Sie einen Workload Security PagerDuty-Webhook:	11
Benachrichtigungen per Webhook	12
Workload Security Webhook-Beispiel für Slack	14
Beispiel für einen Workload-Sicherheits-Webhook für Microsoft Teams	19
Teams-Setup:	19
Erstellen Sie einen Workload Security Teams-Webhook:	19
Benachrichtigungen per Webhook	22

Webhook-Benachrichtigungen

Workload-Sicherheitsbenachrichtigungen mithilfe von Webhooks

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal kritische Warnmeldungen oder Warnmeldungen an verschiedene Anwendungen senden.

Viele kommerzielle Anwendungen unterstützen Webhooks als Standardeingabeschnittstelle, zum Beispiel: Slack, PagerDuty, Teams und Discord. Durch die Unterstützung eines generischen, anpassbaren Webhook-Kanals kann Workload Security viele dieser Bereitstellungskanäle unterstützen. Informationen zur Konfiguration der Webhooks finden Sie auf den Webseiten der jeweiligen Anwendungen. Slack bietet beispielsweise "[dieser nützliche Leitfaden](#)".

Sie können mehrere Webhook-Kanäle erstellen, wobei jeder Kanal einem anderen Zweck, separaten Anwendungen, verschiedenen Empfängern usw. dient.

Die Webhook-Kanalinstanz besteht aus den folgenden Elementen

Name	Beschreibung
URL	Webhook-Ziel-URL, einschließlich des Präfixes http:// oder https:// zusammen mit den URL-Parametern
Verfahren	GET/POST – Standard ist POST
Benutzerdefinierter Header	Geben Sie hier alle benutzerdefinierten Header an
Nachrichtentext	Geben Sie hier den Text Ihrer Nachricht ein
Standard-Alarmparameter	Listet die Standardparameter für den Webhook auf
Benutzerdefinierte Parameter und Geheimnisse	Benutzerdefinierte Parameter und Geheimnisse ermöglichen Ihnen das Hinzufügen einzigartiger Parameter und sicherer Elemente wie Passwörter

Erstellen eines Webhooks

Um einen Workload Security Webhook zu erstellen, gehen Sie zu Admin > Benachrichtigungen und wählen Sie die Registerkarte „Workload Security Webhooks“. Das folgende Bild zeigt einen Beispielbildschirm zum Erstellen eines Slack-Webhooks.

Hinweis: Der Benutzer muss ein Workload Security-Administrator sein, um Workload Security-Webhooks erstellen und verwalten zu können.

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"
    }
  ]
}
```

- Geben Sie in jedes Feld die entsprechenden Informationen ein und klicken Sie auf „Speichern“.
- Sie können auch auf die Schaltfläche „Webhook testen“ klicken, um die Verbindung zu testen. Beachten Sie, dass dadurch der „Nachrichtentext“ (ohne Ersetzungen) gemäß der ausgewählten Methode an die definierte URL gesendet wird.
- SWS-Webhooks umfassen eine Reihe von Standardparametern. Darüber hinaus können Sie Ihre eigenen benutzerdefinierten Parameter oder Geheimnisse erstellen.

Parameter: Was sind sie und wie werden sie verwendet?

Alarmparameter sind dynamische Werte, die pro Alarm ausgefüllt werden. Beispielsweise wird der Parameter `%%severity%%` durch den Schweregradtyp der Warnung ersetzt.

Beachten Sie, dass beim Klicken auf die Schaltfläche „Webhook testen“ keine Ersetzungen durchgeführt werden. Der Test sendet eine Nutzlast, die die Platzhalter des Parameters (`%%<param-name>%%`) anzeigt, diese jedoch nicht durch Daten ersetzt.

Benutzerdefinierte Parameter und Geheimnisse

In diesem Abschnitt können Sie beliebige benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen. Ein benutzerdefinierter Parameter oder ein Geheimnis kann in der URL oder im Nachrichtentext enthalten sein. Mithilfe von Geheimnissen können Benutzer sichere benutzerdefinierte Parameter wie Kennwort, API-Schlüssel usw. konfigurieren.

Das folgende Beispielbild zeigt, wie benutzerdefinierte Parameter bei der Webhook-Erstellung verwendet werden.

The screenshot shows the 'Add Webhook' configuration page. On the left, the 'Message Body' field contains a JSON payload with a placeholder `%%webhookConfiguredBy%%` which is highlighted with a red box. On the right, a table lists various alert parameters and their corresponding placeholder values. Below the table, a 'Custom Parameters and Secrets' section is shown, containing two entries: `%%webhookConfiguredBy%%` with value `system_admin_1` and `%%slack-id%%` with a redacted value. A 'Create Webhook' button is at the bottom.

Placeholder	Description
<code>%%alertDetailsPageUrl%%</code>	https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%
<code>%%alertTimestamp%%</code>	Alert timestamp in Epoch format (milliseconds)
<code>%%changePercentage%%</code>	Change Percentage
<code>%%detected%%</code>	Alert timestamp in GMT (Tue, 27 Oct 2020 01:20:30 GMT)
<code>%%id%%</code>	Alert ID
<code>%%note%%</code>	Note
<code>%%severity%%</code>	Alert severity
<code>%%status%%</code>	Alert status
<code>%%synopsis%%</code>	Alert Synopsis
<code>%%type%%</code>	Alert type
<code>%%userId%%</code>	User id
<code>%%userName%%</code>	User name
<code>%%filesDeleted%%</code>	Files deleted
<code>%%encryptedFilesSuffix%%</code>	Encrypted files suffix
<code>%%filesEncrypted%%</code>	Files encrypted

Custom Parameters and Secrets

Name	Value	Description
<code>%%webhookConfiguredBy%%</code>	<code>system_admin_1</code>	...
<code>%%slack-id%%</code>

+ Parameter

Seite „Workload Security Webhooks – Liste“

Auf der Webhook-Listenseite werden die Felder „Name“, „Erstellt von“, „Erstellt am“, „Status“, „Sicher“ und „Zuletzt gemeldet“ angezeigt. Hinweis: Der Wert der Spalte „Status“ ändert sich ständig basierend auf dem Ergebnis des letzten Webhook-Triggers. Nachfolgend finden Sie Beispiele für Statusergebnisse.

Status	Beschreibung
OK	Benachrichtigung erfolgreich gesendet.

403	Verboten.
404	URL nicht gefunden.
400	<p>Ungültige Anforderung. Dieser Status wird möglicherweise angezeigt, wenn im Nachrichtentext ein Fehler vorliegt, beispielsweise:</p> <ul style="list-style-type: none"> • Schlecht formatiertes JSON. • Bereitstellung eines ungültigen Werts für reservierte Schlüssel. Beispielsweise akzeptiert PagerDuty für „Schweregrad“ nur „kritisch“/„Warnung“/„Fehler“/„Info“. Jedes andere Ergebnis kann zu einem 400-Status führen. • Anwendungsspezifische Validierungsfehler. Beispielsweise erlaubt Slack maximal 10 Felder innerhalb eines Abschnitts. Wenn Sie mehr als 10 angeben, kann dies zu einem 400-Status führen.
410	Ressource ist nicht mehr verfügbar

Die Spalte „Zuletzt gemeldet“ gibt den Zeitpunkt an, zu dem der Webhook zuletzt ausgelöst wurde.

Auf der Webhook-Listenseite können Benutzer Webhooks auch bearbeiten/duplizieren/löschen.

Konfigurieren der Webhook-Benachrichtigung in der Warnrichtlinie

Um einer Warnrichtlinie eine Webhook-Benachrichtigung hinzuzufügen, gehen Sie zu -Workload-Sicherheit > Richtlinien- und wählen Sie eine vorhandene Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu. Wählen Sie im Abschnitt „Aktionen“ > Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus.

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](#)

Webhook-Benachrichtigungen sind an Richtlinien gebunden. Wenn der Angriff (RW/DD/WARN) stattfindet, wird die konfigurierte Aktion (Snapshot erstellen/Benutzer blockieren) ausgeführt und anschließend die zugehörige Webhook-Benachrichtigung ausgelöst.

Hinweis: E-Mail-Benachrichtigungen sind unabhängig von Richtlinien und werden wie gewohnt ausgelöst.

- Wenn eine Richtlinie angehalten wird, werden keine Webhook-Benachrichtigungen ausgelöst.
- An eine einzelne Richtlinie können mehrere Webhooks angehängt werden. Es wird jedoch empfohlen, nicht mehr als 5 Webhooks an eine Richtlinie anzuhängen.

Beispiele für Workload-Sicherheits-Webhooks

Webhooks für "[Locker](#)"

Webhooks für "[PagerDuty](#)" Webhooks für "[Teams](#)" Webhooks für "[Zwietracht](#)"

Workload Security Webhook-Beispiel für Discord

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Discord.



Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im "[Discord-Dokumentation](#)" für die aktuellsten Informationen.

Discord-Setup:

- Wählen Sie in Discord den Server aus und wählen Sie unter „Textkanäle“ die Option „Kanal bearbeiten“ (Zahnradssymbol).
- Wählen Sie **Integrationen > Webhooks anzeigen** und klicken Sie auf **Neuer Webhook**
- Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload-Sicherheits-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Klicken Sie auf „+ Webhook“, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Discord** aus.
4. Fügen Sie die Discord-URL von oben in das Feld *URL* ein.

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": "%%"
        }
      ]
    }
  ]
}
```

Um den Webhook zu testen, ersetzen Sie den URL-Wert im Nachrichtentext vorübergehend durch eine beliebige gültige URL (z. B. <https://netapp.com>) und klicken Sie dann auf die Schaltfläche *Webhook testen*. Discord erfordert die Angabe einer gültigen URL, damit die Test-Webhook-Funktionalität funktioniert.

Denken Sie daran, den Nachrichtentext nach Abschluss des Tests wiederherzustellen.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, denen die Richtlinie zugeordnet werden soll, und erforderliche Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die gewünschten Discord-Webhooks aus und speichern Sie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.

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

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

Workload Security Webhook-Beispiel für PagerDuty

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal

Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für PagerDuty.



Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im "[PagerDuty-Dokumentation](#)" für die aktuellsten Informationen.

PagerDuty-Setup:

1. Navigieren Sie in PagerDuty zu **Dienste > Dienstverzeichnis** und klicken Sie auf die Schaltfläche **+Neuer Dienst**.
2. Geben Sie einen *Namen* ein und wählen Sie *Unsere API direkt verwenden*. Wählen Sie *Dienst hinzufügen*.

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. Wählen Sie die Registerkarte *Integrationen*, um den **Integrationsschlüssel** anzuzeigen. Sie benötigen diesen Schlüssel, wenn Sie unten den Workload Security-Webhook erstellen.
4. Gehen Sie zu **Vorfälle** oder **Dienste**, um Warnungen anzuzeigen.

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	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	Critical Alert: Data Destruction - File Deletion attack from user [REDACTED] account #403996 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 5:41 AM			

Erstellen Sie einen Workload Security PagerDuty-Webhook:

- Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie „+ Webhook“, um einen neuen Webhook zu erstellen.
- Geben Sie dem Webhook einen aussagekräftigen Namen.
- Wählen Sie im Dropdown-Menü *Vorlagentyp* die Option *PagerDuty-Trigger* aus.
- Erstellen Sie ein benutzerdefiniertes Parametergeheimnis mit dem Namen *routingKey* und legen Sie den Wert auf den oben erstellten PagerDuty-*Integrationsschlüssel* fest.

Custom Parameters and Secrets i

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

+ Parameter

Name i	Value
<input type="text" value="routingKey"/>	<input type="text" value="*****"/>
Type	Description
<input type="text" value="Secret"/>	<input type="text"/>

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](#)

Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Wählen Sie **+Angriffsrichtlinie** oder **+Warnrichtlinie**.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die erforderlichen Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen PagerDuty-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.

Add Attack Policy

Policy Name*

For Attack Type(s) *

Ransomware Attack

Data Destruction - File Deletion

On Device

All Devices

Actions

Take Snapshot ?

Block User File Access ?

Time Period

12 hours

Webhooks Notifications

Please Select

Test-Webhook-1

Cancel **Save**

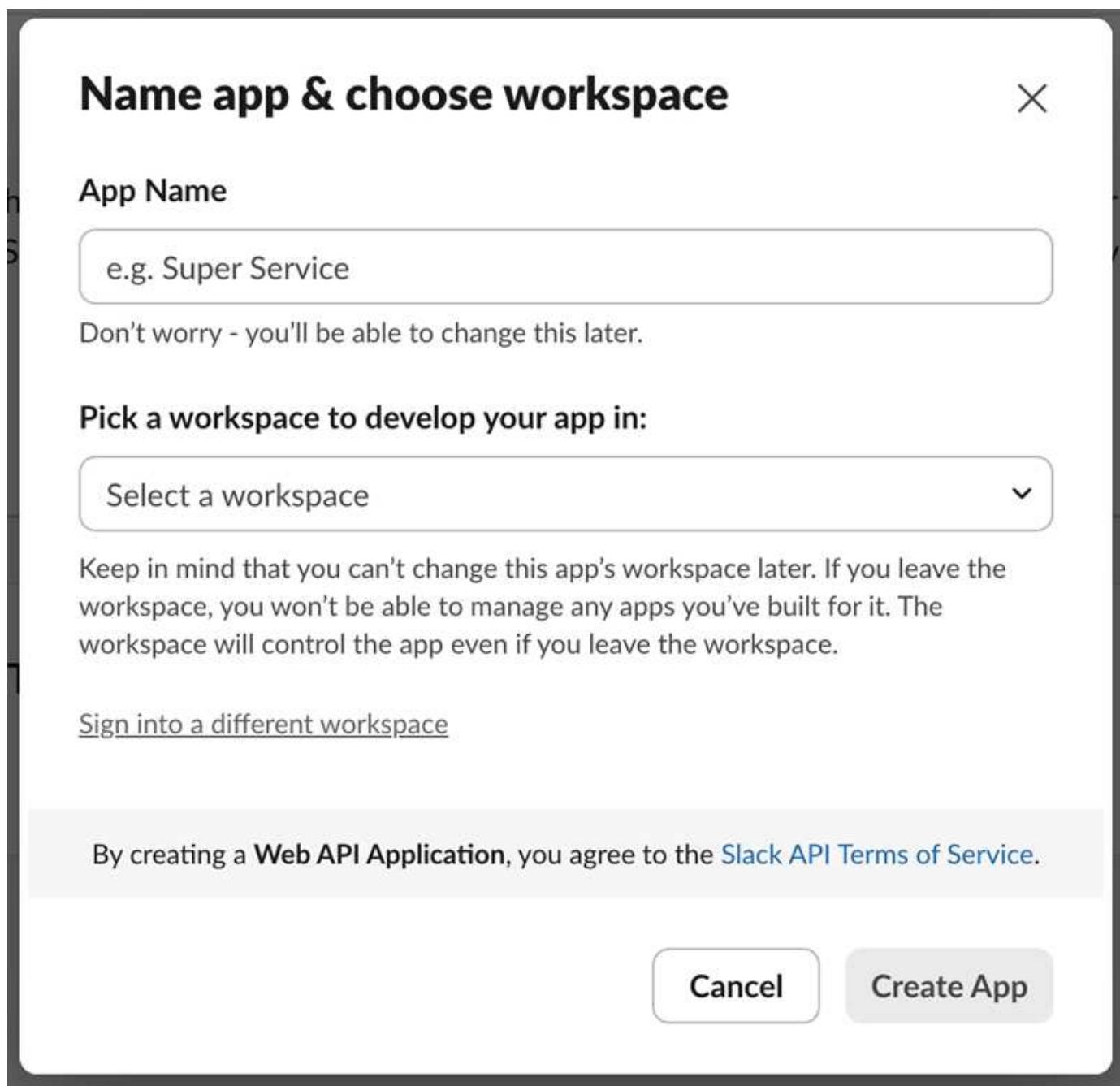
Workload Security Webhook-Beispiel für Slack

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Slack.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Die aktuellsten Informationen finden Sie in der Slack-Dokumentation.

Slack-Beispiel

- Gehe zu <https://api.slack.com/apps> und erstellen Sie eine neue App. Geben Sie ihm einen aussagekräftigen Namen und wählen Sie einen Arbeitsbereich aus.



- Gehen Sie zu „Eingehende Webhooks“, klicken Sie auf „Eingehende Webhooks aktivieren“, wählen Sie „Neuen Webhook hinzufügen“ und wählen Sie den Kanal aus, auf dem gepostet werden soll.
- Kopieren Sie die Webhook-URL. Diese URL wird beim Erstellen eines Workload Security-Webhooks angegeben.

Erstellen Sie einen Slack-Webhook für die Workload-Sicherheit

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie **+ Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü **Vorlagentyp** die Option **Slack** aus.
4. Fügen Sie die oben kopierte URL ein.

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"
    }
  ]
}
```

Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und erforderliche Aktionen aus.

- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.

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](#)

Beispiel für einen Workload-Sicherheits-Webhook für Microsoft Teams

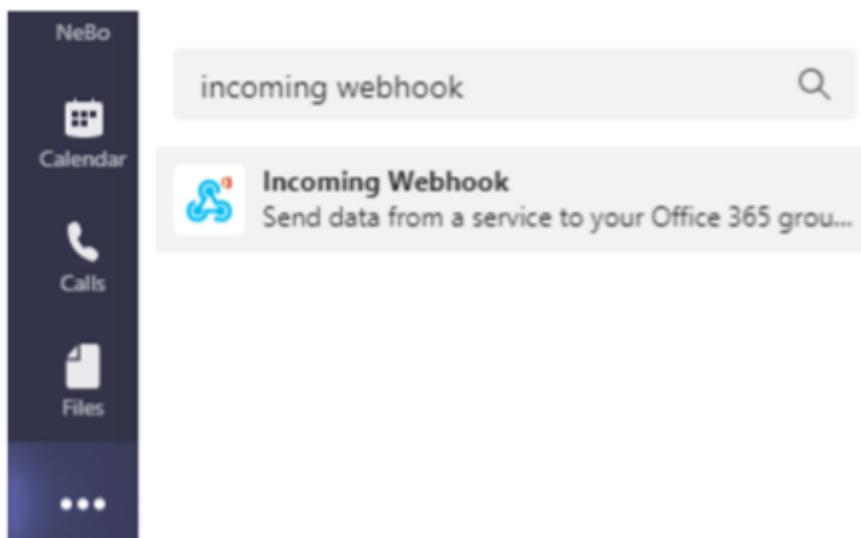
Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Teams.



Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im "[Teams-Dokumentation](#)" für die aktuellsten Informationen.

Teams-Setup:

1. Wählen Sie in Teams den Kebab aus und suchen Sie nach „Eingehender Webhook“.



2. Wählen Sie **Zu einem Team hinzufügen > Ein Team auswählen > Einen Connector einrichten**.
3. Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload Security Teams-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie + Webhook, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „Teams“ aus.

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. Fügen Sie die URL von oben in das Feld *URL* ein.

Schritte zum Erstellen einer Teams-Benachrichtigung mit der Adaptive Card-Vorlage

1. Ersetzen Sie den Nachrichtentext durch die folgende Vorlage:

```
{
  "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. Wenn Sie Power Automate Flows verwenden, sind die Abfrageparameter in der URL im codierten Format. Sie müssen die URL decodieren, bevor Sie sie eingeben.
3. Klicken Sie auf „Test Webhook“, um sicherzustellen, dass keine Fehler vorliegen.
4. Speichern Sie den Webhook.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Wählen Sie **+Angriffsrichtlinie** oder **+Warnrichtlinie**.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.

- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die erforderlichen Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Teams-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.

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](#)

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.