Myra DataHub

SOC-Handbuch (Cloud)

Versionsverfolgung

Version	Datum	Änderungsgrund
V1.16	08/2026	Aktualisierte Abschnitte: • Ansicht Netzwerke • Ansicht Anomalieverlauf • Reiter Benachrichtigungen • Unternehmen ändern • Anmeldung
V1.15	08/2026	Aktualisierte Abschnitte: • Übersicht Myra DataHub-Portal • Ansicht Unternehmenskonten • Unternehmen ändern • Ansicht Netzwerke • Netzwerk hinzufügen • Netzwerk ändern • Netzwerk ansehen • Netzwerk löschen • Manuelle Mitigationen starten • Manuelle Mitigationen beenden • Ansicht Mitigationsverlauf • Ansicht Mitigationsberichte • Ansicht Traffic-Berichte • Unternehmensmanagement • Ansicht Dashboard Neue Abschnitte: • Ansicht Anomalieverlauf • Reiter Benachrichtigungen • Alle Anomalien der Organisation auflisten • Benachrichtigungseinstellung des authentifizierten Nutzenden ändern • Benachrichtigungsadresse zur Organisation hinzufügen • Benachrichtigungsadresse aus der Organisation löschen

Version	Datum	Änderungsgrund
		• Handbuch als PDF Kleinere Korrekturen
V1.14	07/2026	Kleine Korrekturen
V1.13	06/2026	Neue Abschnitte: • Reiter API-Token
V1.12	06/2026	Aktualisierte Abschnitte: • Ansicht Netzwerk • Netzwerk hinzufügen • Netzwerk bearbeiten • Netzwerk ansehen
V1.11	04/2026	Kleine Korrekturen
V1.10	03/2026	Neue Abschnitte: • Traffic-Berichte Kleine Korrekturen
V1.9	03/2026	Aktualisierte Abschnitte aufgrund eines neuen Beschreibungsfeldes Details: • Netzwerk ansehen • Netzwerk hinzufügen
V1.8	02/2026	Kleine Korrekturen
V1.7	12/2025	Neue Abschnitte: • Reiter SIEM-Einstellungen
V1.6	11/2025	Neues Layout
V1.5	09/2025	Aktualisierte Abschnitte für SIEM: • Unternehmen hinzufügen • Unternehmen ändern

Version	Datum	Änderungsgrund
V1.4	08/2025	Aktualisierte Abschnitte: • Detailansicht Monatsbericht
V1.3	07/2025	Kleinere Korrekturen
V1.2	05/2025	Aktualisierte Abschnitte: • Übersicht Myra DataHub-Portal • Ansicht Unternehmensmanagement Neue Abschnitte: • Unternehmen hinzufügen • Unternehmen ändern • Unternehmen löschen • Netzwerk hinzufügen • Netzwerk ändern • Netzwerk löschen • Ansicht Bericht • Ansicht Audit-Log • Ansicht Changelog
V1.1	04/2025	Kleinere Korrekturen
V1.0	03/2025	Ersterstellung

Inhalt

1. Myra DataHub

1.1 Beschreibung

1.1.1 Was ist der Myra DataHub?

> **Video:** Was ist der Myra DataHub? — abspielbar in der Online-Hilfe

Der Myra DataHub ist eine webbasierte Benutzeroberfläche für die Myra Flow Application, die Myra-Partnern für eine bessere Übersicht der Endkunden bereitgestellt wird.

Für Myra-Partner umfasst die Benutzeroberfläche eine Übersicht aller Endkunden eines Partners samt den aufgeschalteten Netzen, Analysen und Mitigation sowie den Konten der Nutzenden. Der Partner kann neue Kunden als Unternehmen anlegen, bearbeiten und löschen, sowie Netzwerke und Nutzende der Organisation hinzufügen und verwalten. Die Endkunden erhalten eine übersichtliche Darstellung ihres Traffic-Verlaufs, eine Auflistung der aktivierten Netze sowie die gesammelten Mitigationsreports.

Der Traffic-Verlauf umfasst eine Darstellung der Bandbreite und Paketrate, sortiert nach Ziel-IP und den Paketraten nach Port, die mit verschiedenen Betrachtungszeiträumen bis zu 24 Stunden angezeigt werden können. Zudem kann der Partner über die Benutzeroberfläche die gesetzten Schwellenwerte einsehen und eine Mitigation manuell starten oder stoppen.

1.2 Erste Schritte

1.2.1 Anmeldung

Um sich mit Ihren Anmeldedaten anzumelden, gehen Sie wie folgt vor:

- Melden Sie sich in der Myra App an, siehe Abschnitt Anmelden mit Benutzername und Passwort im **Handbuch Myra App** und Abschnitt Anmelden mit Single Sign-on (SSO) im **Handbuch Myra App**.
- Klicken Sie auf den Reiter **Network Security**.

→ Die Startseite **Dashboard** des Myra DataHub öffnet sich.

1.3 DataHub-Portal

1.3.1 Übersicht Myra DataHub-Portal

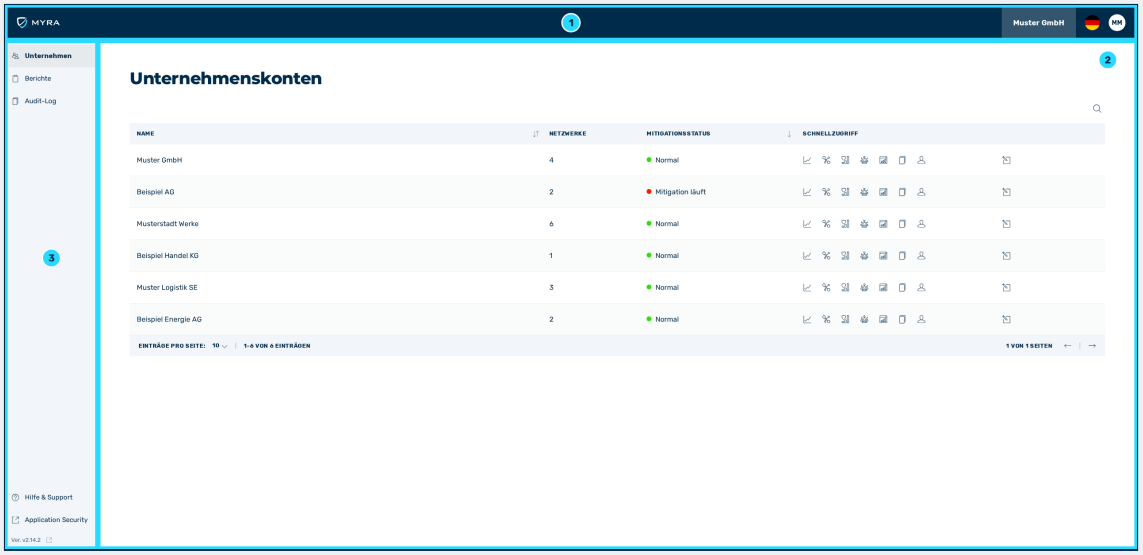


Abbildung 1: Übersicht Startseite

Nach dem Login erscheint die Startseite **Dashboard** des Myra DataHub.

Auf der Startseite können Sie die folgenden Informationen finden:

- Obere Menüleiste mit Zugriff auf die folgenden Schaltflächen (1):
  - Schaltfläche mit dem Namen des Unternehmens für den Zugriff auf die Benutzerverwaltung
  - Schaltfläche mit Flaggensymbol zur Auswahl der Sprache der Benutzeroberfläche
  - Schaltfläche mit Profilbild der Nutzenden zur Verwaltung der eigenen Kontoeinstellungen
  - Im Falle einer Wartung werden hier wichtige Informationen über die Art und Dauer als gesondertes Banner eingeblendet.
- Darstellung des Inhaltes der einzelnen Ansichten (2)

- Reiter mit den folgenden Ansichten (3):
  - Unternehmen
  - Bericht
  - Audit-Log
  - Application Security zum Öffnen der Myra App
  - Hilfe & Support zum Öffnen der Online-Hilfe
  - Anzeige der aktuellen Versionsnummer mit Symbol zum Öffnen der Ansicht **Changelog**

1.3.1.1 Ansicht Unternehmenskonten

Abbildung 2: Ansicht Unternehmenskonten

Die Ansicht **Unternehmenskonten** erscheint automatisch auf der Startseite, wenn Sie sich in den Myra DataHub einloggen. Hier können Sie eine Liste aller Kunden und deren Daten einsehen. Außerdem können Sie in der Ansicht **Unternehmenskonten** als SOC-Admin vorhandene Unternehmen verwalten und ändern.

Folgende Informationen werden Ihnen in einer Tabelle angezeigt:

Element	Beschreibung
Name	Der Name des Kunden.
Netzwerke	Die eingetragenen IP-Adressen des Kunden.
Mitigationsstatus	Der Mitigationsstatus für das entsprechende Unternehmen. **Mitigation läuft** : Eine oder mehrere Mitigationen wurden gestartet.

Element	Beschreibung
	Normal : Eine oder mehrere Mitigationen wurden erfolgreich beendet.
Schnellzugriff	Zeigt die Symbole für den direkten Zugriff auf die möglichen Einstellungen für das ausgewählte Unternehmen an.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
	Das Symbol ermöglicht die gezielte Suche nach Namen, Kunden-ID und Netzwerken.
	Das Symbol öffnet die Ansicht **Dashboard** des jeweiligen Unternehmens mit Informationen zu dessen Netzwerk-Traffic. Siehe **Ansicht Dashboard**.
	Das Symbol öffnet die Ansicht **Netzwerke** des jeweiligen Unternehmens. Hier kann sofort die manuelle Mitigationen gestartet oder beendet werden. Siehe **Ansicht Netzwerke**.
	Das Symbol öffnet die Ansicht **Mitigationsverlauf** des jeweiligen Unternehmens mit einer Auflistung aller vergangenen Mitigationen. Siehe **Ansicht Mitigationsverlauf**.
	Das Symbol öffnet die Ansicht **Audit-Log** des jeweiligen Unternehmens mit einer Auflistung aller Änderungen des Unternehmens. Siehe **Ansicht Audit-Log**.
	Das Symbol öffnet die Ansicht **Benutzerverwaltung** des jeweiligen Unternehmens. Hier können die Einstellungen für Konten eingesehen und geändert werden. Siehe **Ansicht Benutzerverwaltung**.
	Das Symbol öffnet den Dialog **Unternehmen bearbeiten** zur Bearbeitung des Namens und der Einstellungen des Unternehmens. Siehe **Unternehmen ändern**.

Element	Beschreibung

> Um ein Unternehmen zu ändern benötigen Sie SOC-Administrationsrechte.

> Im SOC-Modus agieren Sie als Admin des jeweiligen Unternehmens. Eine orangefarbene Statusleiste unterhalb der oberen Navigationsleiste signalisiert Ihnen, dass Sie sich im SOC-Modus für ein Unternehmen befinden.
>
> Wenn Sie ein Unternehmen geöffnet haben und zurück zur Übersicht alle Unternehmen in der Ansicht **Unternehmenskonten** wollen, müssen Sie die Schaltfläche **Zurück zur Übersicht** verwenden. Der Weg über die Zurücktaste im Browser funktioniert nicht.
>
> Sollten Sie im SOC-Modus eine manuelle Mitigation für ein Unternehmen starten oder andere Änderungen vornehmen, wird dies in den Audit-Logs als Änderung durch Sie als SOC-User festgehalten.

1.3.1.1.1 Unternehmen ändern

> Um ein Unternehmen zu ändern benötigen Sie SOC-Administrationsrechte.

Um ein Unternehmen zu ändern, gehen Sie wie folgt vor:

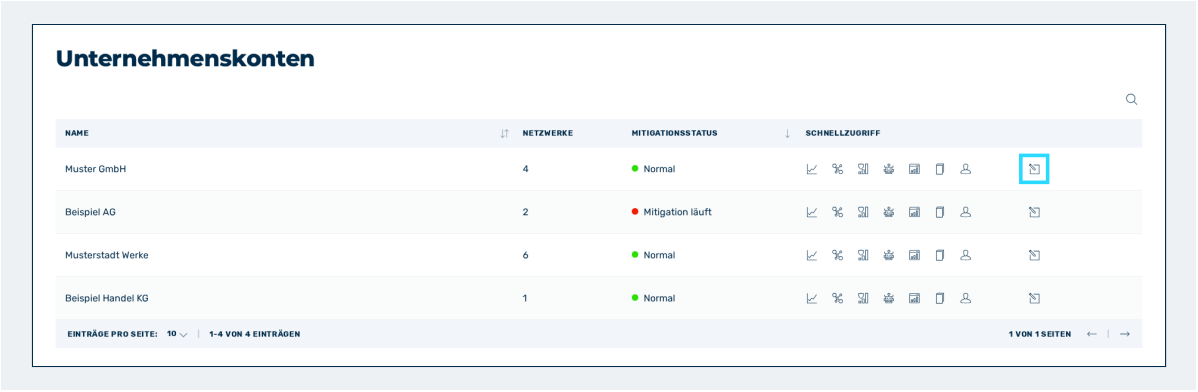


Abbildung 3: Schaltfläche zum Bearbeiten eines Unternehmens

- ► Klicken Sie auf das Symbol .
  - ↳ Der Dialog **Unternehmen bearbeiten** öffnet sich.

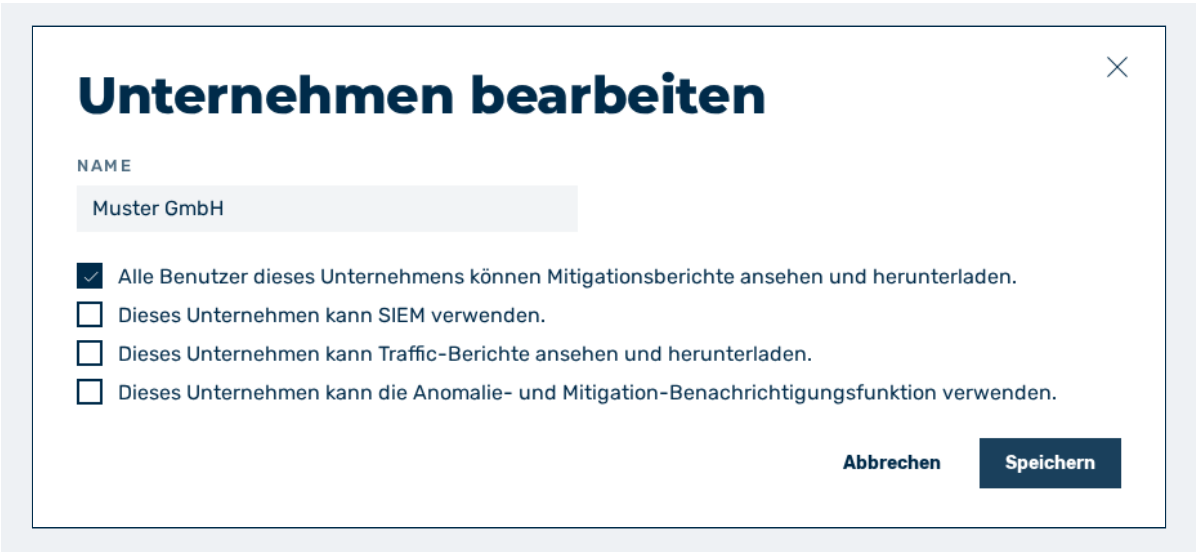


Abbildung 4: Dialog Unternehmen bearbeiten

- ► Geben Sie ins Feld unter **Name** den neuen Namen des Unternehmens ein.

- Falls erforderlich, aktivieren oder deaktivieren Sie die Auswahlbox unter **Alle Benutzer dieses Unternehmens können Mitigationsberichte ansehen und herunterladen.**.

> Wenn die Auswahlbox unter **Alle Benutzer dieses Unternehmens können Mitigationsberichte ansehen und herunterladen.** deaktiviert ist, sehen die Nutzenden des Unternehmens keine Mitigationsberichte mehr und laden auch keine mehr herunter. Diese Option kann nicht für einzelne Nutzende aktiviert werden.

- Falls erforderlich, aktivieren oder deaktivieren Sie die Auswahlbox unter **Dieses Unternehmen kann SIEM verwenden.**.

> SIEM (Security Information and Event Management) ist eine Sicherheitslösung, die Unternehmen hilft, Sicherheitsbedrohungen zu erkennen und darauf zu reagieren. Es erfasst, analysiert und korreliert Daten aus verschiedenen Quellen, um Anomalien und potenzielle Sicherheitsvorfälle zu identifizieren. SIEM-Systeme ermöglichen eine zentrale Überwachung und Reaktion auf Bedrohungen und unterstützen Unternehmen bei der Einhaltung von Compliance-Vorschriften.

> Die Audit-Logs für die SIEM-Integration werden über eine Splunk-Schnittstelle im JSON-Format zur Verfügung gestellt und enthalten die folgenden Informationen:
>
> - Start- und Stop-Events bei Mitigationen
> - Ziel-IP
> - Gemessene Paketrate (in PPS)
> - Gemessene Datenrate (in Bits/s)
> - Konfigurierte Schwellwerte für den IP-Adressen-Bereich
> - Berechtigungen der Nutzenden (Benutzer und Admins)
> - Mitigationsberichte

- ▶ Falls erforderlich, aktivieren oder deaktivieren Sie die Auswahlbox unter **Dieses Unternehmen kann Traffic-Berichte ansehen und herunterladen.**.

> ⓘ Wenn die Auswahlbox unter **Dieses Unternehmen kann Traffic-Berichte ansehen und herunterladen.** deaktiviert ist, sehen die Nutzenden des Unternehmens keine Traffic-Berichte mehr und laden auch keine mehr herunter. Diese Option kann nicht für einzelne Nutzende aktiviert werden.

- ▶ Falls erforderlich, aktivieren oder deaktivieren Sie die Auswahlbox unter **Dieses Unternehmen kann die Anomalie-Funktion verwenden.**.

> ⓘ Wenn die Auswahlbox unter **Dieses Unternehmen kann die Anomalie-Funktion verwenden.** aktiviert ist, steht den Nutzenden des Unternehmens die Ansicht **Anomalieverlauf** zur Verfügung und Myra benachrichtigt sie zusätzlich zu den Mitigationen auch über Traffic-Anomalien.

- ▶ Klicken Sie auf die Schaltfläche **Speichern**.
- ➔ Eine Meldung bestätigt die erfolgreiche Änderung des Unternehmens.

Die Änderungen sind ebenfalls danach in der Tabelle in der Ansicht **Unternehmenskonten** sichtbar.

1.3.1.2 Ansicht Bericht

> ⓘ Die Ansicht **Berichte** wird nur für SOC-Administrierende angezeigt.

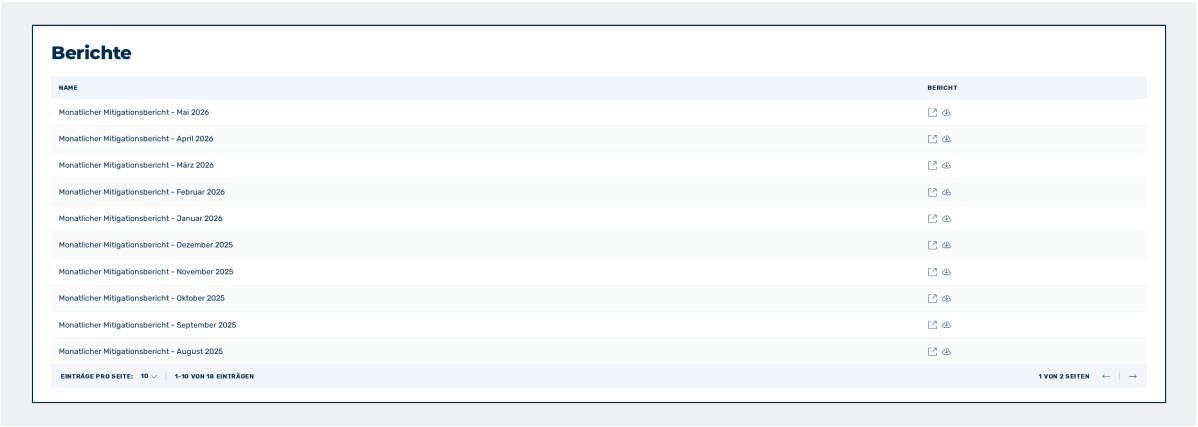


Abbildung 5: Ansicht Berichte

Die Ansicht **Berichte** ermöglicht den Zugriff auf die monatlichen Berichte über alle gestarteten, erfolgreichen und abgebrochenen Mitigationen der einzelnen Unternehmen.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Name	Der Name, der Monat und das Jahr des monatlichen Berichtes.
Bericht	Zeigt die Symbole zum Öffnen und Herunterladen der monatlichen Berichte an.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
	Das Symbol öffnet die Ansicht **<Name des Berichtes>** zum Einsehen der einzelnen Mitigationsinformationen.
	Das Symbol ermöglicht das Herunterladen des kompletten monatlichen Berichtes als CSV-Datei.

1.3.1.2.1 Detailansicht Monatsbericht

Abbildung 6: Detailansicht Monatsbericht

In der Ansicht des Monatsberichtes erhalten Sie detaillierte Informationen über alle gestarteten, beendeten und abgebrochenen Mitigationen der einzelnen Unternehmen.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Name	Der Name des Kunden.
Netzwerk	Die IP-Adresse des Netzwerkes für das eine Mitigation gestartet wurde.
Gestartet	Der Zeitpunkt mit Uhrzeit und Datum, zu dem die Mitigation gestartet wurde.
Beendet	Der Zeitpunkt mit Uhrzeit und Datum, zu dem die Mitigation beendet wurde.
Bandbreiten-Schwellenwert (MBit/s)	Die maximale Bandbreite, die für Ihr Netzwerk erlaubt ist.
Paketraten-Schwellenwert (Pakete/s)	Die maximal erlaubte Anzahl von Paketen pro Sekunde, die für das Netzwerk erlaubt sind.
Maximale Bandbreite (MBit/s)	Die höchste Auslastung der Bandbreite während der Mitigation.
Maximale Paketrate (Pakete/s)	Die höchste Anzahl an Paketen pro Sekunde während der Mitigation.
Datenvolumen (MBit)	Das gesamte Datenvolumen während der Mitigation.
Pakete gesamt	Die Summe aller Pakete während der Mitigation.

Element	Beschreibung
Auslösertyp	Zeigt an, ob es sich um eine automatische oder manuelle Mitigation gehandelt hat.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
	Das Symbol ermöglicht die gezielte Suche nach dem Namen des Berichtes.
CSV herunterladen	Die Schaltfläche **Herunterladen** ermöglicht das Herunterladen des kompletten monatlichen Berichtes als CSV-Datei.

1.3.1.3 Ansicht Audit-Log

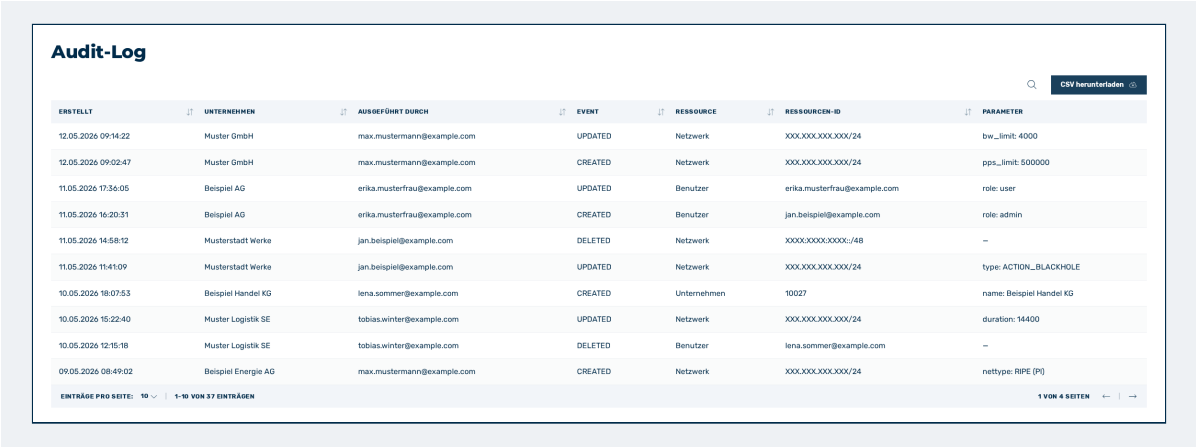


Abbildung 7: Ansicht Audit-Log

In der Ansicht **Audit-Log** erhalten Sie detaillierte Informationen über alle Änderungen, die für das eigene Unternehmen oder die Unternehmen der Kunden vorgenommen wurden.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Erstellt	Die Uhrzeit und das Datum zu der die Änderung vorgenommen wurde.
Unternehmen	Der Name des Unternehmens.

Element	Beschreibung
Ausgeführt durch	Der Name des Nutzenden.
Event	Die Art der Tätigkeit. **CREATED**: Ein neuer Eintrag wurde erstellt. **UPDATED**: Ein vorhandener Eintrag wurde geändert. **DELETED**: Ein vorhandener Eintrag wurde gelöscht.
Ressource	Der Ort der Änderung.
Ressourcen-ID	Der Eintrag, der geändert wurde.
Parameter	Die Werte des entsprechenden Eintrages, die geändert wurden.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
	Das Symbol filter nach dem Namen des Berichtes.
CSV herunterladen	Die Schaltfläche lädt den kompletten monatlichen Bericht als CSV-Datei herunter.

1.3.1.4 Ansicht Versionsverlauf

Die Ansicht **Versionsverlauf** ermöglicht Ihnen den Zugriff auf eine Übersicht aller Änderungen und Anpassungen der einzelnen Versionen des Myra DataHub.

Wenn Sie den Versionsverlauf anzeigen wollen, gehen Sie wie folgt vor:

- ▶ Öffnen Sie die Website des Myra DataHub.
- ▶ Loggen Sie sich ein.
  - ↳ Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.
- ▶ Klicken Sie in der linken Menüleiste unten links auf den Namen der Version oder das Symbol  .

➔ Die Ansicht **Versionsverlauf** öffnet sich.

Die folgenden Informationen werden angezeigt:

- Name der Myra DataHub-Version
- Datum der Veröffentlichung
- Übersicht über die einzelnen Anpassungen und Korrekturen

1.3.2 Unternehmensmanagement

Um zur Website eines Unternehmens zu gelangen, gehen Sie wie folgt vor:

- ▶ Öffnen Sie die Myra App.
- ▶ Loggen Sie sich ein.
  - ↳ Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.
  - ↳ Die Startseite der Myra App öffnet sich.
- ▶ Klicken Sie auf den Reiter **Network Security** in der linken Navigationsleiste.
- ▶ Klicken Sie auf den Namen des gewünschten Unternehmens.
- ➔ Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.

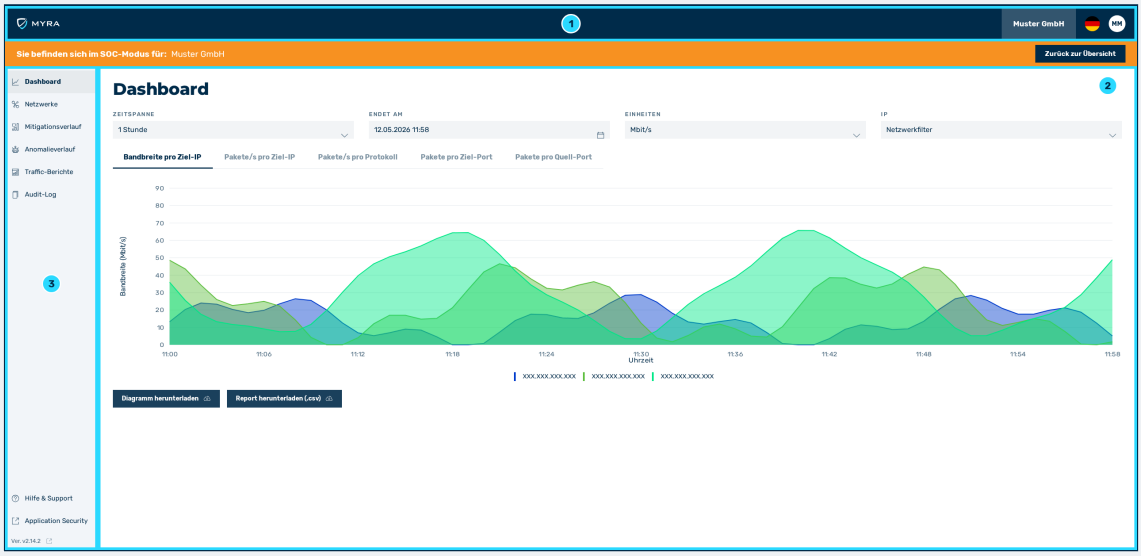


Abbildung 8: Startseite für Unternehmen

Auf der Startseite des jeweiligen Unternehmens können Sie die folgenden Informationen finden:

- Obere Menüleiste mit Zugriff auf die folgenden Schaltflächen (1):
  - Schaltfläche mit dem Namen des Unternehmens für den Zugriff auf die Benutzerverwaltung
  - Schaltfläche mit Flaggensymbol zur Auswahl der Sprache der Benutzeroberfläche
  - Schaltfläche mit Profilbild des Nutzenden zur Verwaltung der eigenen Kontoeinstellungen
  - Im Falle einer Wartung werden hier wichtige Informationen über die Art und Dauer als gesondertes Banner eingeblendet.
- Darstellung des Inhaltes der einzelnen Ansichten (2)
- Reiter mit den folgenden Ansichten (3):
  -  Dashboard
  -  Netzwerk
  -  Mitigationsverlauf
  - Anomalieverlauf
  -  Traffic-Berichte
  -  Audit-Log
  -  Application Security zum Öffnen der Myra App
  - Hilfe & Support zum Öffnen der Online-Hilfe
  - Anzeige der aktuellen Versionsnummer mit Symbol  zum Öffnen der Ansicht **Changelog** (siehe **Ansicht Versionsverlauf**)

Im SOC-Modus agieren Sie als Admin des jeweiligen Unternehmens. Eine orangefarbene Statusleiste unterhalb der oberen Navigationsleiste signalisiert Ihnen, dass Sie sich im SOC-Modus für ein Unternehmen befinden.

Wenn Sie ein Unternehmen geöffnet haben und zurück zur Übersicht alle Unternehmen in der Ansicht **Unternehmenskonten** wollen, müssen Sie die Schaltfläche **Zurück zur Übersicht** verwenden. Der Weg über die Zurücktaste im Browser funktioniert nicht.

Sollten Sie im SOC-Modus eine manuelle Mitigation für ein Unternehmen starten oder andere Änderungen vornehmen, wird dies in den Audit-Logs als Änderung durch Sie als SOC-User festgehalten.

1.3.2.1 Ansicht Dashboard

Abbildung 9: Ansicht Dashboard

Die Ansicht **Dashboard** des jeweiligen Unternehmens bietet Ihnen Zugriff auf verschiedene Traffic-Diagramme, die Ihnen Auskunft über die Netzwerke des Unternehmens geben.

Folgende Diagramme sind in der Ansicht **Dashboard** verfügbar:

Element	Beschreibung
Bandbreite pro Ziel-IP	Dieses Diagramm zeigt die Bandbreite pro Sekunde für die verfügbaren Ziel-IPs an.
Pakete/s pro Ziel-IP	Dieses Diagramm zeigt, wie viele Pakete pro Sekunde an die jeweiligen Ziel-IPs gesendet wurden.
Pakete/s pro Protokoll	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde, gruppiert nach dem Übertragungsprotokoll, an. In der Legende unterhalb des Diagramms finden Sie die Namen der erfassten Protokolle, z. B. ICMP, TCP, UDP.
Pakete pro Ziel-Port	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde für den Ziel-Port an. In der Legende unterhalb der Diagramme finden Sie die Nummern der erfassten Ports.
Pakete pro Quell-Port	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde für den Quell-Port an. In der Legende unterhalb der Diagramme finden Sie die Nummern der erfassten Ports.
Legendenfilter	Zusätzlich zu den Filtern oberhalb der Diagramme gibt es Diagramm-spezifische Filter, die über die Werte in der Legende gesetzt werden können. Folgende Filter sind vorhanden: **IP**: Bandbreite pro Ziel-IP und Pakete/s pro Ziel-IP **Protokoll**: Pakete/s pro Protokoll **Port**: Pakete pro Ziel-Port und Pakete pro Quell-Port

Abbildung 10: Filter im Dashboard

Über Filter haben Sie die Möglichkeit, die dargestellten Daten zu definieren:

Element	Beschreibung
Zeitspanne	Zeigt die Daten pro Sekunde für die ausgewählten Zeitintervalle an: 1 Stunde: Zeigt die Daten pro Sekunde für die ausgewählte Stunde an. (Standardwert) 2 Stunden: Zeigt die Daten pro Sekunde für die ausgewählten 2 Stunden an. 3 Stunden: Zeigt die Daten pro Sekunde für die ausgewählten 3 Stunden an. 4 Stunden: Zeigt die Daten pro Sekunde für die ausgewählten 4 Stunden an. 6 Stunden: Zeigt die Daten pro Sekunde für die ausgewählten 6 Stunden an. 12 Stunden: Zeigt die Daten der ausgewählten 12 Stunden in 10-Sekunden-Gruppen aggregiert an. 24 Stunden: Zeigt die Daten der ausgewählten 24 Stunden in 10-Sekunden-Gruppen aggregiert an. 7 Tage (nur verfügbar für einzelne IP-Adressen): Zeigt die Daten der ausgewählten 7 Tage in Gruppen von einer Stunde aggregiert an.
Endet am	Definiert, bis zu welchem Zeitpunkt die Daten entsprechend dem unter **Zeitspanne** definierten Zeitintervall angezeigt werden sollen. Um das Datum zu ändern, wählen Sie über das Symbol ein Datum und eine Uhrzeit aus. ★ Wählen Sie z. B. als Zeitspanne **1 Stunde** und als Endzeitpunkt **01.08.2024 12:00**, werden Ihnen die Daten für den Zeitraum 01.08.2024 11 Uhr bis 01.08.2024 12 Uhr angezeigt.
Einheiten	Für das Diagramm **Bandbreite pro Ziel-IP** können Sie zwischen den Einheiten **Gbit/s**, **Mbit/s**, **Kbit/s** und **bit/s** wählen. Alle anderen Diagramme verwenden die Einheit Pakete/s, die nicht geändert werden kann.
IP	Ermöglicht die Darstellung für spezifische IP-Adresse oder ganze Netzwerke mit folgenden Werten: Wenn eine konkrete IP-Adresse angegeben wird, zeigt das Diagramm die Daten für diese IP-Adresse an. Wenn eine Subnetzmaske (z. B. /24) eingegeben wird, zeigt das Diagramm die Daten für das gesamte Netzwerk an.

Sie können in jedes Diagramm hineinzoomen, woraufhin der gewählte Zeitabschnitt vergrößert dargestellt wird. Markieren Sie dazu den gewünschten Teilbereich bei gedrückter linker Maustaste.

Zusätzlich können über zwei Schaltflächen die Daten für jedes Diagramm heruntergeladen werden:

- **Diagramm herunterladen**: Lädt das Diagramm als PNG herunter.
- **Report herunterladen (.csv)**: Lädt die Daten aus dem Diagramm als CSV herunter.

1.3.2.2 Ansicht Netzwerke

> Um ein Netzwerk zu erstellen und zu löschen sowie Einstellungen einzusehen und zu ändern, benötigen Sie SOC-Administrationsrechte.

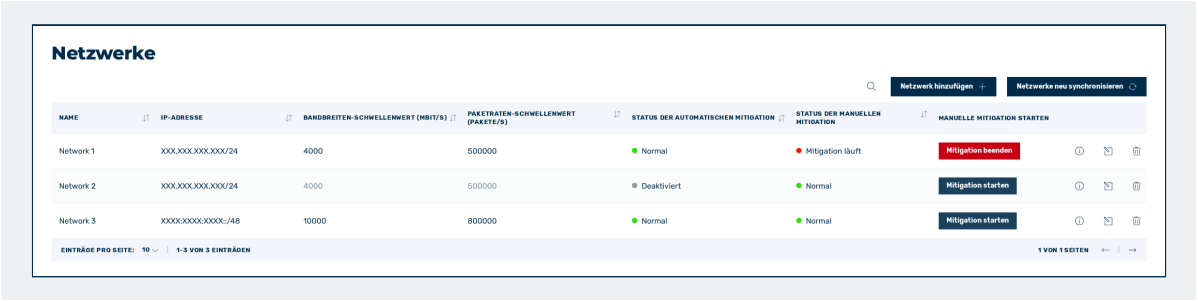


Abbildung 11: Ansicht Netzwerke

In der Ansicht **Netzwerke** erhalten Sie eine Übersicht über die Netzwerke, die IP-Adressbereiche der Netzwerke, das konfigurierte Paketraten-Limit (in Pakete/s), das konfigurierte Bandbreiten-Limit (in MBit/s) und den Status der Mitigation.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Name	Der Name des Netzwerkes.
IP-Adresse	Die IP-Adresse des Netzwerkes.
Bandbreiten-Schwellenwert (MBit/s)	Die maximale Bandbreite, die für Ihr Netzwerk erlaubt ist. Wenn der Schalter für den Netzwerkschutz unter **Automatische Aktionen** deaktiviert ist, erscheinen alle vor der Deaktivierung definierten Werte ausgegraut.

Element	Beschreibung
Paketraten-Schwellenwert (Pakete/s)	Die maximal erlaubte Anzahl von Paketen pro Sekunde, die für das Netzwerk erlaubt sind. ⓘ Wenn der Schalter für den Netzwerkschutz unter **Automatische Aktionen** deaktiviert ist, erscheinen alle vor der Deaktivierung definierten Werte ausgegraut.
Status der automatischen Mitigation	Zeigt den Status der Mitigation an: **Deaktiviert** ⚫: Die automatische Mitigation ist deaktiviert. **Mitigation läuft** 🔴: Eine Mitigation wurde gestartet. **Normal** 🟢: Die Mitigation wurde beendet.
Status der manuellen Mitigation	Zeigt den Status der manuellen Mitigation an: **Mitigation läuft** 🔴: Eine manuelle Mitigation wurde gestartet. **Normal** 🟢: Die manuelle Mitigation wurde beendet.
MANUELLE MITIGATION STARTEN	Öffnet den Dialog **Netzwerk oder IP-Adresse(n) mitigieren**, um die Mitigation für das ausgewählte Netzwerk zu starten.

Zusätzlich haben Sie die folgenden Optionen zur Verwaltung und Konfiguration zur Verfügung:

Element	Beschreibung
🔍	Das Symbol ermöglicht die gezielte Suche nach Namen, IP, Bandbreite und Paketrate.
↓↑	Das Symbol ermöglicht die Sortierung einzelner Spalten.
Netzwerk hinzufügen	Die Schaltfläche öffnet den Dialog **Neues Netzwerk hinzufügen** zum Hinzufügen eines neuen Netzwerkes.
Netzwerke neu synchronisieren	Die Schaltfläche synchronisiert alle Netzwerke.
ⓘ	Das Symbol öffnet den Dialog **Informationen über <Netzwerkname>** zum Einsehen aller gesetzten Einstellungen des ausgewählten Netzwerkes.

Element	Beschreibung
	Das Symbol öffnet den Dialog **Netzwerk bearbeiten** zum Bearbeiten der Einstellungen des ausgewählten Netzwerkes.
	Das Symbol öffnet den Dialog **Netzwerk löschen** zum Löschen des ausgewählten Netzwerkes.
	Das Mitigationssymbol neben der Ansicht **Netzwerke** in der linken Navigationsleiste zeigt an, ob mindestens eine Mitigation läuft.

1.3.2.2.1 Netzwerk ansehen

Um ein Netzwerk zu erstellen und zu löschen sowie Einstellungen einzusehen und zu ändern, benötigen Sie SOC-Administrationsrechte.

Um die Einstellungen für ein Netzwerk einzusehen, gehen Sie wie folgt vor:

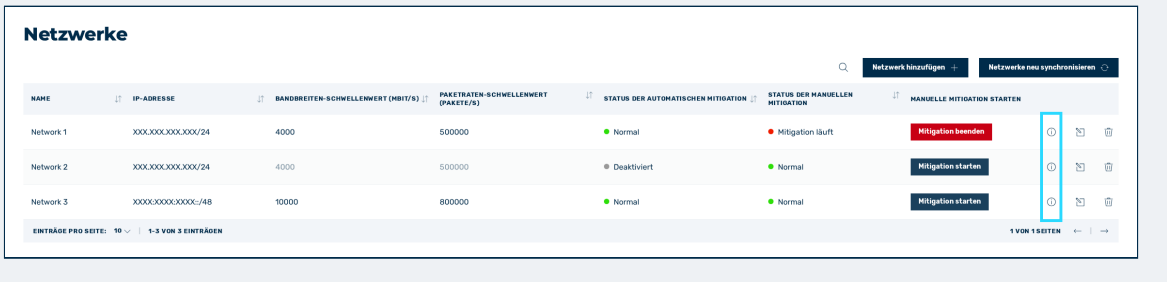


Abbildung 12: Symbol zum Ansehen des Netzwerkes

- ▶ Klicken Sie auf das Symbol ⓘ.
  - ↳ Der Dialog **Informationen über <Name des Netzwerkes>** öffnet sich.

Abbildung 13: Dialog Informationen über Netzwerk

Im Dialog **Informationen über <Name des Netzwerkes>** können Sie die folgenden Informationen einsehen:

Element	Beschreibung
Name	Der Name des Netzwerkes.
IP-Adresse	Die IP-Adresse des Netzwerkes.
Bandbreiten-Schwellenwert (MBit/s)	Der Schwellenwert für die maximale Höhe der möglichen Bandbreite.
Paketraten-Schwellenwert (Pakete/s)	Der Schwellenwert für die maximale Anzahl der erlaubten Pakete pro Sekunde.
Dauer der Mitigation (in Sek)	Die Dauer der Mitigation in Sekunden, nachdem der Datenverkehr unterhalb der Schwellwerte gefallen ist.

Element	Beschreibung
Mitigationstyp	Die Art und Weise, wie die Mitigation durchgeführt wird. Die folgenden Werte sind verfügbar: **CLOUD**: Bei Überschreitung des Schwellenwertes wird der Traffic über das Myra-Rechenzentrum bereinigt.
Mitigationsstrategie	Zeigt an, ob nur eine einzelne IP-Adresse oder das ganze Netzwerk automatisch mitigiert wird. Die folgenden Werte sind verfügbar: **IP**: Es wird nur eine einzelne IP-Adresse des Netzwerkes automatisch mitigiert. **CIDR**: Es wird das komplette Netzwerk automatisch mitigiert.
E-Mail-Adresse für Benachrichtigungen	Die E-Mail-Adresse der Nutzenden, an die Mitteilungen zur Mitigation gehen.
Automatische Aktionen	Zeigt an, ob eine automatische Mitigation für das ausgewählte Netzwerk durchgeführt wird oder nicht. Die folgenden Werte sind verfügbar: **Netzwerkschutz aktiviert**: Die automatische Mitigation ist aktiviert. **Netzwerkschutz deaktiviert**: Die automatische Mitigation ist deaktiviert.
Manuelle Mitigation	Zeigt an, ob für das Netzwerk eine manuelle Mitigation gestartet werden darf. ⓘ Wenn die manuelle Mitigation deaktiviert ist, dann kann die Schaltfläche **Mitigation starten** nicht angeklickt werden.
Subnetz-Mitigation überschreiben	Zeigt an, ob für das Netzwerk die Verwendung von Netzwerken kleiner /32 oder /28 möglich ist.

Für ein Netzwerk im Nur-Daten-Modus zeigt der Dialog ausschließlich **Name** und **IP-Adresse** an. Alle Angaben zu Schwellenwerten und zur Mitigation entfallen, da für das Netzwerk keine Mitigation ausgeführt wird.

1.3.2.2.2 Netzwerk hinzufügen

Um ein Netzwerk zu erstellen und zu löschen sowie Einstellungen einzusehen und zu ändern, benötigen Sie SOC-Administrationsrechte.

Um ein neues Netzwerk der Liste der Netzwerke für ein Unternehmen hinzuzufügen, gehen Sie wie folgt vor:

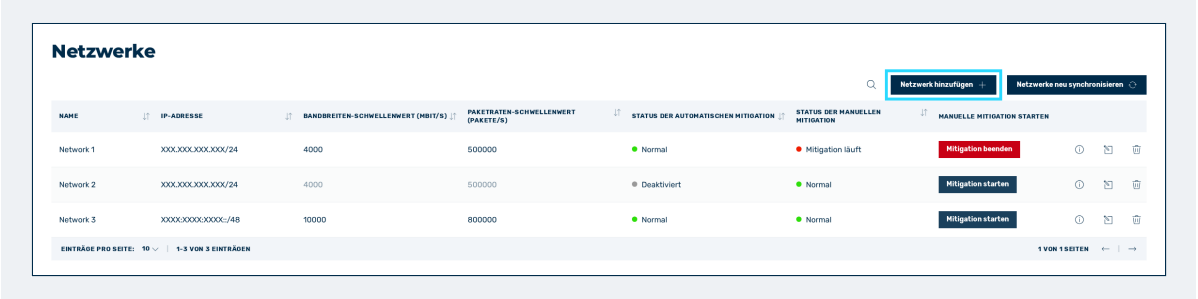


Abbildung 14: Schaltfläche zum Hinzufügen eines Netzwerkes

► Klicken Sie auf die Schaltfläche **Netzwerk hinzufügen**.

↳ Der Dialog **Neues Netzwerk hinzufügen** öffnet sich.

Abbildung 15: Dialog Netzwerk hinzufügen

- Geben Sie ins Feld unter **Name** den Namen des Netzwerkes ein.
- Geben Sie ins Feld unter **IP-Adresse** die IP-Adresse des Netzwerkes ein.
- Geben Sie ins Feld unter **Bandbreiten-Schwellenwert (MBit/s)** die maximal mögliche Bandbreite ein.

> Wenn der Schalter für den Netzwerkschutz unter **Automatische Aktionen** deaktiviert ist, dann können keine Schwellenwerte gesetzt werden.

- Geben Sie ins Feld unter **Paketraten-Schwellenwert (Pakete/s)** die maximale Anzahl der erlaubten Pakete pro Sekunde ein.

> Wenn der Schalter für den Netzwerkschutz unter **Automatische Aktionen** deaktiviert ist, dann können keine Schwellenwerte gesetzt werden.

- Geben Sie ins Feld unter **Dauer der Mitigation (in Sek)** die Dauer der Mitigation in Sekunden, nachdem der Datenverkehr unterhalb der Schwellwerte gefallen ist, an.

- ▶ Wählen Sie in der Drop-down-Liste unter **Mitigationstyp** die entsprechende Mitigationsvariante aus. Die folgenden Werte sind verfügbar:
  - **CLOUD**: Bei Überschreitung des Schwellenwertes wird der Traffic über das Myra-Rechenzentrum bereinigt.
- ▶ Wählen Sie in der Drop-down-Liste unter **Mitigationsstrategie** den entsprechenden Wert aus. Die folgenden Werte sind verfügbar:
  - **IP**: Es wird nur eine einzelne IP-Adresse des Netzwerkes automatisch mitigiert.
  - **CIDR**: Es wird das komplette Netzwerk automatisch mitigiert.
- ▶ Falls erforderlich, geben Sie ins Feld unter **E-Mail-Adresse für Benachrichtigungen** eine E-Mail-Adresse ein.
- ▶ Falls erforderlich, deaktivieren Sie den Schalter für den Netzwerkschutz unter **Automatische Aktionen**.

> ⓘ Wenn der automatische Netzwerkschutz deaktiviert wird, dann wird die Mitigation nicht automatisch gestartet, sondern muss manuell ausgeführt werden.
>
> Das Netzwerk ist trotzdem in der Liste der Netzwerke in der Ansicht **Netzwerke** sichtbar.

- ▶ Falls erforderlich, aktivieren Sie den Schalter für die manuelle Mitigation unter **Manuelle Mitigation**.

> ⓘ Wenn die manuelle Mitigation deaktiviert ist, dann kann die Schaltfläche **Mitigation starten** nicht angeklickt werden.

- ▶ Falls erforderlich, aktivieren Sie den Schalter unter **Nur Daten**.

> ⓘ Im Nur-Daten-Modus wird der Datenverkehr des Netzwerkes ausschließlich aufgezeichnet. Die Felder für die Schwellenwerte, die Dauer der Mitigation, den Mitigationstyp, die Mitigationsstrategie und die E-Mail-Adresse für Benachrichtigungen sowie die Schalter unter **Automatische Aktionen** und **Manuelle Mitigation** werden ausgeblendet. Für das Netzwerk wird keine Mitigation ausgeführt.

- ► Falls erforderlich, aktivieren Sie den Schalter unter **Subnetz-Mitigation überschreiben** für die Nutzung von IPv4 /28 und IPv6 /32 großen Netzwerken.
- ► Klicken Sie auf die Schaltfläche **Speichern**.
- → Das neue Netzwerk wird angelegt und die Daten zum Traffic erscheinen in der Ansicht **Dashboard**.

1.3.2.2.3 Netzwerk ändern

> Um ein Netzwerk zu erstellen und zu löschen sowie Einstellungen einzusehen und zu ändern, benötigen Sie SOC-Administrationsrechte.

Um ein vorhandenes Netzwerk zu ändern, gehen Sie wie folgt vor:

Abbildung 16: Symbol zum Bearbeiten des Netzwerkes

- ► Klicken Sie auf das Symbol .
  - ↳ Der Dialog **Netzwerk bearbeiten** öffnet sich.

Abbildung 17: Dialog Netzwerk bearbeiten

- ▶ Passen Sie die Daten nach Bedarf an.

> Wenn eine Mitigation läuft, dann kann die manuelle Mitigation nicht deaktiviert werden.

- ▶ Klicken Sie auf die Schaltfläche **Speichern**.
- → Eine Meldung bestätigt das erfolgreiche Ändern der Einstellungen des Netzwerkes.

1.3.2.2.4 Netzwerk löschen

> Um ein Netzwerk zu erstellen und zu löschen sowie Einstellungen einzusehen und zu ändern, benötigen Sie SOC-Administrationsrechte.

Um ein Netzwerk zu löschen, gehen Sie wie folgt vor:

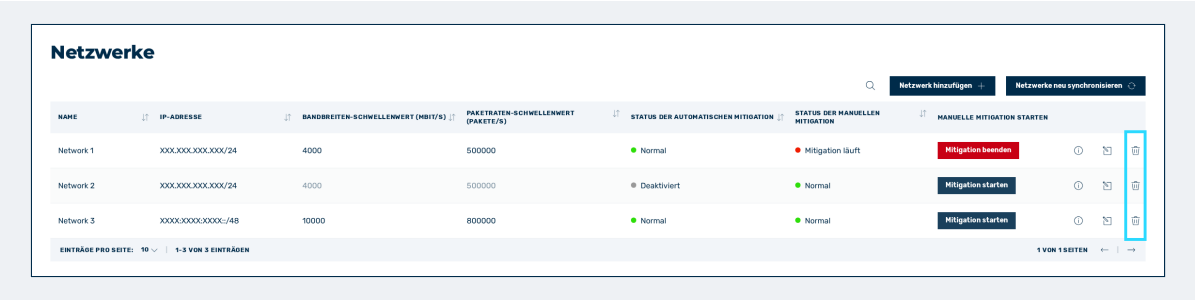


Abbildung 18: Dialog zum Löschen des Netzwerkes

► Klicken Sie auf das Symbol .

↳ Die Ansicht **Netzwerk löschen** öffnet sich.

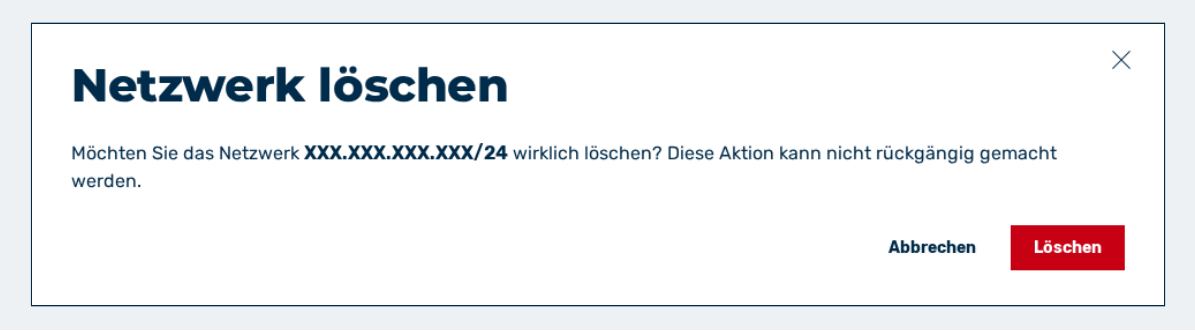


Abbildung 19: Dialog Netzwerk löschen

► Klicken Sie auf die Schaltfläche **Löschen**.

➔ Eine Meldung bestätigt das erfolgreiche Löschen des Netzwerkes und das Netzwerk verschwindet aus der Liste der Netzwerke.

1.3.2.2.5 Manuelle Mitigationen starten

Mitigationen sind nur für das gesamte Netzwerk möglich.

Das Starten einer manuellen Mitigation ist nur möglich, wenn diese für das Netzwerk vom SOC-Admin aktiviert wurde.

Sollten Sie den Verdacht haben, dass ein Unternehmen Ziel eines Angriffes geworden ist, können Sie jederzeit eine manuelle Mitigation starten.

Um eine manuelle Mitigation zu starten, gehen Sie wie folgt vor:

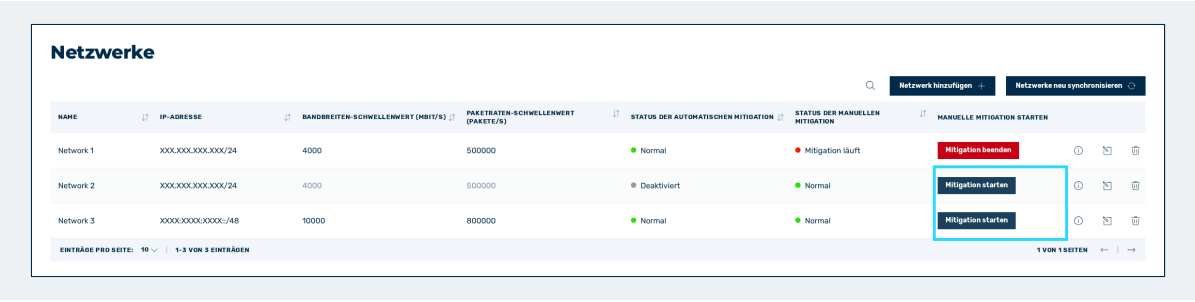


Abbildung 20: Schaltflächen für den Start einer Mitigation

► Klicken Sie auf die Schaltfläche **Mitigation starten**.

↳ Der Dialog **Netzwerk oder IP-Adresse(n) mitigieren** öffnet sich.

Abbildung 21: Dialog Netzwerk oder IP-Adresse(n) mitigieren

► Klicken Sie auf die Schaltfläche **Mitigation starten**.

➔ Eine Meldung bestätigt den erfolgreichen Start der Mitigation.

Neben der Ansicht **Netzwerke** in der linken Navigationsleiste wird das Mitigationssymbol angezeigt und in der Spalte **Status der manuellen Mitigation** wechselt der Status zu einem der folgenden Werte:

- **Mitigation läuft**: Die manuelle Mitigation wurde für das gesamte Netzwerk gestartet

Im Falle einer manuellen Mitigation erfolgt eine Umleitung des Traffics über das Scrubbing Center, Angriffe werden mitigiert oder blockiert und Sie erhalten eine Benachrichtigung per E-Mail.

Das Mitigationssymbol neben der Ansicht **Netzwerke** in der linken Navigationsleiste bleibt so lange bestehen, wie Mitigationen vom Myra DataHub ausgeführt werden. Das Mitigaionssymbol verschwindet erst, wenn alle laufenden Mitigationen beendet wurden.

1.3.2.2.6 Manuelle Mitigationen beenden

Um eine manuell gestartete Mitigation zu beenden, gehen Sie wie folgt vor:

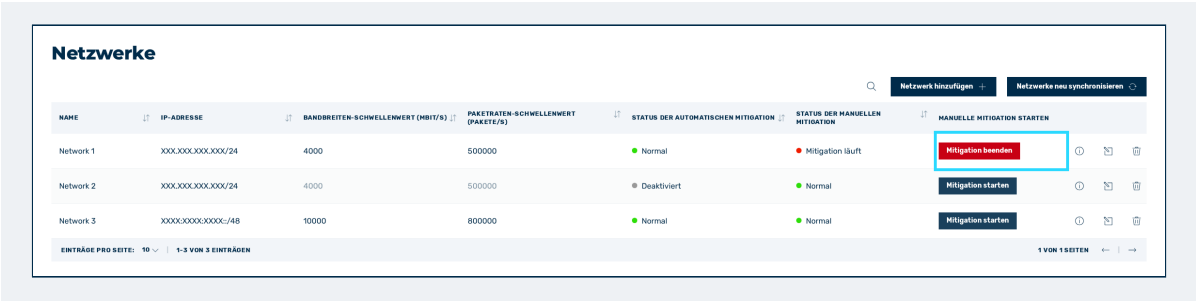


Abbildung 22: Schaltflächen zum Beenden einer Mitigation

- Klicken Sie auf die Schaltfläche **Mitigation beenden** oder Schaltfläche **(X) Mitigation(en) beenden**.
  - ↳ Der Dialog **Netzwerk oder IP-Adresse(n) mitigieren** öffnet sich.
- Klicken Sie auf die Schaltfläche **Mitigation beenden**.

Abbildung 23: Dialog zum Beenden einer Mitigation - gesamtes Netzwerk

Das Mitigationssymbol neben der Ansicht **Netzwerke** in der linken Navigationsleiste bleibt so lange bestehen, wie Mitigationen vom Myra DataHub ausgeführt werden. Das Mitigaionssymbol verschwindet erst, wenn alle laufenden Mitigationen beendet wurden.

1.3.2.3 Ansicht Mitigationsverlauf

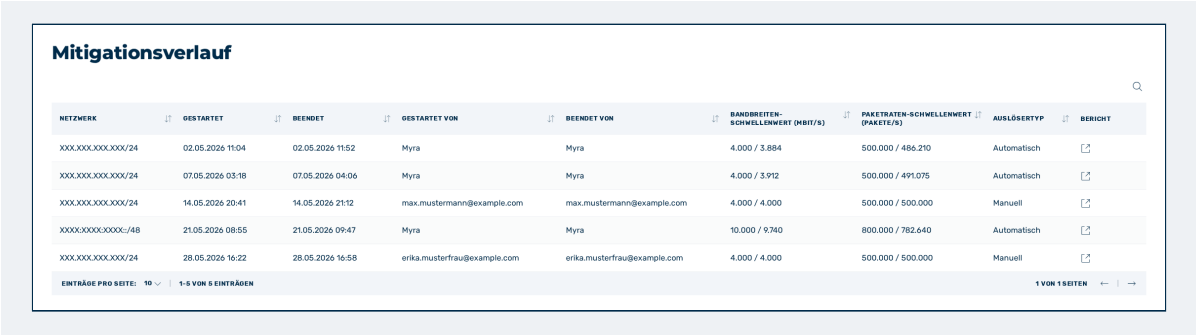


Abbildung 24: Ansicht Mitigationsverlauf

In der Ansicht **Mitigationsverlauf** erhalten Sie eine Übersicht über alle erfolgten Mitigationen, die automatisch oder manuell ausgelöst wurden. Für jede abgeschlossene Mitigation können Sie einen Mitigationsbericht abrufen.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Netzwerk	Die IP-Adresse des Netzwerkes.
Gestartet	Der Zeitpunkt mit Datum und Uhrzeit, zu dem die Mitigation gestartet wurde.
Beendet	Der Zeitpunkt mit Datum und Uhrzeit, zu dem die Mitigation beendet wurde.
Gestartet von	Zeigt an, wer die manuelle Mitigation gestartet hat.
Beendet von	Zeigt an, wer die manuelle Mitigation beendet hat.
Bandbreiten-Schwellenwert (MBit/s)	Zeigt während einer automatischen Mitigation den definierten Bandbreiten-Schwellenwert und die Überschreitung des Schwellenwertes an.
Paketraten-Schwellenwert (Pakete/s)	Zeigt während einer automatischen Mitigation den definierten Paketraten-Schwellenwert und die Überschreitung des Schwellenwertes an.
Auslösertyp	Zeigt an, ob die Mitigation manuell oder automatisch gestartet wurde.
Bericht	

Element	Beschreibung
	Ermöglicht über das Symbol das Öffnen des Mitigationsberichtes in einem neuen Fenster.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
	Das Symbol ermöglicht die gezielte Suche nach Namen, IP, Bandbreite und Paketrate.

1.3.2.3.1 Mitigationsberichte öffnen

Um den Mitigationsbericht zu öffnen, führen Sie den folgenden Schritt aus:

- ▶ Klicken Sie auf das Symbol in der Spalte **Bericht**.
- → Die Ansicht **Bericht - <Name des Berichtes> (<Name des Unternehmens>)** öffnet sich.

1.3.2.3.2 Ansicht Mitigationsberichte

Abbildung 25: Ansicht Mitigationsberichte

Die Ansicht **Bericht - <Name des Berichtes> (<Name des Unternehmens>)** stellt eine Übersicht über die einzelnen Daten zur Verfügung, die während der erfolgreichen Mitigation erfasst wurden.

Folgende Informationen werden Ihnen in der Tabelle **Details** angezeigt:

Element	Beschreibung
Netzwerk	Die IP-Adresse des Netzwerkes.
Mitigationzeitraum	Zeigt die Zeitspanne an, in der die Mitigation durchgeführt wurde.
Bandbreite – Konfigurierter Schwellenwert	Zeigt den konfigurierten Bandbreiten-Schwellenwert an, bei dem die automatische Mitigation ausgelöst wird.
Bandbreite – Ausgelöst durch	Zeigt den Wert an, der die automatische Mitigation bei Überschreitung des Bandbreiten-Schwellenwertes ausgelöst hat.
Bandbreite – Maximal	Zeigt den Spitzenwert während der Mitigation an.
Pakete – Konfigurierter Schwellenwert	Zeigt den konfigurierten Paketraten-Schwellenwert an, bei dem die automatische Mitigation ausgelöst wird.
Pakete – Ausgelöst durch	Zeigt den Wert an, der die automatische Mitigation bei Überschreitung des Paketraten-Schwellenwertes ausgelöst hat.
Pakete – Maximal	Zeigt den Spitzenwert während der Mitigation an.
Auslösertyp	Zeigt an, ob die Mitigation manuell oder automatisch gestartet wurde.

Darüber hinaus umfasst der Mitigationsbericht sieben Diagramme, die die folgenden Zeiträume abbilden:

- Auslastung des Netzwerkes der ersten 24 Stunden vor dem Start der Mitigation
- Auslastung des Netzwerkes vom Start bis zum Ende der Mitigation

Folgende Diagramme sind verfügbar:

Element	Beschreibung
Bandbreite	

Element	Beschreibung
pro Ziel-IP	Dieses Diagramm zeigt die Bandbreite pro Sekunde für die verfügbaren Ziel-IPs an.
Pakete/s pro Ziel-IP	Dieses Diagramm zeigt, wie viele Pakete pro Sekunde an die jeweiligen Ziel-IPs gesendet wurden.
Pakete/s pro Protokoll	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde, gruppiert nach dem Übertragungsprotokoll, an. In der Legende unterhalb des Diagramms finden Sie die Namen der erfassten Protokolle, z. B. ICMP, TCP, UDP.
Pakete pro Ziel-Port	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde für den Ziel-Port an. In der Legende unterhalb der Diagramme finden Sie die Nummern der erfassten Ports.
Pakete pro Quell-Port	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde für den Quell-Port an. In der Legende unterhalb der Diagramme finden Sie die Nummern der erfassten Ports.
Legendenfilter	Zusätzlich zu den Filtern oberhalb der Diagramme gibt es Diagramm-spezifische Filter, die über die Werte in der Legende gesetzt werden können. Folgende Filter sind vorhanden: **IP**: Bandbreite pro Ziel-IP und Pakete/s pro Ziel-IP **Protokoll**: Pakete/s pro Protokoll **Port**: Pakete pro Ziel-Port und Pakete pro Quell-Port

Über die Schaltfläche **Bericht herunterladen** können Sie die Berichte als PDF herunterladen.

1.3.2.4 Ansicht Anomalieverlauf

Die Ansicht **Anomalieverlauf** erscheint nur, wenn für das Unternehmen die Anomalie-Funktion aktiviert ist (siehe **Unternehmen ändern**).

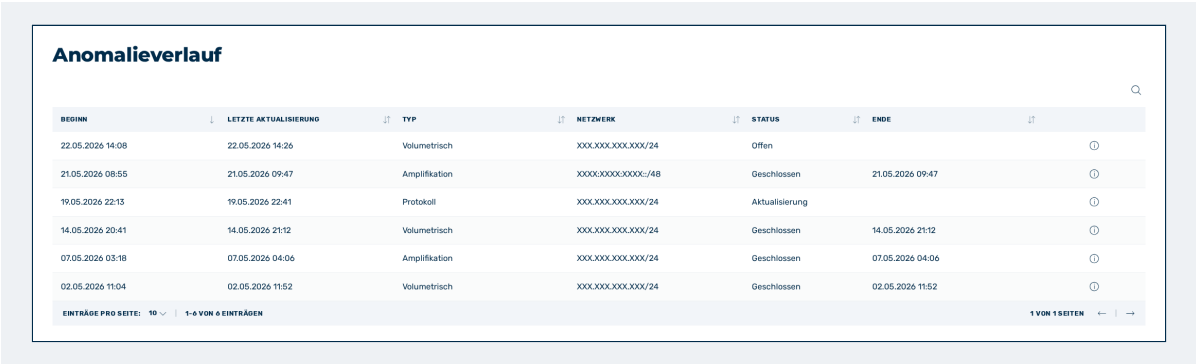


Abbildung 26: Ansicht Anomalieverlauf

In der Ansicht **Anomalieverlauf** erhalten Sie eine Übersicht über alle erkannten Anomalien im Datenverkehr Ihrer Netzwerke. Die Einträge sind standardmäßig nach dem Beginn der Anomalie absteigend sortiert.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Beginn	Der Zeitpunkt mit Datum und Uhrzeit, zu dem die Anomalie erkannt wurde.
Letzte Aktualisierung	Der Zeitpunkt mit Datum und Uhrzeit, zu dem der Eintrag zuletzt aktualisiert wurde.
Typ	Die Art der erkannten Anomalie. Die folgenden Werte sind verfügbar: **Volumetrisch**: Eine Traffic-Flut, die Ihre Bandbreite oder Paketkapazität allein durch das schiere Volumen auslasten soll, unabhängig vom verwendeten Protokoll — zum Beispiel extreme Traffic-Spitzen oder Fluten von einer großen Zahl verteilter Quelladressen. **Protokoll**: Ein Angriff, der die Funktionsweise eines Netzwerkprotokolls oder des Verbindungsaufbaus missbraucht, um Verbindungstabellen, Zustände oder Verarbeitungsressourcen statt der Bandbreite zu erschöpfen — zum Beispiel SYN-Floods oder anderer anomaler TCP- und UDP-Traffic.

Element	Beschreibung
	Amplifikation: Ein Angriff, bei dem Server Dritter im Internet dazu verleitet werden, große Antworten mit gefälschtem Absender an Ihre Adresse zu senden, sodass aus einer kleinen Anfrage eine sehr viel größere Flut wird — zum Beispiel DNS-Reflection. ⓘ Die Ansicht zeigt für eine Anomalie gegebenenfalls mehrere Typen gleichzeitig an.
Netzwerk	Das Netzwerk in CIDR-Notation, in dem die Anomalie erkannt wurde.
Status	Der aktuelle Status der Anomalie. Die folgenden Werte sind verfügbar: **Offen**: Myra hat die Anomalie erkannt und die Anomalie dauert an. **Aktualisierung**: Zur Anomalie liegen neue Informationen vor. **Geschlossen**: Die Anomalie ist beendet.
Ende	Der Zeitpunkt mit Datum und Uhrzeit, zu dem die Anomalie beendet wurde.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
ⓘ	Das Symbol **Details anzeigen** öffnet den Dialog **Anomaliedetails** für den ausgewählten Eintrag.
🔍	Das Symbol ermöglicht die Suche nach Typ, Netzwerk und Status.

ⓘ Wenn keine Anomalien vorliegen, zeigt die Ansicht den Text **Keine Anomalien gefunden.** an.

1.3.2.4.1 Dialog Anomaliedetails

Abbildung 27: Dialog Anomaliedetails

Im Dialog **Anomaliedetails** können Sie die folgenden Informationen zu einer Anomalie einsehen:

Element	Beschreibung
Netzwerk	Das Netzwerk in CIDR-Notation, in dem die Anomalie erkannt wurde.
Typ	Die Art der erkannten Anomalie.
Status	Der aktuelle Status der Anomalie.
Beginn	Der Zeitpunkt mit Datum und Uhrzeit, zu dem die Anomalie erkannt wurde.
Letzte Aktualisierung	Der Zeitpunkt mit Datum und Uhrzeit, zu dem der Eintrag zuletzt aktualisiert wurde.
Ende	Der Zeitpunkt mit Datum und Uhrzeit, zu dem die Anomalie beendet wurde.
	Weitere von der Erkennung gelieferte Angaben zur Anomalie.

Element	Beschreibung
Zusätzliche Informationen	Wenn keine weiteren Angaben vorliegen, zeigt der Bereich den Text **Keine zusätzlichen Informationen verfügbar.** an.

1.3.2.5 Ansicht Traffic-Berichte

Abbildung 28: Ansicht Traffic-Berichte

In der Ansicht **Traffic-Berichte** erhalten Sie pro IP-Adresse für den gewählten Zeitraum eine Übersicht des Traffics.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
IP	Eine spezifische IP-Adresse.
CIDR	Das Netzwerk, dem die IP-Adresse zugewiesen ist.
GESAMTER TRAFFIC	Zeigt den gesamten Traffic an, der über diese IP-Adresse gelaufen ist.
PAKETE GESAMT	Zeigt die Summe aller Pakete an, die über diese IP-Adresse empfangen wurden.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
Art des Berichtes	Über die Drop-Down-Liste für die Art des Berichtes können Sie einstellen, ob Sie pro IP-Adresse eine Auswertung für einen bestimmten Tag oder den aktuellen Monat erhalten wollen.

Element	Beschreibung
Datum	Definiert den Tag für den Sie die Übersicht des Traffics pro IP-Adresse erhalten wollen. Die Drop-Down-Liste ist nur verfügbar, wenn Sie als Art des Berichtes **Täglich** ausgewählt haben.
	Das Symbol ermöglicht die gezielte Suche nach dem Namen des Berichtes.
CSV herunterladen	Die Schaltfläche lädt den kompletten Bericht als CSV-Datei herunter.

1.3.2.6 Ansicht Audit-Log

Um den Audit-Log einsehen zu können, benötigen Sie Admin-Rechte.

Abbildung 29: Ansicht Audit-Log

In der Ansicht **Audit-Log** erhalten Sie detaillierte Informationen über alle Änderungen, die für das eigene Unternehmen vorgenommen wurden.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Erstellt	Die Uhrzeit und das Datum zu der die Änderung vorgenommen wurde.

Element	Beschreibung
Ausgeführt durch	Der Name des Nutzenden.
Event	Die Art der Tätigkeit. **CREATED**: Ein neuer Eintrag wurde erstellt. **UPDATED**: Ein vorhandener Eintrag wurde geändert. **DELETED**: Ein vorhandener Eintrag wurde gelöscht.
Ressource	Der Ort der Änderung.
Ressourcen-ID	Der Eintrag, der geändert wurde.
Parameter	Die Werte des entsprechenden Eintrages, die geändert wurden.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
	Das Symbol filter nach dem Namen des Berichtes.
CSV herunterladen	Die Schaltfläche lädt den kompletten monatlichen Bericht als CSV-Datei herunter.

1.3.3 Benutzerverwaltung

Im Myra DataHub gibt es zwei Arten von Benutzerverwaltung. Sie haben eine Benutzerverwaltung zum Anlegen von SOC-Usern und eine Benutzerverwaltung pro Unternehmen für die Kunden.

Je nachdem, für wen Sie ein neues Konto anlegen wollen, gehen Sie wie folgt vor:

Konto für einen SOC-User:

- ► Öffnen Sie die Website des Myra DataHub.
- ► Loggen Sie sich ein.
  - ↳ Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.

Abbildung 30: Öffnen der Benutzerverwaltung – Variante 1

- ► Klicken Sie oben rechts auf den Namen des Unternehmens.
- ➔ Die Ansicht **Benutzerverwaltung** öffnet sich.

Konto für Unternehmen

- ► Öffnen Sie die Website des Myra DataHub.
- ► Loggen Sie sich ein.
  - ↳ Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.
- ► Klicken Sie auf den Namen eines Unternehmens.
  - ↳ Die Ansicht **Dashboard** des jeweiligen Unternehmens öffnet sich.

Abbildung 31: Öffnen der Benutzerverwaltung – Variante 1

- ► Klicken Sie oben rechts auf den Namen des Unternehmens.
- ➔ Die Ansicht **Benutzerverwaltung** öffnet sich.

1.3.3.1 Ansicht Benutzerverwaltung

In der Ansicht **Benutzerverwaltung** können Sie neue Nutzende einsehen, verwalten und löschen. Außerdem können Sie für das Unternehmen die SIEM-Einstellungen anpassen und die Empfänger der Benachrichtigungen verwalten.

Die Ansicht enthält die folgenden Reiter:

- Benutzerverwaltung
- SIEM-Einstellungen
- Benachrichtigungen

1.3.3.2 Reiter Benutzerverwaltung

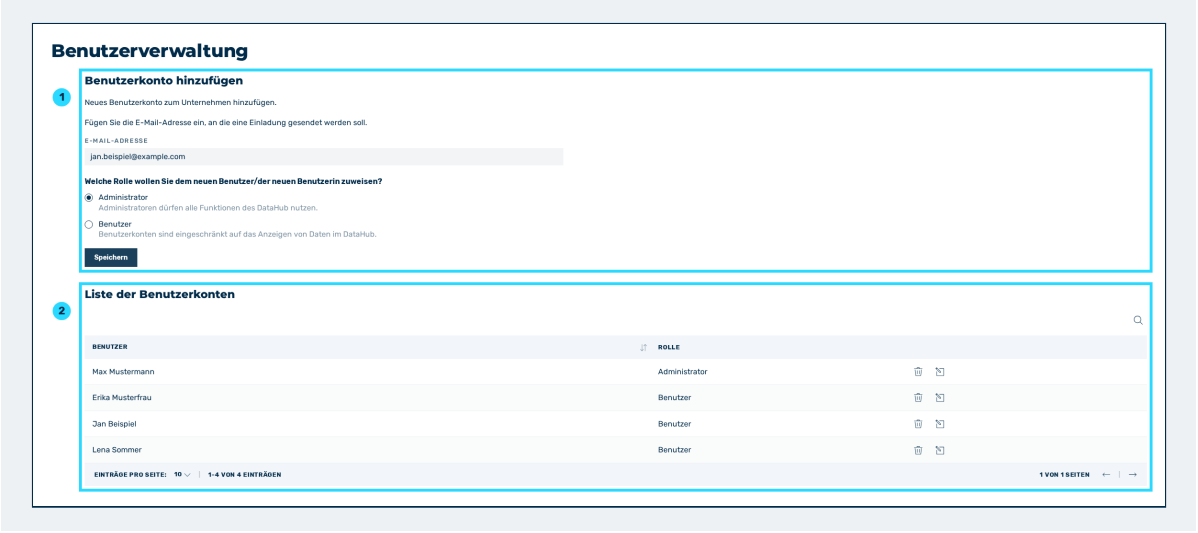


Abbildung 32: Ansicht Benutzerverwaltung

Im Reiter **Benutzerverwaltung** finden Sie eine Übersicht aller Informationen und Einstellungen, die Sie für die Verwaltung der Nutzenden eines Unternehmens zur Verfügung haben.

Der Reiter **Benutzerverwaltung** umfasst zwei Bereiche:

- **Benutzerkonto hinzufügen**

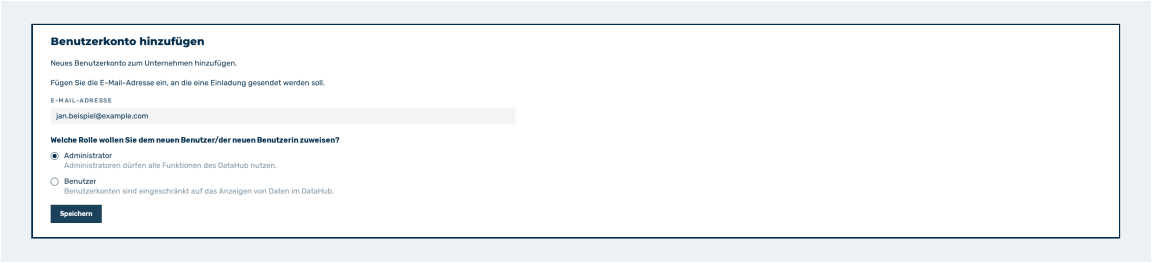


Abbildung 33: Bereich Benutzerkonto hinzufügen

Ermöglicht die Erstellung neuer Nutzenden mit Admin- und Benutzerrechten. Siehe **Konto hinzufügen**.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
BENUTZER	Der Name der Nutzenden. ⓘ Beim Hinzufügen eines neuen Nutzenden wird der Name vor dem @-Symbol als Name des Nutzenden im System hinterlegt. Der Name kann nachträglich vom Admin (siehe Ansicht Benutzerverwaltung im **Handbuch Myra App**) oder dem Nutzenden selbst (siehe Dialog Benutzer <E-Mail-Adresse> bearbeiten im **Handbuch Myra App**) angepasst werden.
ROLLE	Die Berechtigungen, die die Nutzenden im Unternehmen haben. Die folgenden Werte sind verfügbar: **Administrator**: Nutzende mit der Rolle **Administrator** dürfen jede Portalfunktion nutzen. **Benutzer**: Nutzende mit der Rolle **Benutzer** sind eingeschränkt und dürfen nur Daten einsehen.

Liste der Benutzerkonten

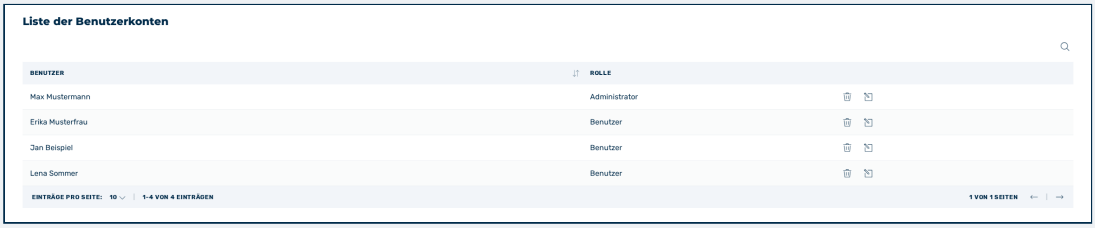


Abbildung 34: Bereich Liste der Benutzerkonten

Zeigt alle angelegten Nutzenden des Unternehmens an.

Außerdem sind die folgenden Optionen verfügbar:

Element	Beschreibung
	Das Symbol öffnet den Dialog **Benutzerkonto löschen** zum Löschen des ausgewählten Nutzenden.
	Das Symbol öffnet den Dialog **Benutzerkonto aktualisieren** zum Ändern des Namens und der Rolle des Nutzenden.
	Das Symbol ermöglicht die gezielte Suche nach Namen von Nutzenden.

1.3.3.2.1 Konto hinzufügen

> Es können nur Konten hinzugefügt werden, die bereits in der Myra App angelegt wurden.

Um ein Konto hinzuzufügen, gehen Sie wie folgt vor:

- ▶ Navigieren Sie zum Bereich **Benutzerkonto hinzufügen**.

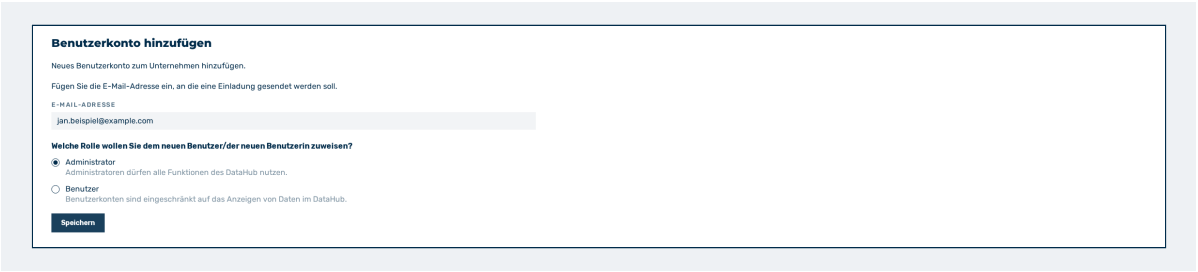


Abbildung 35: Bereich Benutzerkonto hinzufügen

- ► Klicken Sie auf die Drop-Down-Liste **Benutzer auswählen**.
- ► Wählen Sie einen Nutzenden aus der Liste aus oder suchen Sie nach einem spezifischen Nutzenden.
- ► Wählen Sie unter **Welche Rolle wollen Sie dem neuen Benutzer/der neuen Benutzerin zuweisen?** die entsprechende Rechtegruppe aus.

  Sie haben zwei Rechtegruppen zur Auswahl:

  - ↳ **Administrator**: Nutzende mit der Rolle **Administrator** dürfen jede Portalfunktion nutzen.
  - ↳ **Benutzer**: Nutzende mit der Rolle **Benutzer** sind eingeschränkt und dürfen nur Daten einsehen.
- ► Klicken Sie auf die Schaltfläche **Speichern**.
- → Eine Meldung bestätigt das erfolgreiche Anlegen des Nutzenden. Der neue Eintrag ist auch in der Liste der Konten sichtbar.

1.3.3.2.2 Konto ändern

Um ein Konto zu ändern, gehen Sie wie folgt vor:

- ► Navigieren Sie zum Bereich **Liste der Benutzerkonten**.

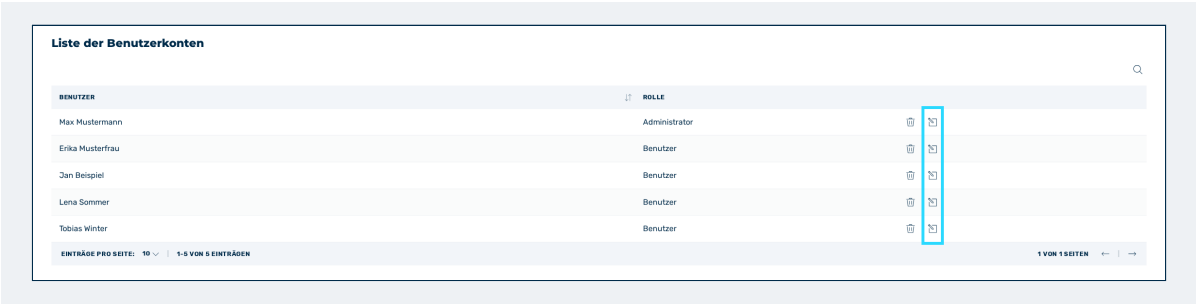


Abbildung 36: Bereich Liste der Benutzerkonten

- ► Klicken Sie neben das entsprechende Konto auf das Symbol  .
  - ↳ Der Dialog **Benutzerkonto aktualisieren** öffnet sich.

Abbildung 37: Dialog Benutzerkonto aktualisieren

- ▸ Falls erforderlich, ändern Sie unter **Name** den Namen des Nutzenden.
- ▸ Falls erforderlich, ändern Sie unter Rolle die Berechtigung des Nutzenden.

  Sie haben zwei Rechtegruppen zur Auswahl:

  - ↳ **Administrator**: Nutzende mit der Rolle **Administrator** dürfen jede Portalfunktion nutzen.
  - ↳ **Benutzer**: Nutzende mit der Rolle **Benutzer** sind eingeschränkt und dürfen nur Daten einsehen.
- ▸ Klicken Sie auf die Schaltfläche **Speichern**.
- ➔ Eine Meldung bestätigt das erfolgreiche Ändern des Kontos.

1.3.3.3 Reiter SIEM-Einstellungen

ⓘ Für die Anzeige des Reiters SIEM-Einstellungen muss die Option zur Nutzung vom SIEM in den Organisationseinstellungen aktiviert werden.

Im Reiter **SIEM-Einstellungen** finden Sie eine Übersicht aller Informationen und Einstellungen, die Sie für die Verwaltung der Nutzenden eines Unternehmens zur Verfügung haben.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
SIEM-Anbieter	Definiert den SIEM-Anbieter. ⓘ Aktuell wird als HTTP-Event-Collector (HEC) nur Splunk unterstützt.
Host	Definiert den Namen des Host für die Übertragung der Daten.
Port	Definiert den Port des Hosts für die Verbindung zur Übertragung der Daten.
API-Token	Definiert den API-Token für die Authentifizierung beim Host. ⓘ Der verwendete API-Token muss ein HEX-Token sein.

Die folgenden Informationen werden bei Aktivierung von SIEM im SIEM-Log angezeigt:

Erfasste Daten im SIEM-Log

Funktion	Event
Unternehmen	Unternehmen ändern
Netzwerke	Netzwerk hinzufügen
	Netzwerk bearbeiten
	Netzwerk löschen
Mitigation	Automatische Mitigation gestartet
	Automatische Mitigation beendet
	Manuelle Mitigation starten
	Manuelle Mitigation beenden
Benutzerverwaltung	Konto hinzufügen
	Konto löschen
	E-Mail verifizieren
	Passwort zurücksetzen

Funktion	Event
	2FA aktivieren und deaktivieren

Die folgenden Informationen werden nicht im SIEM-Log angezeigt:

Funktion	Event
Unternehmen	Unternehmen bearbeiten
SOC-Modus	SOC-Nutzer/Admin hinzufügen
	SOC-Nutzer/Admin löschen
	E-Mail verifizieren
	Passwort zurücksetzen
	2FA aktivieren und deaktivieren

1.3.3.4 Reiter Benachrichtigungen

Der Reiter **Benachrichtigungen** wird nicht angezeigt, wenn Sie als SOC-Nutzender die Benutzerverwaltung Ihres eigenen SOC-Unternehmens geöffnet haben.

Im Reiter **Benachrichtigungen** sehen Sie, welche Nutzenden des Unternehmens E-Mail-Benachrichtigungen zu Anomalien und Mitigationen erhalten. Außerdem können Sie zusätzliche Empfänger hinzufügen, die keine Nutzenden der Anwendung sind.

Der Reiter teilt sich in die folgenden Bereiche:

1.3.3.4.1 Bereich Benachrichtigungen

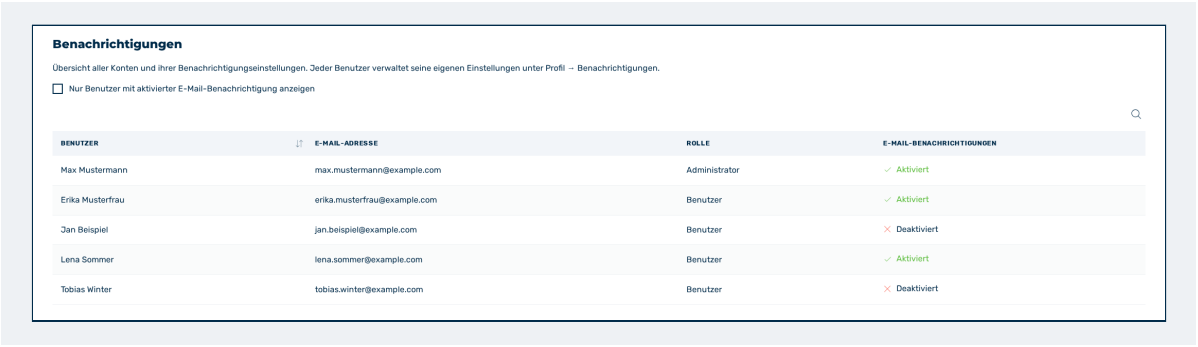


Abbildung 38: Bereich Benachrichtigungen

Der Bereich **Benachrichtigungen** enthält eine Übersicht aller Konten und ihrer Benachrichtigungseinstellungen. Jeder Nutzende verwaltet seine eigenen Einstellungen unter **Persönliches Konto** → **Benachrichtigungen** (siehe Reiter Benachrichtigungen).

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Benutzer	Der Name des Nutzenden.
E-Mail-Adresse	Die E-Mail-Adresse des Nutzenden.
Rolle	Die Benutzerrolle des Nutzenden im Unternehmen.
E-Mail-Benachrichtigungen	Zeigt an, ob der Nutzende E-Mail-Benachrichtigungen erhält. Die folgenden Werte sind verfügbar: **Aktiviert**: Der Nutzende erhält E-Mail-Benachrichtigungen. **Deaktiviert**: Der Nutzende erhält keine E-Mail-Benachrichtigungen.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
Nur Benutzer mit aktivierter E-Mail-Benachrichtigung anzeigen	Das Kontrollkästchen blendet alle Nutzenden ohne aktivierte E-Mail-Benachrichtigung aus.

Bei gesetztem Kontrollkästchen zeigt eine Markierung daneben die Anzahl der Nutzenden mit aktivierter E-Mail-Benachrichtigung an. Wenn kein Nutzender dem gesetzten Filter entspricht, dann zeigt der Bereich den Text **Keine Benutzer entsprechen dem aktuellen Filter.** an.

1.3.3.4.2 Bereich Zusätzliche Kontakte

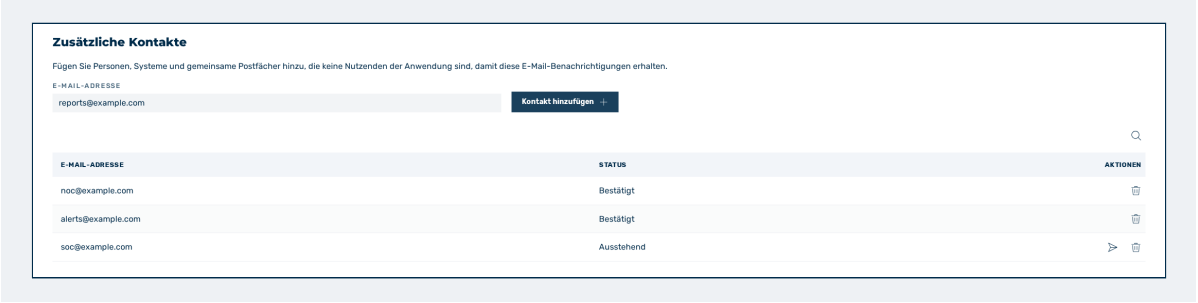


Abbildung 39: Bereich Zusätzliche Kontakte

Im Bereich **Zusätzliche Kontakte** fügen Sie Personen, Systeme und gemeinsame Postfächer hinzu, die keine Nutzenden der Anwendung sind, damit diese E-Mail-Benachrichtigungen erhalten.

Um einen zusätzlichen Kontakt hinzuzufügen, gehen Sie wie folgt vor:

- ▶ Geben Sie ins Feld unter **E-Mail-Adresse** die E-Mail-Adresse des Kontaktes ein.
- ▶ Klicken Sie auf die Schaltfläche **Kontakt hinzufügen**.
- ➔ Der Kontakt wird der Liste hinzugefügt und eine Bestätigungs-E-Mail wird gesendet. Der Kontakt bleibt so lange im Status **Ausstehend**, bis er bestätigt wurde.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
E-Mail-Adresse	Die E-Mail-Adresse des Kontaktes.
Status	Der Status des Kontaktes. Die folgenden Werte sind verfügbar: **Bestätigt**: Der Kontakt hat die Bestätigungs-E-Mail bestätigt und erhält Benachrichtigungen. **Ausstehend**: Der Kontakt hat die Bestätigungs-E-Mail noch nicht bestätigt.

Element	Beschreibung
Aktionen	Die verfügbaren Aktionen für den Kontakt.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
Bestätigungs-E-Mail erneut senden	Das Symbol sendet eine neue Bestätigungs-E-Mail an den Kontakt. ⓘ Das Symbol wird nur für Kontakte im Status **Ausstehend** angezeigt.
Kontakt entfernen	Das Symbol öffnet den Dialog **Kontakt entfernen** zum Löschen des ausgewählten Kontaktes.

ⓘ Wenn noch keine zusätzlichen Kontakte hinterlegt sind, dann zeigt der Bereich den Text **Noch keine zusätzlichen Kontakte.** an.

1.3.4 Persönliches Konto

Wenn Sie Ihre Profilinformationen anzeigen oder ändern wollen, gehen Sie wie folgt vor:

- ▸ Öffnen Sie die Website des Myra DataHub.
- ▸ Loggen Sie sich ein.
  - ↳ Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.
- ▸ Klicken Sie oben rechts auf die Schaltfläche mit Ihrem Profilbild.

Abbildung 40: Optionen unter dem Profilbild

- ▸ Klicken Sie im Menü auf den Menüpunkt **Persönliches Konto**.
- ➔ Die Ansicht **Persönliches Konto** öffnet sich.

Die Ansicht **Persönliches Konto** verfügt über die folgenden Reiter:

- Profil
- Benachrichtigungen
- API-Token

1.3.4.1 Reiter Profil

Im Reiter **Profil** finden Sie eine Übersicht aller Informationen und Einstellungen, die Sie für Ihr Konto vornehmen können.

Die Ansicht teilt sich in vier Bereiche auf:

- **Persönliche Details**: Informationen zu Anzeigenamen und E-Mail
- **Aktive Sitzungen**: Überblick über alle Sitzungen des Nutzenden

1.3.4.1.1 Benutzernamen ändern

Im Bereich **Persönliche Details** der Ansicht **Persönliches Konto** können Sie den in der Anwendung angezeigten Namen ändern.

Abbildung 41: Bereich Persönliches Konto

Um den Namen zu ändern, gehen Sie wie folgt vor:

- ► Ersetzen Sie im Textfeld **Name** den eingetragenen Namen durch den neuen Namen.
- ► Klicken Sie auf die Schaltfläche **Speichern**.
- ➔ Eine Meldung bestätigt das erfolgreiche Ändern des Namens.

1.3.4.1.2 Aktive Webbrowser-Sitzungen beenden

Im Bereich **Aktive Sitzungen** in der Ansicht **Persönliches Konto** haben Sie die Möglichkeit, sich von allen anderen Webbrowser-Sitzungen als der gerade im aktuellen Browserfenster laufenden abzumelden.

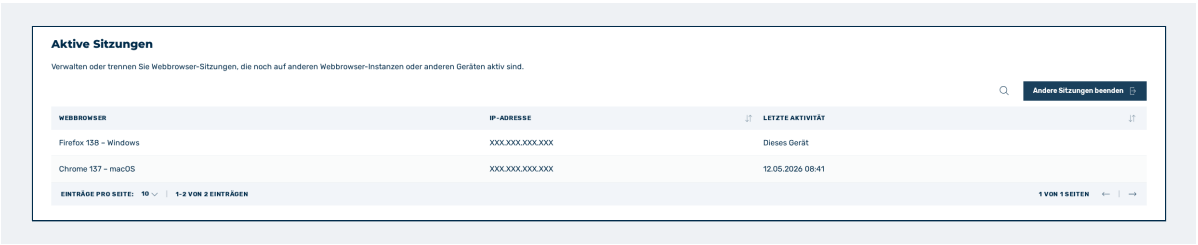


Abbildung 42: Bereich Aktive Sitzungen

Um sich von einem Webbrowser abzumelden, führen Sie den folgenden Schritt aus:

- ► Klicken Sie auf die Schaltfläche **Andere Sitzungen beenden**.
- ➔ Eine Meldung bestätigt das erfolgreiche Beenden von nicht aktiven Sitzungen.

> ⓘ Die laufende Sitzung im aktuellen Webbrowser wird dabei nicht beendet.

1.3.4.2 Reiter Benachrichtigungen

Der Reiter **Benachrichtigungen** erscheint, wenn Sie einem Unternehmen angehören. Über Traffic-Anomalien benachrichtigt Myra nur, wenn für das jeweilige Unternehmen die Anomalie-Funktion aktiviert ist (siehe Unternehmen ändern).

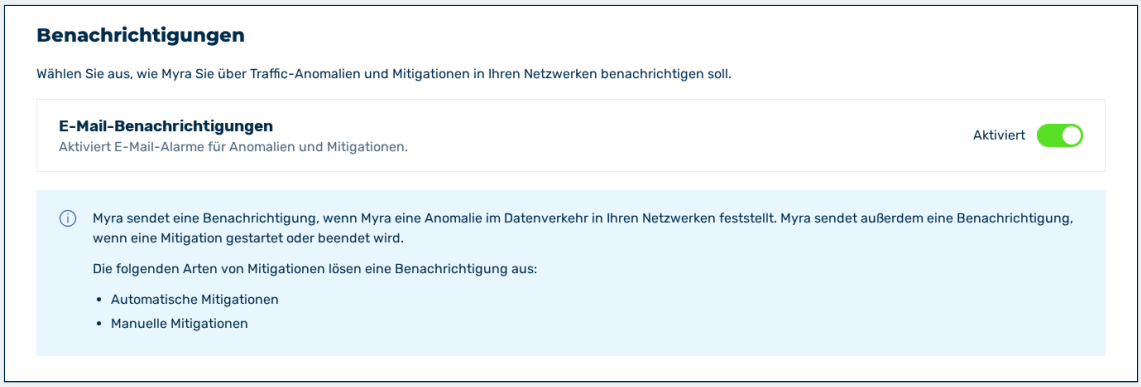


Abbildung 43: Reiter Benachrichtigungen

Im Reiter **Benachrichtigungen** legen Sie fest, wie Myra Sie über Traffic-Anomalien und Mitigationen in Ihren Netzwerken benachrichtigt.

Myra sendet eine Benachrichtigung, wenn Myra eine Anomalie im Datenverkehr in Ihren Netzwerken feststellt. Myra sendet außerdem eine Benachrichtigung, wenn eine Mitigation gestartet oder beendet wird.

Die folgenden Arten von Mitigationen lösen eine Benachrichtigung aus:

- Automatische Mitigationen
- Manuelle Mitigationen
- Mitigationen, die vom Myra Support-Team eingeleitet werden

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
E-Mail-Benachrichtigungen	Der Schalter aktiviert E-Mail-Alarme für Anomalien und Mitigationen. Die folgenden Werte sind verfügbar: **Aktiviert**: Sie erhalten E-Mail-Benachrichtigungen.

Element	Beschreibung
	Deaktiviert: Sie erhalten keine E-Mail-Benachrichtigungen.

Um die E-Mail-Benachrichtigungen zu aktivieren, gehen Sie wie folgt vor:

► Aktivieren Sie den Schalter unter **E-Mail-Benachrichtigungen**.

➔ Die Einstellung wird sofort gespeichert und die Meldung **Benachrichtigungen aktualisiert** erscheint.

Als SOC-Nutzender werden Sie nicht automatisch für die Benachrichtigungen eines Unternehmens registriert. Der Reiter zeigt Ihnen deshalb keinen Schalter, sondern nur einen entsprechenden Hinweis an. Um Benachrichtigungen zu erhalten, tragen Sie Ihre E-Mail-Adresse im jeweiligen Unternehmen als zusätzlichen Kontakt ein (siehe **Reiter Benachrichtigungen**).

1.3.4.3 Reiter API-Token

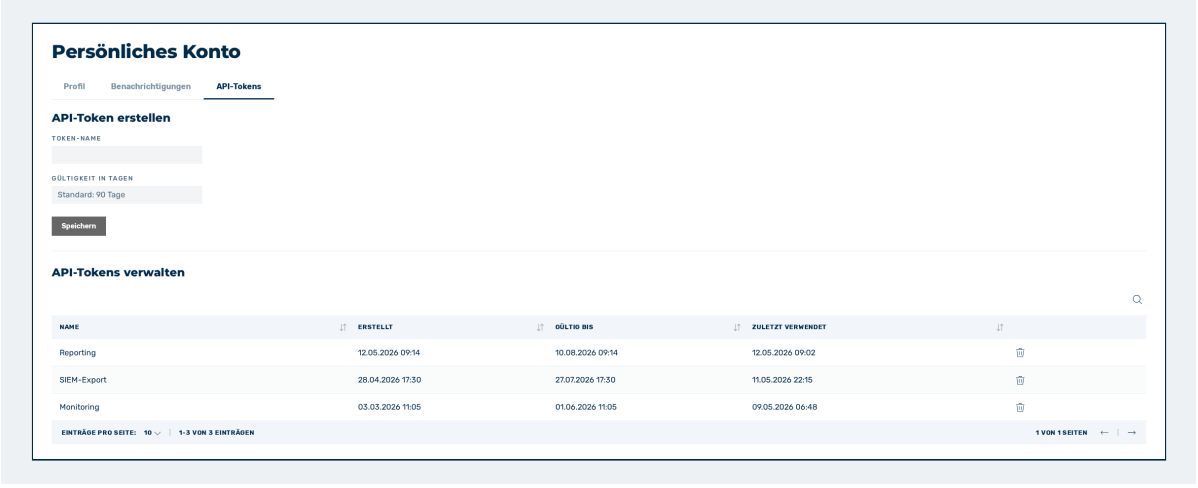


Abbildung 44: Reiter API-Token

Im Reiter **API-Token** können Sie neue API-Tokens erzeugen sowie bereits hinzugefügte API-Tokens einsehen und löschen.

Den API-Token benötigen Sie für die Authentifizierung mittels Bearer-Tokens für die Verwendung der API für den Myra DataHub. Der Token erlaubt es Ihnen ganz einfach und sicher über die Angabe des Tokens als Bearer-Token im Header Ihrer API-Anfrage, die APIv2 von Myra zu verwenden.

Der Reiter teilt sich in die folgenden Bereiche:

1.3.4.3.1 Bereich API-Token erstellen

Im Bereiche **API-Token erstellen** können Sie neue API-Tokens erstellen, sowie deren Gültigkeit festlegen.

Folgende Optionen sind verfügbar:

Element	Beschreibung
Token-Name	Der Name des Tokens.
Gültigkeit in Tagen	Die Anzahl an Tagen für die Gültigkeit des Token.
Speichern	Die Schaltfläche erstellt den Token und öffnet den Dialog **API-Token erstellt** zum Kopieren des Token.

1.3.4.3.2 Bereich API-Tokens verwalten

Eine Übersicht aller Tokens.

Die folgenden Informationen sind verfügbar:

Element	Beschreibung
Name	Der Name des Tokens.
Erstellt	Das Datum und die Uhrzeit, an dem der Token erzeugt wurde.
Gültig bis	Die Anzahl an Tagen für die Gültigkeit des Token. ⓘ Die Angabe eines Ablaufdatums ist optional und muss nicht bei der Erstellung eines API-Tokens gesetzt werden. Um die Sicherheit bei der Verwendung eines API-Tokens zu erhöhen, empfiehlt Myra die Angabe eines Ablaufdatums.
Zuletzt verwendet	Das Datum und die Uhrzeit, an dem zuletzt mit dem Token eine API-Anfrage ausgeführt wurde.

Die folgenden Optionen sind verfügbar:

Element	Beschreibung
	Das Symbol öffnet den Dialog **API-Token löschen** zum Löschen des ausgewählten Eintrages.
Feld Filter	Das Feld filtert die Einträge nach Namen.

1.4 Berechtigungen

1.4.1 Rollen und Berechtigungen

Seiten	Optionen	Unternehmen		SOC	
		User	Admin	User	Admin
Profil	Name ändern	Ja	Ja	Ja	Ja
	Passwort ändern	Ja	Ja	Ja	Ja
	Zwei-Faktor-Authentifizierung anpassen	Ja	Ja	Ja	Ja
	Webbrowser-Sitzung beenden	Ja	Ja	Ja	Ja
Unternehmen	Ansicht **Unternehmensseite anzeigen**	Nein	Nein	Ja	Ja
Unternehmens-management	Unternehmen ändern	Nein	Nein	Nein	Ja
Berichte	Ansicht **Berichte**	Nein	Nein	Ja	Ja
	Berichte herunterladen	Nein	Nein	Ja	Ja
Audit-Log (SOC)	Ansicht **Audit-Log**	Nein	Nein	Ja	Ja
	Audit-Log herunterladen	Nein	Nein	Ja	Ja
SOC-Mode	SOC-Mode	Nein	Nein	Ja	Ja

Seiten	Optionen	Unternehmen		SOC	
		User	Admin	User	Admin
Nutzerverwaltung	Konto hinzufügen (Unternehmen)	Nein	Ja (User & Admin)	Ja (User & Admin)	Ja (User & Admin)
	Konto ändern (Unternehmen)	Nein	Ja (User & Admin)	Ja (User & Admin)	Ja (User & Admin)
	Konto löschen (Unternehmen)	Nein	Ja (User & Admin)	Ja (User & Admin)	Ja (User & Admin)
	Konto hinzufügen (SOC)	Nein	Nein	Ja (User)	Ja (User & Admin)
	Konto ändern (SOC)	Nein	Nein	Ja (User)	Ja (User & Admin)
	Konto löschen (SOC)	Nein	Nein	Ja (User)	Ja (User & Admin)
Dashboard	Ansicht **Dashboard**	Ja	Ja	Ja	Ja
	Diagramme herunterladen	Ja	Ja	Ja	Ja
	Berichte herunterladen	Ja	Ja	Ja	Ja
Netzwerke	Ansicht **Netzwerke**	Ja	Ja	Ja	Ja
	Manuelle Mitigation starten/beenden	Nein	Ja	Ja	Ja
	Netzwerk hinzufügen	Nein	Nein	Nein	Ja

Seiten	Optionen	Unternehmen		SOC	
		User	Admin	User	Admin
	Netzwerk-Details anzeigen	Nein	Nein	Nein	Ja
	Netzwerk ändern	Nein	Nein	Nein	Ja
	Netzwerk löschen	Nein	Nein	Nein	Ja
Mitigationsverlauf	Ansicht **Mitigationsverlauf**	Ja	Ja	Ja	Ja
	Mitigationsbericht anzeigen	Ja	Ja	Ja	Ja
	Mitigationsbericht herunterladen	Ja	Ja	Ja	Ja
Audit-Log (Unternehmen)	Ansicht **Audit-Log**	Nein	Ja	Ja	Ja
	Audit-Log herunterladen	Nein	Ja	Ja	Ja
Handbuch	Handbuch anzeigen	Ja	Ja	Ja	Ja
Sprache	Sprache wechseln	Ja	Ja	Ja	Ja
Changelog	Versionsverlauf des Myra DataHub	Nein	Nein	Ja	Ja

2. API

2.1 Verwendung der Myra API

> Nicht alle API-Endpunkte stehen SOC-Nutzenden zur Verfügung.
>
> Ob ein Endpunkt über den API-Token eines SOC-Nutzenden verwendet werden kann, wird in jedem Endpunkt genau beschrieben.

Die Web-API von Myra basiert auf REST und verwendet HTTP-Anfragen. Wir unterstützen den programmatischen Zugriff auf fast alle Vorgänge, die Sie über unsere Weboberfläche ausführen können. Sie können beispielsweise neue Domains anlegen und konfigurieren, Ihre Cache-Einstellungen entsprechend Ihrem Bereitstellungszyklus verwalten oder Ihre DNS-Einstellungen ändern.

Die API von Myra für den Myra DataHub ist erreichbar unter: **https://networksecurity.myracloud.com/api/documentation**

Im Folgenden erklären wir Ihnen die wichtigsten Schritte, um sich bei der APIv2 anzumelden und die ersten Anfragen starten zu können.

2.2 Allgemein

2.2.1 Zugriff zur Myra API erhalten

Sie können sich über die folgenden Wege an der Myra API authentifizieren.

- Authentifizierung mittels eines Bearer-Tokens durch Verwendung eines API-Tokens

> Wenn Sie Anfragen über die API an den Myra DataHub stellen, dann hat der verwendete API-Token die gleichen Berechtigungen wie Ihr Konto.

2.2.2 Authentifizierung mittels Bearer-Token

Um sich mittels eines Bearer-Tokens an der API zu authentifizieren, sind die folgenden Schritte auszuführen:

- API-Token erstellen
- Bearer-Token im Header eintragen

2.2.2.1 API-Token erstellen

Um einen API-Token zu erstellen, gehen Sie wie folgt vor:

- Öffnen Sie die Myra DataHub.
- Melden Sie sich an.
- Öffnen Sie Ihr persönliches Konto, siehe **Persönliches Konto**.
  - ↳ Die Ansicht **Persönliches Konto** öffnet sich.
- Klicken Sie auf den Reiter **API-Token**.

Abbildung 45: Namen und Gültigkeit für den API-Token eingeben

- Navigieren Sie zum Bereich **API-Token erstellen**.
- Geben Sie im Textfeld unter **TOKEN-NAME** einen Namen ein.

> ⓘ Der Name eines API-Tokens soll Ihnen dabei helfen die verschiedenen Einsatzzwecke Ihrer API-Token besser identifizieren zu können.

- Falls erforderlich, definieren Sie im Textfeld unter **GÜLTIGKEIT IN TAGEN** eine Gültigkeit für den API-Token.

> ⓘ Standardmäßig hat ein API-Token eine Gültigkeit von 90 Tagen.

- Klicken Sie auf die Schaltfläche **Speichern**.

↳ Der Dialog **API-Token erstellt** öffnet sich.

Abbildung 46: Namen und Gültigkeit für den API-Token eingeben

► Um die Daten des API-Tokens zu kopieren, klicken Sie auf das Symbol neben jeden Eintrag.

> Der API-Token ist nur beim Erzeugen eines neuen API-Tokens einsehbar und muss an einem sicheren Ort gespeichert werden.
>
> Sobald Sie die Schaltfläche Schließen im Dialog API-Token erstellt klicken, können Sie nur noch den Namen, das Erstelldatum und das Gültigkeitsdatum einsehen.
>
> Sollten Sie den Token verloren haben, müssen Sie einen neuen API-Token erzeugen.

► Um den Dialog zu schließen, klicken Sie auf die Schaltfläche Schließen.

➔ Der neue API-Token erscheint in der Liste aller API-Token und kann sofort genutzt werden.

2.2.2.2 Anfrage mittels Bearer-Token an die API stellen

Um eine Anfrage mittels Bearer-Token an die API zu senden, gehen Sie wie folgt vor:

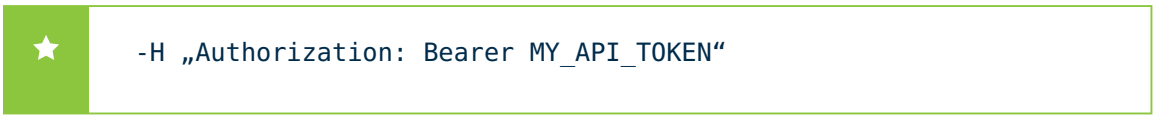
► Öffnen Sie das Programm über das Sie die Anfrage senden wollen.

► Fügen Sie die Methode für die Anfrage hinzu.

► Fügen Sie die Adresse der API zusammen mit der URI hinzu.

> `https://networksecurity.myracloud.com/domains/1234`

- Fügen Sie das Token als Bearer-Token als Authentifizierungsmethode zum Header hinzu.



- Fügen Sie für PUT- und POST-Anfragen einen Body in JSON-Format mit den erforderlichen Informationen zur Anfrage hinzu.

➔ Die Anfrage sieht wie folgt aus:

```
curl -X GET "https://networksecurity.myracloud.com/domains/1234"
-H "Authorization: Bearer MY_API_TOKEN"
```

2.2.3 Verwendete API-Methoden

Die Myra API für den Myra DataHub verwendet die folgenden Methoden:

Element	Beschreibung
GET	Mit der GET-Methode können Sie ein bestimmtes Objekt oder eine Liste von Objekten mit Einstellungen und Einträgen im Myra DataHub anfordern.
POST	Mit der POST-Methode können Sie neue Einstellungen oder Einträge für bestimmte Funktionen im Myra DataHub hinzufügen.
PUT	Mit der PUT-Methode können Sie bestimmte Informationen bestehender Einstellungen oder Einträge im Myra DataHub ändern. Nur die Attribute `id`, `modified` und die Attribute zum Ändern einer bestimmten Option müssen im Body definiert werden. ⓘ Die Einstellungen für Subdomains bilden eine Ausnahme, da ein Ändern der Einstellung die komplette Übergabe aller Attribute des entsprechenden Objektes erforderlich macht. Attribute, die nicht definiert werden, werden auf den Standardwert zurückgesetzt.
DELETE	Mit der DELETE-Methode können Sie ganze Einträge einer Option im Myra DataHub löschen.

2.2.4 Mögliche Antworten auf eine Anfrage

Alle API-Anfragen geben einen Statuscode und ein Objekt zurück, das Ihnen Aufschluss über den Erfolg oder mögliche Fehler, wie fehlende Informationen oder Berechtigungen, gibt.

2.2.4.1 Mögliche Statuscodes

Statuscode	Erklärung	Objekt
200 OK	Die Anfrage war erfolgreich.	QueryVO
201 Created	Die Anfrage war erfolgreich und es wurde ein neues Objekt erstellt.	ResultVO
202 Accepted	Die Anfrage war erfolgreich, wurde jedoch noch nicht abgeschlossen. Dies kann der Fall sein, wenn die Anfrage einen Prozess anstößt, wie das Ändern einer Konfiguration, die bis zu 7 Minuten braucht, bis sie umgesetzt wurde.	ResultVO
400 Bad Request	Die Anfrage war nicht erfolgreich. Die Anfrage war fehlerhaft oder es fehlen Informationen.	ViolationVO
401 Unauthorized	Die Anfrage war nicht erfolgreich, da die Authentifizierung der Anfrage fehlerhaft war.	ViolationVO
403 Forbidden	Die Anfrage war nicht erfolgreich, da das verwendete Konto nicht über die erforderlichen Berechtigungen verfügt.	ViolationVO

2.2.4.2 Verwendete Objekte

Element	Beschreibung
QueryVO	Ein Objekt `QueryVO` wird zurückgegeben, wenn eine Liste von Objekten aus einer GET-Anfrage empfangen wird.
ResultVO	Bei erfolgreichen POST-, PUT- und DELETE-Anfragen wird ein Objekt `ResultVO` zurückgegeben.
ViolationVO	Bei fehlerhaften Anfragen wird ein Objekt `ViolationVO` zurückgegeben.

2.3 API-Endpunkte

In den folgenden Abschnitten listen wir Ihnen alle Endpunkte für unsere API auf, über die Sie den Myra DataHub konfigurieren können.

Alternativ finden Sie alle Endpunkte auch in unserer Swagger-Dokumentation unter:

- **https://networksecurity.myracloud.com/api/documentation**

2.3.1 Organisationsverwaltung

2.3.1.1 Organisation löschen

Gelöschte Organisationen können nicht wiederhergestellt werden. Nach dem Löschen ist für die weitere Nutzung der Organisation eine Neuanlage erforderlich.

Diese Anfrage steht ausschließlich SOC-Nutzenden zur Verfügung.

Eine Organisation kann nicht gelöscht werden, solange für eines ihrer Netzwerke eine aktive Mitigation läuft.

Senden einer `DELETE` -Anfrage an den Endpunkt `/organisations/{organisation}` .

2.3.1.1.1 Beschreibung

Die Delete-Organisation-Anfrage löscht eine Organisation aus dem System.

2.3.1.1.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.1.3 Anfrage

Um eine Organisation zu löschen, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein.

Weitere Informationen sind nicht erforderlich.

Das System gibt als Antwort auf eine erfolgreiche Anfrage ausschließlich den HTTP-Statuscode 200 zurück.

2.3.1.1.4 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
400	Die Anfrage war nicht erfolgreich. Die Anfrage war fehlerhaft oder es fehlen Informationen.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.1.2 SIEM-Konfiguration einer Organisation löschen

Gelöschte Einträge lassen sich nicht wiederherstellen. Um einen Eintrag nach dem Löschen erneut zu nutzen, legen Sie ihn neu an.

Senden einer `DELETE` -Anfrage an den Endpunkt `/organisations/{organisation}/siem` .

2.3.1.2.1 Beschreibung

Die Delete-Organisation-SIEM-Anfrage löscht die SIEM-Konfiguration der Organisation.

2.3.1.2.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.2.3 Anfrage

Um die SIEM-Konfiguration zu löschen, fügen Sie die **Organisation-ID** `{organisation}` dem Pfad der Anfrage hinzu.

Weitere Informationen sind nicht erforderlich.

Das System gibt bei einer erfolgreichen Anfrage lediglich den HTTP-Statuscode 200 zurück.

2.3.1.2.4 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.1.3 Organisationen mit Netzwerk- und Mitigationsdetails auflisten

> ⓘ Die Objekte `OrganisationVO` sind in `data` verpackt, ergänzt durch die Paginierungsblöcke `links` und `meta`.

Senden einer `GET`-Anfrage an den Endpunkt `/organisations`.

2.3.1.3.1 Beschreibung

Mit der List-Organisations-Paginated-Anfrage fordern Sie eine paginierte Liste aller Organisationen an, angereichert mit Netzwerk-CIDRs und dem aktuellen Mitigationsstatus.

2.3.1.3.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.1.3.3 Anfrage

Um eine paginierte Liste aller Organisationen anzufordern, ist im Pfad der Anfrage keine zusätzliche Information erforderlich.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `OrganisationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Organisation.	`string`
`name`	Der Name der Organisation.	`string`
`created_at`	Der ursprüngliche Erstellungszeitstempel im ISO-8601-Format.	`string($date-time)`
`updated_at`	Der letzte Aktualisierungszeitstempel im ISO-8601-Format.	`string($date-time)`
`users`	Die der Organisation zugewiesenen Nutzenden.	`array`
`showReports`	Definiert, ob Mitigationsberichte aktiviert sind.	`true` `false`
`siemEnabled`	Definiert, ob die SIEM-Integration aktiviert ist.	`true` `false`
`cidrs`	Die kommagetrennte Liste der CIDRs.	`string`
`under_mitigation`	Zeigt an, ob sich aktuell ein Netzwerk in Mitigation befindet.	`true` `false`

2.3.1.3.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "name": "Test Organisation",
      "created_at": "2026-01-01T00:00:00+00:00",
      "updated_at": "2026-01-01T00:00:00+00:00",
      "users": [
        {
          "id": "xY9pQ5wR1",
          "name": "Max Mustermann",
          "email": "max@mustermann.de",
          "has2Fa": false,
```

```
          "permissions": {},
          "activeOrganisation": {
            "id": "xY9pQ5wR1",
            "name": "Test Organisation"
          },
          "hasActiveMitigations": false,
          "hasSiem": false,
          "invitedSince": "2024-01-15 10:30:00",
          "status": "active",
          "role": "admin",
          "teams": [
            {
              "id": "xY9pQ5wR1",
              "name": "Test Organisation"
            }
          ],
          "teams_as_admin": [
            {
              "id": "xY9pQ5wR1",
              "name": "Test Organisation"
            }
          ],
          "features": [
            {
              "name": "L_NUMBER",
              "value": null,
              "enabled": 1
            }
          ]
        }
      ],
      "showReports": true,
      "siemEnabled": false,
      "cidrs": "127.0.0.1/32, 10.0.0.0/24",
      "under_mitigation": false
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
```

```
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```


2.3.1.3.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.1.4 Alle Organisationen des Nutzenden auflisten

Senden einer `GET` -Anfrage an den Endpunkt `/organisations/all` .

2.3.1.4.1 Beschreibung

Mit der List-Organisations-Anfrage fordern Sie eine Liste aller Organisationen an, auf die Sie Zugriff haben.

2.3.1.4.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.1.4.3 Anfrage

Um eine Liste aller Organisationen anzufordern, fügen Sie dem Pfad der Anfrage keine zusätzlichen Informationen hinzu.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `OrganisationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Organisation.	`string`
`name`	Der Name der Organisation.	`string`
`created_at`	Das Erstellungsdatum im ISO-8601-Format.	`string($date-time)`
`updated_at`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`

Die Antwort ist nicht paginiert.

2.3.1.4.4 Beispiel

Beispiel-Antwort:


```
[
  {
    "id": "xY9pQ5wR1",
    "name": "Test Organisation",
    "created_at": "2026-01-01T00:00:00+00:00",
    "updated_at": "2026-01-01T00:00:00+00:00",
    "users": [
      {
        "id": "xY9pQ5wR1",
        "name": "Max Mustermann",
        "email": "max@mustermann.de",
        "has2Fa": false,
        "permissions": {},
        "activeOrganisation": {
          "id": "xY9pQ5wR1",
          "name": "Test Organisation"
        },
        "hasActiveMitigations": false,
        "hasSiem": false,
        "invitedSince": "2024-01-15 10:30:00",
        "status": "active",
        "role": "admin",
        "teams": [
          {
            "id": "xY9pQ5wR1",
            "name": "Test Organisation"
          }
        ],
        "teams_as_admin": [
```

```
            {
              "id": "xY9pQ5wR1",
              "name": "Test Organisation"
            }
          ],
          "features": [
            {
              "name": "L_NUMBER",
              "value": null,
              "enabled": 1
            }
          ]
        }
      ],
      "showReports": true,
      "siemEnabled": false,
      "customer_id": "abc",
      "cidrs": "127.0.0.1/32, 10.0.0.0/24",
      "under_mitigation": false,
      "customer_reference": "abc"
    }
  ]
```


2.3.1.4.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.

2.3.1.5 Organisation anhand der ID abrufen

Senden einer `GET` -Anfrage an den Endpunkt `/organisations/{organisation}` .

2.3.1.5.1 Beschreibung

Mit der Get-Organisation-Anfrage fordern Sie eine einzelne Organisation für eine angegebene ID an.

2.3.1.5.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.5.3 Anfrage

Um eine Organisation anzufordern, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein.

Als Ergebnis erhalten Sie ein Objekt `OrganisationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Organisation.	`string`
`name`	Der Name der Organisation.	`string`
`created_at`	Der ursprüngliche Erstellungszeitpunkt im ISO-8601-Format.	`string($date-time)`
`updated_at`	Der Zeitpunkt der letzten Aktualisierung im ISO-8601-Format.	`string($date-time)`
`users`	Die zur Organisation gehörenden Nutzenden.	`array`
`showReports`	Definiert, ob Mitigationsberichte aktiviert sind.	`true` `false`
`siemEnabled`	Definiert, ob die SIEM-Integration aktiviert ist.	`true` `false`

2.3.1.5.4 Beispiel

Beispiel-Antwort:


```
{
  "id": "xY9pQ5wR1",
  "name": "Test Organisation",
  "created_at": "2026-01-01T00:00:00+00:00",
  "updated_at": "2026-01-01T00:00:00+00:00",
  "users": [
    {
      "id": "xY9pQ5wR1",
      "name": "Max Mustermann",
      "email": "max@mustermann.de",
      "has2Fa": false,
```

```
      "permissions": {},
      "activeOrganisation": {
        "id": "xY9pQ5wR1",
        "name": "Test Organisation"
      },
      "hasActiveMitigations": false,
      "hasSiem": false,
      "invitedSince": "2024-01-15 10:30:00",
      "status": "active",
      "role": "admin",
      "teams": [
        {
          "id": "xY9pQ5wR1",
          "name": "Test Organisation"
        }
      ],
      "teams_as_admin": [
        {
          "id": "xY9pQ5wR1",
          "name": "Test Organisation"
        }
      ],
      "features": [
        {
          "name": "L_NUMBER",
          "value": null,
          "enabled": 1
        }
      ]
    }
  ],
  "showReports": true,
  "siemEnabled": false,
  "cidrs": "127.0.0.1/32, 10.0.0.0/24",
  "under_mitigation": false
}
```


2.3.1.5.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	

STATUSCODE	BESCHREIBUNG
	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.1.6 Alle Mitigationen einer Organisation auflisten

> Die Schwellenwert- und Traffic-Kennzahlen — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` sowie (falls die Funktion für den Bericht verworfener Daten aktiviert ist) `dropped_bits` und `dropped_packets` — werden nur für automatische (durch Erkennung ausgelöste) Mitigationen zurückgegeben. Bei manuellen Mitigationen, die keine Erkennungsdaten enthalten, entfallen sie.

Senden einer `GET`-Anfrage an den Endpunkt `/organisations/{organisation}/mitigations`.

2.3.1.6.1 Beschreibung

Mit der List-Organisation-Mitigations-Anfrage fordern Sie eine Liste aller Mitigationen für eine angegebene Organisation an.

2.3.1.6.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.6.3 Anfrage

Um eine Liste aller Mitigationen anzufordern, fügen Sie die **Organisation-ID** `{organisation}` dem Pfad der Anfrage hinzu.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `MitigationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Mitigation.	`string`
`organisation`	Die zugehörige Organisation, angegeben als Objekt.	`object`
`network`	Das mitigierte Netzwerk oder bei einer Teil-Mitigation die spezifische IP-Adresse.	`string`
`mitigation_type`	Der Typ der angewendeten Mitigation.	`ACTION_BLACKHOLE` `ACTION_MITIGATE_ONPREM` `ACTION_MITIGATE_CLOUD`
`mitigation_cause`	Wie die Mitigation ausgelöst wurde.	`MANUAL_TRIGGER` `AUTO_TRIGGER` `OPS_TRIGGER` `UNKNOWN_TRIGGER`
`start`	Das Startdatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`end`	Das Enddatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`created_at`	Das Erstellungsdatum im ISO-8601-Format.	`string($date-time)`
`updated_at`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`
`actual_bw`	Die tatsächliche Bandbreite der Mitigation.	`number($float)`

Attribut	Beschreibung	Werte
`actual_pps`	Die tatsächlichen Pakete pro Sekunde der Mitigation.	`number($float)`
`configured_bw`	Die konfigurierte Bandbreite der Mitigation.	`number($float)`
`configured_pps`	Die konfigurierten Pakete pro Sekunde der Mitigation.	`number($float)`
`configured_bw_percentage`	Die konfigurierte Bandbreite als Prozentsatz.	`number`
`configured_pps_percentage`	Die konfigurierten Pakete pro Sekunde als Prozentsatz.	`number`
`peak_bw`	Die Spitzenbandbreite der Mitigation.	`number($float)`
`peak_pps`	Die Spitzen-Pakete pro Sekunde der Mitigation.	`number($float)`
`total_bw`	Die Gesamtbandbreite der Mitigation.	`number($float)`
`total_pps`	Die gesamten Pakete pro Sekunde der Mitigation.	`number($float)`
`has_report`	Zeigt an, ob ein Bericht für die Mitigation verfügbar ist.	`true` `false`
`start_user`	Die Nutzenden, die die Mitigation gestartet haben, angegeben als Objekt mit ID und Anzeigename.	`object`
`end_user`	Die Nutzenden, die die Mitigation beendet haben, angegeben als Objekt mit ID und Anzeigename. Der Wert ist null, solange die Mitigation noch läuft.	`object`

2.3.1.6.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "network": "192.0.2.0/24",
      "mitigation_type": "ACTION_MITIGATE_ONPREM",
      "mitigation_cause": "MANUAL_TRIGGER",
      "start": "2026-01-01T00:00:00+00:00",
      "end": "2026-01-01T00:00:00+00:00",
      "created_at": "2026-01-01T00:00:00+00:00",
      "updated_at": "2026-01-01T00:00:00+00:00",
      "actual_bw": 0,
      "actual_pps": 0,
      "configured_bw": 0,
      "configured_pps": 0,
      "configured_bw_percentage": 0,
      "configured_pps_percentage": 0,
      "peak_bw": 0,
      "peak_pps": 0,
      "total_bw": 0,
      "total_pps": 0,
      "has_report": true,
      "start_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      },
      "end_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      }
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
```

```
          "active": false
        }
      ],
      "path": "https://datahub-api.com/api/networks",
      "per_page": 15,
      "to": 15,
      "total": 64
    }
  }
```


2.3.1.6.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.1.7 Alle Netzwerke einer Organisation auflisten

Die Attribute `pps_limit_percentage` und `bw_limit_percentage` sind nur vorhanden, wenn für die Organisation prozentuale Schwellenwerte aktiviert sind.

Senden einer `GET` -Anfrage an den Endpunkt `/organisations/{organisation}/networks` .

2.3.1.7.1 Beschreibung

Mit der List-Organisation-Networks-Anfrage fordern Sie eine paginierte Liste aller Netzwerke einer angegebenen Organisation an.

2.3.1.7.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.7.3 Anfrage

Um eine Liste aller Netzwerke einer Organisation anzufordern, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `NetworkVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Netzwerks.	`string`
`organisation`	Die zugehörige Organisation, referenziert über ID und Name.	`object`
`name`	Der Name des Netzwerks.	`string`
`cidr`	Der CIDR-Bereich des Netzwerks.	`string`
`enabled`	Zeigt an, ob die automatische Mitigation aktiviert ist.	`true` `false`
`data_only`	Zeigt an, ob das Netzwerk nur überwacht wird, das heißt, es ist im Dashboard sichtbar, kann aber nicht mitigiert werden.	`true` `false`

`mitigation_type`	Der Mitigationstyp des Netzwerks.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`auto_mitigation_strategy`	Die Strategie der automatischen Mitigation des Netzwerks.	`string`
`duration`	Die Dauer der automatischen Mitigation.	`integer`
	Der Mitigations-Override für das Subnetz.	`true` `false`

Attribut	Beschreibung	Werte
`subnet_mitigation_override`		
`pps_limit`	Der konfigurierte Grenzwert für Pakete pro Sekunde.	`integer`
`bw_limit`	Der konfigurierte Bandbreiten-Grenzwert.	`integer`
`autoStatus`	Zeigt an, ob das Netzwerk aktuell unter automatischer Mitigation steht.	`true` `false`
`manualStatus`	Zeigt an, ob das Netzwerk aktuell unter manueller Mitigation steht.	`true` `false`
`active_partial_manual_mitigations`	Die aktiven partiellen manuellen Mitigationen.	`array`
`active_partial_auto_mitigations`	Die aktiven partiellen automatischen Mitigationen.	`array`
`allow_manual_mitigation`	Zeigt, ob für das Netzwerk manuelle Mitigationen gestartet werden dürfen.	`true` `false`
`extra`	Zusätzliche benutzerdefinierte Felder, die für die Organisation definiert sind.	`object`

2.3.1.7.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "name": "Customer-A-Prod",
      "cidr": "192.0.2.0/24",
      "enabled": true,
      "data_only": false,
      "mitigation_type": "ACTION_BLACKHOLE",
```

```
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "subnet_mitigation_override": false,
      "pps_limit": 0,
      "bw_limit": 0,
      "autoStatus": true,
      "manualStatus": true,
      "active_partial_manual_mitigations": [
        {}
      ],
      "active_partial_auto_mitigations": [
        {}
      ],
      "allow_manual_mitigation": true,
      "extra": {}
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```


2.3.1.7.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	

STATUSCODE	BESCHREIBUNG
	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.1.8 Alle Nutzenden einer Organisation auflisten

Senden einer `GET` -Anfrage an den Endpunkt `/organisations/{organisation}/users` .

2.3.1.8.1 Beschreibung

Mit der List-Organisation-Users-Anfrage fordern Sie eine Liste aller Nutzenden einer angegebenen Organisation an, mit Ausnahme von Agent-Konten.

2.3.1.8.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.8.3 Anfrage

Um eine Liste aller Nutzenden einer Organisation anzufordern, fügen Sie die **Organisation-ID** `{organisation}` dem Pfad der Anfrage hinzu.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `UserVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Nutzenden.	`string`
`name`	Der vollständige Name der Nutzenden.	`string`
`email`	Die E-Mail-Adresse der Nutzenden.	`string`

Attribut	Beschreibung	Werte
`role`	Die Rolle der Nutzenden innerhalb der Organisation.	`admin` `editor`
`status`	Der aktuelle Status des Benutzerkontos.	`string`
`invitedSince`	Das Datum, an dem die Nutzenden eingeladen wurden, oder leer, falls die Einladung bereits angenommen wurde.	`string($date-time)`
`has2Fa`	Definiert, ob die Zwei-Faktor-Authentifizierung für die Nutzenden aktiviert ist.	`true` `false`

2.3.1.8.4 Beispiel

Beispiel-Antwort:


```
[
  {
    "id": "xY9pQ5wR1",
    "name": "Max Mustermann",
    "email": "max@mustermann.de",
    "has2Fa": false,
    "permissions": {},
    "activeOrganisation": {
      "id": "xY9pQ5wR1",
      "name": "Test Organisation"
    },
    "hasActiveMitigations": false,
    "hasSiem": false,
    "invitedSince": "2024-01-15 10:30:00",
    "status": "active",
    "role": "admin",
    "teams": [
      {
        "id": "xY9pQ5wR1",
        "name": "Test Organisation"
      }
    ],
    "teams_as_admin": [
      {
        "id": "xY9pQ5wR1",
        "name": "Test Organisation"
      }
    ],
    "features": [
      {
        "name": "L_NUMBER",
```

```
        "value": null,
        "enabled": 1
      }
    ]
  }
]
```

2.3.1.8.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.1.9 Einstellungen einer Organisation ändern

Senden einer `PATCH` -Anfrage an den Endpunkt `/organisations/{organisation}` .

2.3.1.9.1 Beschreibung

Nur SOC. Mit der Change-Organisation-Anfrage ändern Sie die Einstellungen einer Organisation.

2.3.1.9.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.9.3 Anfrage

Um die Einstellungen einer Organisation zu ändern, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein.

Für eine detaillierte Spezifikation, welche Informationen zum Ändern der Einstellungen einer Organisation erforderlich sind, können die folgenden Attribute im Body definiert werden.

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`name`	Der Name der Organisation.	`string`
`showReports`	Definiert, ob Berichte für diese Organisation angezeigt werden.	`true` `false`
`siemEnabled`	Definiert, ob SIEM für diese Organisation aktiviert ist.	`true` `false`
`siemProvider`	Der Name des SIEM-Anbieters.	`string`
`trafficReportsEnabled`	Zeigt an, ob Traffic-Reports für diese Organisation angezeigt und heruntergeladen werden können.	`true` `false`

Das System gibt bei einer erfolgreichen Anfrage lediglich einen HTTP-Statuscode 200 zurück.

2.3.1.9.4 Beispiel

Beispiel-Request-Body:

```
{
  "name": "string",
  "showReports": true,
  "siemEnabled": true,
  "siemProvider": "string",
  "trafficReportsEnabled": true
}
```

2.3.1.9.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.1.10 SIEM-Konfiguration einer Organisation ändern

Der Body muss die Attribute `id` und `modified` enthalten, um den entsprechenden Eintrag zu identifizieren.

Die ID des Eintrags im Pfad der Anfrage muss mit dem Wert des Attributs `id` im Body übereinstimmen.

Senden einer `PATCH` -Anfrage an den Endpunkt `/organisations/{organisation}/siem` .

2.3.1.10.1 Beschreibung

Mit der Change-Organisation-SIEM-Anfrage ändern Sie die SIEM-Verbindungsdetails einer Organisation.

2.3.1.10.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: `OrganisationVO`

2.3.1.10.3 Anfrage

Um die SIEM-Verbindungsdetails zu ändern, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein.

Für eine detaillierte Spezifikation, welche Informationen zum Ändern der SIEM-Verbindungsdetails erforderlich sind, muss im Body ein Objekt `OrganisationVO` mit den folgenden Attributen definiert werden:

Attribut	Beschreibung	Werte
`id`	Die ID des Eintrags.	`integer`
`modified`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`siemProvider`	Der Name des SIEM-Anbieters (z. B. splunk).	`string`
`siemConnectionDetails`	Die Verbindungsdetails für den SIEM-Anbieter.	`object`

Das System gibt als Antwort das Objekt `OrganisationVO` mit den aktualisierten Informationen zurück.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Organisation.	`string`
`name`	Der Name der Organisation.	`string`
`created_at`	Der ursprüngliche Erstellungszeitpunkt.	`string($date-time)`
`updated_at`	Der Zeitpunkt der letzten Aktualisierung.	`string($date-time)`
`users`	Die der Organisation zugewiesenen Nutzenden.	`array`
`showReports`		`true`

Attribut	Beschreibung	Werte
	Definiert, ob Mitigationsberichte aktiviert sind.	`false`
`siemEnabled`	Definiert, ob die SIEM-Integration aktiviert ist.	`true` `false`

2.3.1.10.4 Beispiel

Beispiel-Request-Body:

```
{
  "siemProvider": "string",
  "siemConnectionDetails": {
    "host": "string",
    "port": 0,
    "apiToken": "string"
  }
}
```

2.3.1.10.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.1.11 Nutzende innerhalb einer Organisation ändern

> Der Body muss die Attribute `id` und `modified` enthalten, um den entsprechenden Eintrag zu identifizieren.

> Die ID des Eintrags im Pfad der Anfrage muss mit dem Wert des Attributs `id` im Body übereinstimmen.

Senden einer `PATCH` -Anfrage an den Endpunkt `/organisations/{organisation}/users/{user}` .

2.3.1.11.1 Beschreibung

Mit der Update-Organisation-User-Anfrage ändern Sie den Namen und die Rolle von Nutzenden innerhalb einer bestimmten Organisation.

2.3.1.11.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}` ; **Benutzer-ID** `{user}`

Objekte: keine

2.3.1.11.3 Anfrage

Um Nutzende innerhalb einer Organisation zu ändern, fügen Sie die **Organisation-ID** `{organisation}` und die **Benutzer-ID** `{user}` in den Pfad der Anfrage ein.

Für eine detaillierte Spezifikation, welche Informationen zum Ändern von Nutzenden erforderlich sind, müssen die folgenden Attribute im Body definiert werden:

Attribut	Beschreibung	Werte
`id`	Die ID des Nutzenden.	`string`
`modified`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`name`	Der neue Name des Nutzenden.	`string`
`role`	Die neue Rolle des Nutzenden.	`admin` `editor`

Als Ergebnis erhalten Sie ein Objekt mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Nutzenden.	`string`
`name`	Der Name des Nutzenden.	`string`
`email`	Die E-Mail-Adresse des Nutzenden.	`string`
`status`	Der aktuelle Status des Nutzenden.	`string`
`invitedSince`	Das Datum, an dem der Nutzende eingeladen wurde, oder leer, wenn die Einladung bereits angenommen wurde.	`string`
`role`	Die Rolle des Nutzenden innerhalb der Organisation.	`admin` `editor`

2.3.1.11.4 Beispiel

Beispiel-Request-Body:

```
{
  "name": "string",
  "role": "string"
}
```

2.3.1.11.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.1.12 Organisation hinzufügen

Der Body enthält nicht die Attribute `id`, `created` und `modified`. Das System legt diese Werte nach dem Erstellen des Eintrags fest.

Diese Anfrage steht ausschließlich SOC-Nutzenden zur Verfügung.

Senden einer `POST`-Anfrage an den Endpunkt `/organisations`.

2.3.1.12.1 Beschreibung

Mit der Add-Organisation-Anfrage fügen Sie dem System eine neue Organisation hinzu.

2.3.1.12.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: `OrganisationVO`

2.3.1.12.3 Anfrage

Um eine Organisation hinzuzufügen, ist im Pfad der Anfrage keine zusätzliche Information erforderlich.

Für eine detaillierte Spezifikation, welche Informationen zum Hinzufügen einer Organisation erforderlich sind, muss im Body ein Objekt `OrganisationVO` mit den folgenden Attributen definiert werden:

Attribut	Beschreibung	Werte
`name`	Der Name der Organisation. Maximale Länge: 255 Zeichen.	`string`

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`showReports`	Definiert, ob Mitigationsberichte aktiviert sind.	`true` `false`
`siemEnabled`	Definiert, ob die SIEM-Integration aktiviert ist.	`true` `false`

Das System gibt als Antwort das Objekt `OrganisationVO` mit den Informationen zum neuen Eintrag zurück.

2.3.1.12.4 Beispiel

Beispiel-Request-Body:

```
{
  "name": "string",
  "showReports": true,
  "siemEnabled": true
}
```

2.3.1.12.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.

STATUSCODE	BESCHREIBUNG
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.1.13 Bestätigungs-E-Mail für eine Benachrichtigungsadresse erneut senden

> Die Adresse muss bereits für die Organisation registriert und darf noch nicht verifiziert sein; andernfalls gibt die Anfrage einen 404- oder 409-Fehler zurück.

> Für diese Anfrage benötigen Sie Administrationsrechte für die Organisation oder SOC-Rechte.

> Pro Stunde sind höchstens fünf Anfragen an diesen Endpunkt möglich.

Senden einer `POST` -Anfrage an den Endpunkt `/organisations/{organisation}/notification-emails/resend` .

2.3.1.13.1 Beschreibung

Mit der Resend-Verification-Anfrage senden Sie die Bestätigungs-E-Mail für eine nicht verifizierte Benachrichtigungsadresse einer Organisation erneut.

2.3.1.13.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.13.3 Anfrage

Um die Bestätigungs-E-Mail erneut zu senden, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein und definieren die Zieladresse im Body:

Attribut	Beschreibung	Werte
`email`	Die Benachrichtigungsadresse, an die die Bestätigungs-E-Mail erneut gesendet wird.	`string`

Das System gibt als Antwort auf eine erfolgreiche Anfrage nur den HTTP-Statuscode 200 zurück.

2.3.1.13.4 Beispiel

Beispiel-Request-Body:

```
{
  "email": "alerts@example.com"
}
```

2.3.1.13.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
404	Die Anfrage war nicht erfolgreich, da die angeforderte Ressource nicht gefunden wurde.
409	Die Anfrage war nicht erfolgreich, da ein Konflikt mit dem aktuellen Zustand vorliegt.

STATUSCODE	BESCHREIBUNG
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.1.14 Nutzende zur Organisation hinzufügen

Die Attribute `userId` und `userFullName` sind für Myra-Deployments erforderlich.

Senden einer `POST` -Anfrage an den Endpunkt `/organisations/{organisation}/users/add` .

2.3.1.14.1 Beschreibung

Mit der Add-Organisation-User-Anfrage fügen Sie einer angegebenen Organisation Nutzende hinzu.

2.3.1.14.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: `UserVO`

2.3.1.14.3 Anfrage

Um der Organisation Nutzende hinzuzufügen, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein.

Für eine detaillierte Spezifikation, welche Informationen zum Hinzufügen von Nutzenden erforderlich sind, muss im Body ein Objekt `UserVO` mit den folgenden Attributen definiert werden:

Attribut	Beschreibung	Werte
`userEmail`	Die E-Mail-Adresse der Nutzenden.	`string`
`userRole`	Die Rolle der Nutzenden.	`admin` `editor`

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`userId` (erforderlich bei Myra-Deployments)	Die MyraCloud-ID der Nutzenden.	`integer`
`userFullName` (erforderlich bei Myra-Deployments)	Der vollständige Name der Nutzenden.	`string`

Als Ergebnis gibt das System das Objekt `message` zurück, das bestätigt, dass die Nutzenden hinzugefügt wurden.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`message`	Die Bestätigungsmeldung der Anfrage.	`string`

2.3.1.14.4 Beispiel

Beispiel-Request-Body:

```
{
  "userEmail": "string",
  "userRole": "string",
  "userId": 0,
  "userFullName": "string"
}
```

2.3.1.14.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	

STATUSCODE	BESCHREIBUNG
	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.1.15 Nutzenden aus einer Organisation entfernen

Nutzende können ihr eigenes Konto unabhängig von ihrer Rolle nicht aus einer Organisation entfernen; ein entsprechender Versuch liefert die Antwort `403` .

Senden einer `POST` -Anfrage an den Endpunkt `/organisations/{organisation}/users/remove` .

2.3.1.15.1 Beschreibung

Mit der Remove-Organisation-User-Anfrage entfernen Sie einen Nutzenden aus einer angegebenen Organisation.

2.3.1.15.2 Voraussetzungen

Werte der Anfrage: **Organisations-ID** `{organisation}`

Objekte: keine

2.3.1.15.3 Anfrage

Um einen Nutzenden aus einer Organisation zu entfernen, fügen Sie die **Organisations-ID** `{organisation}` in den Pfad der Anfrage ein.

Für eine detaillierte Spezifikation, welche Informationen zum Entfernen eines Nutzenden aus der Organisation erforderlich sind, muss im Body das folgende Attribut definiert werden:

Attribut	Beschreibung	Werte
`userId`	Die ID des zu entfernenden Nutzenden.	`string`

Als Ergebnis erhalten Sie ein Objekt mit einer Bestätigungsmeldung.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`message`	Die Bestätigungsmeldung, die nach dem Entfernen des Nutzenden zurückgegeben wird.	`string`

2.3.1.15.4 Beispiel

Beispiel-Request-Body:

```
{
  "userId": "string"
}
```

2.3.1.15.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
404	Die Anfrage war nicht erfolgreich, da die angeforderte Ressource nicht gefunden wurde.

2.3.1.16 Benachrichtigungsadresse zur Organisation hinzufügen

Für diese Anfrage benötigen Sie Administrationsrechte für die Organisation oder SOC-Rechte.

Die Adresse darf noch nicht für die Organisation registriert sein; andernfalls gibt die Anfrage einen 422-Fehler zurück.

Senden einer `POST`-Anfrage an den Endpunkt `/organisations/{organisation}/notification-emails`.

2.3.1.16.1 Beschreibung

Mit der Add-Notification-Email-Anfrage registrieren Sie für eine Organisation einen zusätzlichen Benachrichtigungskontakt, der kein Nutzender der Anwendung ist, zum Beispiel ein gemeinsames Postfach oder einen externen Partner. An die Adresse wird eine Bestätigungs-E-Mail gesendet, mit der der Kontakt die Anmeldung bestätigt.

2.3.1.16.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}`

Objekte: keine

2.3.1.16.3 Anfrage

Um einen Benachrichtigungskontakt hinzuzufügen, fügen Sie die **Organisation-ID** `{organisation}` in den Pfad der Anfrage ein und definieren die Zieladresse im Body:

Attribut	Beschreibung	Werte
`email`	Die hinzuzufügende Benachrichtigungsadresse.	`string`

Als Ergebnis erhalten Sie das erzeugte Objekt `NotificationEmail`. Der Kontakt bleibt unbestätigt, bis der Empfänger die Bestätigungs-E-Mail bestätigt hat.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Benachrichtigungsadresse.	`string`
`email`	Die Benachrichtigungsadresse.	`string`
`verified`	Zeigt an, ob die Adresse bestätigt wurde.	`true`, `false`

Attribut	Beschreibung	Werte
`verified_at`	Datum und Uhrzeit der Bestätigung der Adresse im ISO-8601-Format. Solange die Adresse nicht bestätigt ist, ist der Wert `null` .	`string($date-time)`

2.3.1.16.4 Beispiel

Beispiel-Request-Body:

```
{
  "email": "alerts@example.com"
}
```

2.3.1.16.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
201	Die Anfrage war erfolgreich und die Benachrichtigungsadresse wurde angelegt.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.1.17 Benachrichtigungsadresse aus der Organisation löschen

Für diese Anfrage benötigen Sie Administrationsrechte für die Organisation oder SOC-Rechte.

Senden einer `DELETE` -Anfrage an den Endpunkt `/organisations/{organisation}/notification-emails/{notificationEmail}` .

2.3.1.17.1 Beschreibung

Mit der Remove-Notification-Email-Anfrage entfernen Sie einen zusätzlichen Benachrichtigungskontakt aus einer Organisation.

2.3.1.17.2 Voraussetzungen

Werte der Anfrage: **Organisation-ID** `{organisation}` , **Benachrichtigungsadressen-ID** `{notificationEmail}`

Objekte: keine

2.3.1.17.3 Anfrage

Um einen Benachrichtigungskontakt zu entfernen, fügen Sie die **Organisation-ID** `{organisation}` und die **Benachrichtigungsadressen-ID** `{notificationEmail}` in den Pfad der Anfrage ein.

Das System gibt als Antwort auf eine erfolgreiche Anfrage nur den HTTP-Statuscode 204 zurück.

2.3.1.17.4 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
204	Die Anfrage war erfolgreich und die Antwort enthält keinen Inhalt.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
404	Die Anfrage war nicht erfolgreich, da die angeforderte Ressource nicht gefunden wurde.

2.3.2 Netzwerke

2.3.2.1 Netzwerk aus der Organisation löschen

Gelöschte Netzwerke lassen sich nicht wiederherstellen. Um ein Netzwerk nach dem Löschen weiter zu nutzen, legen Sie es neu an.

Diese Anfrage steht ausschließlich SOC-Nutzenden zur Verfügung.

Senden einer `DELETE` -Anfrage an den Endpunkt `/networks/{network}` .

2.3.2.1.1 Beschreibung

Die Delete-Network-Anfrage löscht ein Netzwerk aus der Organisation.

2.3.2.1.2 Voraussetzungen

Werte der Anfrage: **Netzwerk-ID** `{network}`

Objekte: keine

2.3.2.1.3 Anfrage

Um ein Netzwerk zu löschen, fügen Sie die **Netzwerk-ID** `{network}` in den Pfad der Anfrage ein.

Es sind keine weiteren Informationen erforderlich.

Das System gibt als Antwort auf eine erfolgreiche Anfrage nur den HTTP-Statuscode 200 zurück.

2.3.2.1.4 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	

STATUSCODE	BESCHREIBUNG
	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.2.2 Alle Netzwerke mit ihrem Mitigationsstatus auflisten

> ⓘ Die Attribute `pps_limit_percentage` und `bw_limit_percentage` sind nur vorhanden, wenn die Organisation prozentuale Schwellenwerte aktiviert hat.

> ⓘ SOC-Konten müssen stattdessen eine Organisation explizit über den Endpunkt `/organisations/{organisation}/networks` ansprechen.

Senden einer `GET` -Anfrage an den Endpunkt `/networks-with-mitigations` .

2.3.2.2.1 Beschreibung

Mit der List-Networks-With-Mitigations-Anfrage fordern Sie eine Liste aller Netzwerke der aktiven Organisation einschließlich ihres aktuellen Mitigationsstatus an.

2.3.2.2.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.2.2.3 Anfrage

Um eine Liste aller Netzwerke mit ihrem Mitigationsstatus anzufordern, fügen Sie keine zusätzliche Information in den Pfad der Anfrage ein.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `NetworkV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Netzwerks.	`string`
`organisation`	Die zugehörige Organisation.	`object`
`name`	Der Name des Netzwerks.	`string`
`cidr`	Die CIDR des Netzwerks.	`string`
`enabled`	Zeigt an, ob die automatische Mitigation aktiviert ist.	`true` `false`
`data_only`	Zeigt an, dass das Netzwerk ein Monitor-only-Netzwerk ist: im Dashboard sichtbar, aber nicht mitigierbar.	`true` `false`

`mitigation_type`	Der Mitigationstyp des Netzwerks.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`auto_mitigation_strategy`	Die Strategie der automatischen Mitigation des Netzwerks.	`string`
`duration`	Die Dauer der automatischen Mitigation.	`integer`
`subnet_mitigation_override`	Der Mitigations-Override für das Subnetz.	`true` `false`
`pps_limit`	Das konfigurierte Limit für Pakete pro Sekunde.	`integer`
`bw_limit`	Das konfigurierte Bandbreitenlimit.	`integer`
`autoStatus`	Zeigt an, ob das Netzwerk sich aktuell in einer automatischen Mitigation befindet.	`true` `false`
`manualStatus`	Zeigt an, ob das Netzwerk sich aktuell in einer manuellen Mitigation befindet.	`true` `false`

Attribut	Beschreibung	Werte
`active_partial_manual_mitigations`	Die aktiven partiellen manuellen Mitigationen.	`array`
`active_partial_auto_mitigations`	Die aktiven partiellen automatischen Mitigationen.	`array`
`allow_manual_mitigation`	Zeigt an, ob für das Netzwerk manuelle Mitigationen gestartet werden können.	`true` `false`
`extra`	Zusätzliche benutzerdefinierte Felder der Organisation.	`object`

2.3.2.2.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "name": "Customer-A-Prod",
      "cidr": "192.0.2.0/24",
      "enabled": true,
      "data_only": false,
      "mitigation_type": "ACTION_BLACKHOLE",
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "subnet_mitigation_override": false,
      "pps_limit": 0,
      "bw_limit": 0,
      "autoStatus": true,
      "manualStatus": true,
      "active_partial_manual_mitigations": [
        {}
      ],
      "active_partial_auto_mitigations": [
        {}
      ],
      "allow_manual_mitigation": true,
      "extra": {}
    }
```

```
    ],
    "links": {
      "first": "https://datahub-api.com/api/networks?page=1",
      "last": "https://datahub-api.com/api/networks?page=5",
      "prev": null,
      "next": "https://datahub-api.com/api/networks?page=2"
    },
    "meta": {
      "current_page": 1,
      "from": 1,
      "last_page": 5,
      "links": [
        {
          "url": "https://datahub-api.com/api/networks?page=2",
          "label": "Next »",
          "active": false
        }
      ],
      "path": "https://datahub-api.com/api/networks",
      "per_page": 15,
      "to": 15,
      "total": 64
    }
  }
```


2.3.2.2.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.2.3 Alle Netzwerke der Organisation auflisten

SOC-Konten müssen stattdessen eine Organisation explizit über den Endpunkt `/organisations/{organisation}/networks` ansprechen.

Senden einer `GET` -Anfrage an den Endpunkt `/networks` .

2.3.2.3.1 Beschreibung

Mit der List-Networks-Anfrage fordern Sie eine Liste aller Netzwerke der Organisation an.

2.3.2.3.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.2.3.3 Anfrage

Um eine Liste aller Netzwerke anzufordern, ist im Pfad der Anfrage keine zusätzliche Information erforderlich.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `NetworkV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Netzwerks.	`string`
`organisation`	Die zugehörige Organisation, referenziert durch `id` und `name` .	`object`
`name`	Der Name des Netzwerks.	`string`
`cidr`	Der IP-Bereich des Netzwerks in CIDR-Notation.	`string`
`enabled`	Definiert, ob die automatische Mitigation aktiviert ist.	`true` `false`
`data_only`	Definiert, ob das Netzwerk nur überwacht wird: im Dashboard sichtbar, aber nicht mitigierbar.	`true` `false`
`mitigation_type`	Die Art der Mitigation, die bei Überschreitung der Schwellenwerte angewendet wird.	`ACTION_BLACKHOLE` `ACTION_MITIGATE_ONPREM`

Attribut	Beschreibung	Werte
		`ACTION_MITIGATE_CLOUD`
`auto_mitigation_strategy`	Die Strategie für die automatische Mitigation.	`string`
`duration`	Die Dauer der automatischen Mitigation in Sekunden.	`integer`
`subnet_mitigation_override`	Definiert, ob die Subnetzgrößen-Beschränkung überschrieben wird.	`true` `false`
`pps_limit`	Das konfigurierte PPS-Limit.	`integer`
`bw_limit`	Das konfigurierte Bandbreitenlimit.	`integer`
`autoStatus`	Zeigt an, ob sich das Netzwerk aktuell in automatischer Mitigation befindet.	`true` `false`
`manualStatus`	Zeigt an, ob sich das Netzwerk aktuell in manueller Mitigation befindet.	`true` `false`
`active_partial_manual_mitigations`	Die aktiven partiellen manuellen Mitigationen des Netzwerks.	`array`
`active_partial_auto_mitigations`	Die aktiven partiellen automatischen Mitigationen des Netzwerks.	`array`
`allow_manual_mitigation`	Zeigt an, ob für das Netzwerk manuelle Mitigationen gestartet werden können.	`true` `false`
`extra`	Zusätzliche benutzerdefinierte Felder der Organisation.	`object`

2.3.2.3.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
```

```
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "name": "Customer-A-Prod",
      "cidr": "192.0.2.0/24",
      "enabled": true,
      "data_only": false,
      "mitigation_type": "ACTION_BLACKHOLE",
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "subnet_mitigation_override": false,
      "pps_limit": 0,
      "bw_limit": 0,
      "autoStatus": true,
      "manualStatus": true,
      "active_partial_manual_mitigations": [
        {}
      ],
      "active_partial_auto_mitigations": [
        {}
      ],
      "allow_manual_mitigation": true,
      "extra": {}
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```

2.3.2.3.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.2.4 Netzwerk anhand der ID abrufen

> Die Attribute `pps_limit_percentage` und `bw_limit_percentage` sind nur vorhanden, wenn die Organisation prozentuale Schwellenwerte aktiviert hat.

> SOC-Konten müssen eine Organisation stattdessen explizit über den Endpunkt `/organisations/{organisation}/networks` adressieren.

Senden einer `GET` -Anfrage an den Endpunkt `/networks/{network}` .

2.3.2.4.1 Beschreibung

Mit der Get-Network-Anfrage fordern Sie ein einzelnes Netzwerk für eine angegebene ID an.

2.3.2.4.2 Voraussetzungen

Werte der Anfrage: **Netzwerk-ID** `{network}`

Objekte: keine

2.3.2.4.3 Anfrage

Um ein einzelnes Netzwerk anzufordern, fügen Sie die **Netzwerk-ID** `{network}` in den Pfad der Anfrage ein.

Als Ergebnis erhalten Sie ein Objekt `NetworkVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Netzwerks.	`string`
`organisation`	Die zugehörige Organisation.	`object`
`name`	Der Name des Netzwerks.	`string`
`cidr`	Der CIDR-Bereich des Netzwerks.	`string`
`enabled`	Definiert, ob die automatische Mitigation aktiviert ist.	`true` `false`
`data_only`	Definiert, ob das Netzwerk nur überwacht wird: im Dashboard sichtbar, aber nicht mitigierbar.	`true` `false`

`mitigation_type`	Der Mitigationstyp des Netzwerks.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`auto_mitigation_strategy`	Die Strategie der automatischen Mitigation des Netzwerks.	`string`
`duration`	Die Dauer der automatischen Mitigation.	`integer`
`subnet_mitigation_override`	Der Mitigations-Override für das Subnetz.	`true` `false`
`pps_limit`	Das konfigurierte PPS-Limit.	`integer`
`bw_limit`	Das konfigurierte Bandbreitenlimit.	`integer`
`autoStatus`	Definiert, ob für das Netzwerk aktuell eine automatische Mitigation läuft.	`true` `false`
`manualStatus`	Definiert, ob für das Netzwerk aktuell eine manuelle Mitigation läuft.	`true` `false`

Attribut	Beschreibung	Werte
`active_partial_manual_mitigations`	Die aktiven partiellen manuellen Mitigationen.	`array`
`active_partial_auto_mitigations`	Die aktiven partiellen automatischen Mitigationen.	`array`
`allow_manual_mitigation`	Zeigt an, ob für das Netzwerk manuelle Mitigationen gestartet werden können.	`true` `false`
`extra`	Zusätzliche benutzerdefinierte Felder der Organisation.	`object`

2.3.2.4.4 Beispiel

Beispiel-Antwort:


```
{
  "id": "xY9pQ5wR1",
  "organisation": {
    "id": "aB3cD4eF5",
    "name": "ACME GmbH"
  },
  "name": "Customer-A-Prod",
  "cidr": "192.0.2.0/24",
  "enabled": true,
  "data_only": false,
  "mitigation_type": "ACTION_BLACKHOLE",
  "auto_mitigation_strategy": "IP",
  "duration": 0,
  "subnet_mitigation_override": false,
  "pps_limit": 0,
  "bw_limit": 0,
  "autoStatus": true,
  "manualStatus": true,
  "active_partial_manual_mitigations": [
    {}
  ],
  "active_partial_auto_mitigations": [
    {}
  ],
  "allow_manual_mitigation": true,
  "extra": {}
}
```

2.3.2.4.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.2.5 Alle Mitigationen eines Netzwerks auflisten

Die Schwellenwert- und Traffic-Werte — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` sowie (wenn die Funktion für den Bericht zu verworfenen Daten aktiviert ist) `dropped_bits` und `dropped_packets` — werden nur für automatische (durch Erkennung ausgelöste) Mitigationen zurückgegeben. Bei manuellen Mitigationen, die keine Erkennungsdaten enthalten, entfallen sie.

SOC-Konten müssen stattdessen eine Organisation explizit über den Endpunkt `/organisations/{organisation}/mitigations` adressieren.

Senden einer `GET` -Anfrage an den Endpunkt `/networks/{network}/mitigations`.

2.3.2.5.1 Beschreibung

Mit der List-Network-Mitigations-Anfrage fordern Sie eine Liste aller Mitigationen eines angegebenen Netzwerks an.

2.3.2.5.2 Voraussetzungen

Werte der Anfrage: **Netzwerk-ID** `{network}`

Objekte: keine

2.3.2.5.3 Anfrage

Um eine Liste aller Mitigationen eines Netzwerks anzufordern, fügen Sie die **Netzwerk-ID** `{network}` in den Pfad der Anfrage ein.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `MitigationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Mitigation.	`string`
`organisation`	Die zugehörige Organisation.	`object`
`network`	Das Netzwerk oder, bei einer partiellen Mitigation, die spezifische IP, die mitigiert wird.	`string`
`mitigation_type`	Der Typ der Mitigation.	`ACTION_BLACKHOLE` `ACTION_MITIGATE_ONPREM` `ACTION_MITIGATE_CLOUD`
`mitigation_cause`	Die Art, wie die Mitigation ausgelöst wurde.	`MANUAL_TRIGGER` `AUTO_TRIGGER` `OPS_TRIGGER` `UNKNOWN_TRIGGER`
`start`	Das Startdatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`end`	Das Enddatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`created_at`	Das Erstellungsdatum im ISO-8601-Format.	`string($date-time)`
`updated_at`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`

Attribut	Beschreibung	Werte
`actual_bw`	Die tatsächliche Bandbreite der Mitigation.	`number($float)`
`actual_pps`	Die tatsächlichen Pakete pro Sekunde der Mitigation.	`number($float)`
`configured_bw`	Die konfigurierte Bandbreite der Mitigation.	`number($float)`
`configured_pps`	Die konfigurierten Pakete pro Sekunde der Mitigation.	`number($float)`
`configured_bw_percentage`	Die konfigurierte Bandbreite in Prozent.	`number`
`configured_pps_percentage`	Die konfigurierten Pakete pro Sekunde in Prozent.	`number`
`peak_bw`	Die Spitzenbandbreite der Mitigation.	`number($float)`
`peak_pps`	Die maximalen Pakete pro Sekunde der Mitigation.	`number($float)`
`total_bw`	Die Gesamtbandbreite der Mitigation.	`number($float)`
`total_pps`	Die gesamten Pakete pro Sekunde der Mitigation.	`number($float)`
`has_report`	Zeigt an, ob ein Bericht für die Mitigation verfügbar ist.	`true` `false`
`start_user`	Die Nutzenden, die die Mitigation gestartet haben.	`object`
`end_user`	Die Nutzenden, die die Mitigation beendet haben. Dieser Wert ist null, solange die Mitigation läuft.	`object`

2.3.2.5.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "network": "192.0.2.0/24",
      "mitigation_type": "ACTION_MITIGATE_ONPREM",
      "mitigation_cause": "MANUAL_TRIGGER",
      "start": "2026-01-01T00:00:00+00:00",
      "end": "2026-01-01T00:00:00+00:00",
      "created_at": "2026-01-01T00:00:00+00:00",
      "updated_at": "2026-01-01T00:00:00+00:00",
      "actual_bw": 0,
      "actual_pps": 0,
      "configured_bw": 0,
      "configured_pps": 0,
      "configured_bw_percentage": 0,
      "configured_pps_percentage": 0,
      "peak_bw": 0,
      "peak_pps": 0,
      "total_bw": 0,
      "total_pps": 0,
      "has_report": true,
      "start_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      },
      "end_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      }
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
```

```
          "active": false
        }
      ],
      "path": "https://datahub-api.com/api/networks",
      "per_page": 15,
      "to": 15,
      "total": 64
    }
  }
```


2.3.2.5.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.2.6 Einstellungen eines Netzwerks ändern

Der Body muss die Attribute `id` und `modified` enthalten, um den entsprechenden Eintrag zu identifizieren.

Die ID des Eintrags im Pfad der Anfrage muss mit dem Wert des Attributs `id` im Body übereinstimmen.

Die Attribute `pps_limit` und `pps_limit_percentage` schließen sich gegenseitig aus; Gleiches gilt für `bw_limit` und `bw_limit_percentage`.

Der Status `enabled` und das Attribut `subnet_mitigation_override` lassen sich nicht ändern, solange für das Netzwerk eine aktive Mitigation läuft.

Diese Anfrage steht ausschließlich SOC-Nutzenden zur Verfügung.

Senden einer `PATCH` -Anfrage an den Endpunkt `/networks/{network}` .

2.3.2.6.1 Beschreibung

Mit der Change-Network-Anfrage ändern Sie die Einstellungen eines Netzwerks der Organisation.

2.3.2.6.2 Voraussetzungen

Werte der Anfrage: **Netzwerk-ID** `{network}`

Objekte: `NetworkV0`

2.3.2.6.3 Anfrage

Um die Einstellungen eines Netzwerks zu ändern, fügen Sie die **Netzwerk-ID** `{network}` in den Pfad der Anfrage ein.

Für eine detaillierte Spezifikation, welche Informationen zum Ändern der Einstellungen eines Netzwerks erforderlich sind, muss im Body ein Objekt `NetworkV0` mit den folgenden Attributen definiert werden:

Attribut	Beschreibung	Werte
`id`	Die ID des Netzwerks.	`string`
`modified`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`
`cidr`	Der CIDR-Bereich des Netzwerks.	`string`
`enabled`	Definiert, ob die automatische Mitigation für das Netzwerk aktiviert ist. Bei „false" können keine automatischen Mitigationen	`true` `false`

Attribut	Beschreibung	Werte
	ausgelöst werden; manuelle Mitigationen und Ops-Mitigationen sind davon nicht betroffen.	
`pps_limit`	Der PPS-Schwellenwert.	`integer`
`bw_limit`	Der Bandbreiten-Schwellenwert in Mbps.	`integer`

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`name`	Der Name des Netzwerks.	`string`
`pps_limit_calculated`	Der berechnete PPS-Schwellenwert.	`integer`
`bw_limit_calculated`	Der berechnete Bandbreiten-Schwellenwert.	`integer`
`team_id`	Die ID der Organisation, zu der dieses Netzwerk gehört.	`string`
`autoStatus`	Definiert, ob für das Netzwerk aktuell eine automatische Mitigation läuft.	`true` `false`
`manualStatus`	Definiert, ob für das Netzwerk aktuell eine manuelle Mitigation läuft.	`true` `false`
`active_partial_mitigations`	Die aktiven partiellen manuellen Mitigationen.	`array`
	Die aktiven partiellen automatischen Mitigationen.	`array`

Attribut	Beschreibung	Werte
`active_partial_auto_mitigations`		
`country_blocks`	Die aktiven Länderblockierungen.	`array`
`data_only`	Bei „true" wird das Netzwerk im Dashboard nur zur Überwachung angezeigt und kann nicht mitigiert werden.	`true` `false`
`subnet_mitigation_override`	Definiert, ob die Subnetzgrößen-Beschränkung für Cloud- oder Hybrid-Mitigation überschrieben wird.	`true` `false`
`extra`	Zusätzliche Informationen zum Netzwerk.	`object`
`mitigation_type`	Der konfigurierte Mitigationstyp.	`string`
`emails`	Die E-Mail-Adressen für Benachrichtigungen.	`array`
`duration`	Die Standard-Mitigationsdauer in Sekunden.	`integer`
`auto_mitigation_strategy`	Die für automatische Mitigationen verwendete Strategie.	`string`

Als Ergebnis erhalten Sie ein Objekt `NetworkVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Netzwerks.	`string`
`name`	Der Name des Netzwerks.	`string`
`cidr`	Der CIDR-Bereich des Netzwerks.	

Attribut	Beschreibung	Werte
		string
enabled	Definiert, ob die automatische Mitigation für das Netzwerk aktiviert ist. Bei „false" können keine automatischen Mitigationen ausgelöst werden; manuelle Mitigationen und Ops-Mitigationen sind davon nicht betroffen.	true false
pps_limit	Der PPS-Schwellenwert.	integer
bw_limit	Der Bandbreiten-Schwellenwert in Mbps.	integer
pps_limit_calculated	Der berechnete PPS-Schwellenwert.	integer
bw_limit_calculated	Der berechnete Bandbreiten-Schwellenwert.	integer
team_id	Die ID der Organisation, zu der dieses Netzwerk gehört.	string
autoStatus	Definiert, ob für das Netzwerk aktuell eine automatische Mitigation läuft.	true false
manualStatus	Definiert, ob für das Netzwerk aktuell eine manuelle Mitigation läuft.	true false
active_partial_mitigations	Die aktiven partiellen manuellen Mitigationen.	array
	Die aktiven partiellen automatischen Mitigationen.	

Attribut	Beschreibung	Werte
active_partial_auto_mitigations		array
country_blocks	Die aktiven Länderblockierungen.	array
data_only	Bei „true" wird das Netzwerk im Dashboard nur zur Überwachung angezeigt und kann nicht mitigiert werden.	true false
extra	Zusätzliche Informationen zum Netzwerk.	object
mitigation_type	Der konfigurierte Mitigationstyp.	string
emails	Die E-Mail-Adressen für Benachrichtigungen.	array
duration	Die Standard-Mitigationsdauer in Sekunden.	integer
auto_mitigation_strategy	Die für automatische Mitigationen verwendete Strategie.	string

2.3.2.6.4 Beispiel

Beispiel-Request-Body:

```
{
  "name": "Production Network",
  "cidr": "127.0.0.1/32",
  "enabled": true,
  "pps_limit": 1000,
  "bw_limit": 200,
  "pps_limit_calculated": 800,
  "bw_limit_calculated": 160,
```

```
  "team_id": "xY9pQ5wR1",
  "autoStatus": false,
  "manualStatus": false,
  "active_partial_mitigations": [
    {}
  ],
  "active_partial_auto_mitigations": [
    {}
  ],
  "country_blocks": [
    {}
  ],
  "data_only": false,
  "allow_manual_mitigation": true,
  "extra": {},
  "mitigation_type": "string",
  "emails": [
    "string"
  ],
  "duration": 3600,
  "auto_mitigation_strategy": "ip"
}
```


2.3.2.6.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.2.7 Netzwerk zur Organisation hinzufügen

Der Body enthält nicht die Attribute `id`, `created` und `modified`. Das System legt diese Werte nach dem Erstellen des Eintrags fest.

Die Attribute `pps_limit` und `pps_limit_percentage` schließen sich gegenseitig aus; das Gleiche gilt für `bw_limit` und `bw_limit_percentage`.

Für `ACTION_MITIGATE_CLOUD` gilt: IPv4-Netzwerke benötigen mindestens /24, IPv6-Netzwerke mindestens /48.

Diese Anfrage steht ausschließlich SOC-Nutzenden zur Verfügung.

Senden einer `POST`-Anfrage an den Endpunkt `/networks`.

2.3.2.7.1 Beschreibung

Mit der Add-Network-Anfrage fügen Sie der Organisation ein neues Netzwerk hinzu.

2.3.2.7.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: `NetworkV0`

2.3.2.7.3 Anfrage

Um ein Netzwerk hinzuzufügen, ist im Pfad der Anfrage keine zusätzliche Information erforderlich.

Für eine detaillierte Spezifikation, welche Informationen zum Hinzufügen eines Netzwerks erforderlich sind, muss im Body ein Objekt `NetworkV0` mit den folgenden Attributen definiert werden:

Attribut	Beschreibung	Werte
`cidr`	Der IP-Bereich in CIDR-Notation. Muss innerhalb der Organisation eindeutig sein.	`string`

Attribut	Beschreibung	Werte
`enabled`	Definiert, ob die automatische Mitigation für das Netzwerk aktiviert ist. Bei `false` werden keine automatischen Mitigationen ausgelöst; manuelle und Ops-Mitigationen sind davon nicht betroffen.	`true` `false`
`pps_limit`	Der absolute PPS-Schwellenwert. Erforderlich, falls `pps_limit_percentage` nicht angegeben ist.	`integer`
`bw_limit`	Der absolute Bandbreiten-Schwellenwert in Mbps. Erforderlich, falls `bw_limit_percentage` nicht angegeben ist.	`integer`

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`name`	Der Name des Netzwerks.	`string`
`team_id`	Die ID der Organisation, zu der das Netzwerk hinzugefügt wird.	`string`
`pps_limit_calculated`	Der berechnete PPS-Schwellenwert.	`integer`
`bw_limit_calculated`	Der berechnete Bandbreiten-Schwellenwert.	`integer`
`autoStatus`	Zeigt an, ob sich das Netzwerk aktuell in automatischer Mitigation befindet.	`true` `false`
`manualStatus`	Zeigt an, ob sich das Netzwerk aktuell in manueller Mitigation befindet.	`true` `false`
`active_partial_mitigations`	Die aktiven partiellen manuellen Mitigationen.	`array`
	Die aktiven partiellen automatischen Mitigationen.	`array`

Attribut	Beschreibung	Werte
`active_partial_auto_mitigations`		
`country_blocks`	Die aktiven Ländersperren.	`array`
`data_only`	Bei `true` wird das Netzwerk im Dashboard nur zur Überwachung angezeigt und kann nicht mitigiert werden.	`true` `false`
`allow_manual_mitigation`	Zeigt an, ob für das Netzwerk manuelle Mitigationen gestartet werden können. Der Standardwert ist `true` , falls das Attribut fehlt.	`true` `false`
`subnet_mitigation_override`	Definiert, ob die Subnetzgrößen-Beschränkung für Cloud- oder Hybrid-Mitigation überschrieben wird.	`true` `false`
`extra`	Zusätzliche benutzerdefinierte Felder der Organisation.	`object`

`mitigation_type`	Der anzuwendende Mitigationstyp.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`emails`	Die E-Mail-Adressen, die bei Start oder Ende einer Mitigation benachrichtigt werden.	`array`
`duration`	Die maximale Mitigationsdauer in Sekunden (Minimum 300).	`integer`

`auto_mitigation_strategy`	Die Strategie für die automatische Mitigation.	`IP`
		`CIDR`
		`INTERNET`
		`DEFAULT`

Das System gibt als Antwort das Objekt `NetworkV0` mit den Informationen zum neuen Netzwerk zurück.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`message`	Die Statusmeldung der Anfrage.	`string`
`network`	Das neu erstellte Netzwerk als `NetworkV0` -Objekt.	`object`

2.3.2.7.4 Beispiel

Beispiel-Request-Body:

```
{
  "name": "Production Network",
  "cidr": "127.0.0.1/32",
  "enabled": true,
  "pps_limit": 1000,
  "bw_limit": 200,
  "pps_limit_calculated": 800,
  "bw_limit_calculated": 160,
  "team_id": "xY9pQ5wR1",
  "autoStatus": false,
  "manualStatus": false,
  "active_partial_mitigations": [
    {}
  ],
  "active_partial_auto_mitigations": [
    {}
  ],
  "country_blocks": [
    {}
  ],
  "data_only": false,
  "allow_manual_mitigation": true,
  "extra": {},
  "mitigation_type": "string",
  "emails": [
    "string"
  ],
  "duration": 3600,
  "auto_mitigation_strategy": "ip"
}
```

2.3.2.7.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.2.8 Manuelle Mitigation für ein Netzwerk starten

Wenn für das Netzwerk bereits eine manuelle Mitigation aktiv ist, kann keine zweite gestartet werden. Die bestehende Mitigation muss zuerst gestoppt werden. Data-only-Netzwerke können nicht mitigiert werden.

Eine partielle Mitigation kann bei einem Single-Host-Netzwerk (einem IPv4 `/32` oder IPv6 `/128`) nicht gestartet werden, da es nur eine einzelne Adresse umfasst. Lassen Sie `ip` weg, um stattdessen das gesamte Netzwerk zu mitigieren.

Senden einer `POST`-Anfrage an den Endpunkt `/networks/{network}/mitigation/start`.

2.3.2.8.1 Beschreibung

Mit der Start-Manual-Mitigation-Anfrage starten Sie eine manuelle Mitigation für ein angegebenes Netzwerk.

2.3.2.8.2 Voraussetzungen

Werte der Anfrage: **Netzwerk-ID** `{network}`

Objekte: keine

2.3.2.8.3 Anfrage

Um eine manuelle Mitigation zu starten, fügen Sie die **Netzwerk-ID** `{network}` in den Pfad der Anfrage ein.

Der Body erfordert keine Attribute. Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`ip`	Eine Liste einzelner IPs innerhalb des Netzwerks für eine partielle Mitigation. Fehlt die Angabe, wird die gesamte Netzwerk-CIDR mitigiert. Es werden sowohl IPv4 als auch IPv6 akzeptiert.	`array`

Als Ergebnis erhalten Sie ein oder mehrere Objekte `MitigationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Mitigation.	`string`
`organisation`	Die zugehörige Organisation.	`object`
`network`	Das Netzwerk oder bei einer partiellen Mitigation die spezifische IP, die mitigiert wird.	`string`

`mitigation_type`	Der Typ der Mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`mitigation_cause`	Wie die Mitigation ausgelöst wurde.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

Attribut	Beschreibung	Werte
`start`	Das Startdatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`end`	Das Enddatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`created_at`	Das Erstellungsdatum im ISO-8601-Format.	`string($date-time)`
`updated_at`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`
`actual_bw`	Die tatsächliche Bandbreite.	`number($float)`
`actual_pps`	Die tatsächlichen Pakete pro Sekunde.	`number($float)`
`configured_bw`	Die konfigurierte Bandbreite.	`number($float)`
`configured_pps`	Die konfigurierten Pakete pro Sekunde.	`number($float)`
`configured_bw_percentage`	Die konfigurierte Bandbreite in Prozent.	`number`
`configured_pps_percentage`	Die konfigurierten Pakete pro Sekunde in Prozent.	`number`
`peak_bw`	Die Spitzenbandbreite.	`number($float)`
`peak_pps`	Die maximalen Pakete pro Sekunde.	`number($float)`
`total_bw`	Die Gesamtbandbreite.	`number($float)`
`total_pps`	Die gesamten Pakete pro Sekunde.	`number($float)`
`has_report`		`true` `false`

Attribut	Beschreibung	Werte
	Zeigt an, ob für die Mitigation ein Bericht verfügbar ist.	
`start_user`	Die Person, die die Mitigation gestartet hat.	`object`
`end_user`	Die Person, die die Mitigation beendet hat. Dieser Wert ist null, solange die Mitigation läuft.	`object`

2.3.2.8.4 Beispiel

Beispiel-Request-Body:

```
{
  "ip": [
    "192.0.2.1"
  ]
}
```

2.3.2.8.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
304	Die Ressource wurde seit der letzten Anfrage nicht verändert.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.2.9 Aktive manuelle Mitigation eines Netzwerks stoppen

Senden einer `POST` -Anfrage an den Endpunkt `/networks/{network}/mitigation/stop` .

2.3.2.9.1 Beschreibung

Mit der Stop-Mitigation-Anfrage stoppen Sie die aktive manuelle Mitigation für ein angegebenes Netzwerk.

2.3.2.9.2 Voraussetzungen

Werte der Anfrage: **Netzwerk-ID** `{network}`

Objekte: keine

2.3.2.9.3 Anfrage

Um die aktive manuelle Mitigation zu stoppen, fügen Sie die **Netzwerk-ID** `{network}` in den Pfad der Anfrage ein.

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
`ip`	Eine Liste einzelner IPs innerhalb des Netzwerks, für die die Mitigation gestoppt werden soll. Fehlt die Angabe, wird die Mitigation für den gesamten Netzwerk-CIDR gestoppt.	`array`

Als Ergebnis erhalten Sie ein oder mehrere Objekte `MitigationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Mitigation.	`string`
`organisation`	Die zugehörige Organisation.	`object`
`network`	Das Netzwerk oder, bei einer partiellen Mitigation, die spezifische IP, die mitigiert wird.	`string`
	Der Typ der Mitigation.	

Attribut	Beschreibung	Werte
mitigation_type		ACTION_BLACKHOLE ACTION_MITIGATE_ONPREM ACTION_MITIGATE_CLOUD
mitigation_cause	Wie die Mitigation ausgelöst wurde.	MANUAL_TRIGGER AUTO_TRIGGER OPS_TRIGGER UNKNOWN_TRIGGER
start	Das Startdatum der Mitigation im ISO-8601-Format.	string($date-time)
end	Das Enddatum der Mitigation im ISO-8601-Format.	string($date-time)
created_at	Das Erstellungsdatum im ISO-8601-Format.	string($date-time)
updated_at	Das Datum der letzten Änderung im ISO-8601-Format.	string($date-time)
actual_bw	Die tatsächliche Bandbreite.	number($float)
actual_pps	Die tatsächlichen Pakete pro Sekunde.	number($float)
configured_bw	Die konfigurierte Bandbreite.	number($float)
configured_pps	Die konfigurierten Pakete pro Sekunde.	number($float)
configured_bw_percentage	Die konfigurierte Bandbreite in Prozent.	number
configured_pps_percentage	Die konfigurierten Pakete pro Sekunde in Prozent.	number
peak_bw	Die Spitzenbandbreite.	number($float)
peak_pps	Die maximalen Pakete pro Sekunde.	number($float)

Attribut	Beschreibung	Werte
`total_bw`	Die Gesamtbandbreite.	`number($float)`
`total_pps`	Die gesamten Pakete pro Sekunde.	`number($float)`
`has_report`	Ob ein Bericht für die Mitigation verfügbar ist.	`true` `false`
`start_user`	Die Nutzenden, die die Mitigation gestartet haben.	`object`
`end_user`	Die Nutzenden, die die Mitigation beendet haben; null, solange die Mitigation läuft.	`object`

2.3.2.9.4 Beispiel

Beispiel-Request-Body:

```
{
  "ip": [
    "string"
  ]
}
```

2.3.2.9.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
304	Die Ressource wurde seit der letzten Anfrage nicht verändert.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	

STATUSCODE	BESCHREIBUNG
	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.2.10 Resync der Netzwerke der Organisation auslösen

> SOC-Konten können diesen Endpunkt nicht mit einem persönlichen Zugriffstoken aufrufen. Es gibt dafür kein organisationsbezogenes Token-Äquivalent. Nutzen Sie stattdessen die Zugriffsmöglichkeiten über die Webanwendung (Sitzungsauthentifizierung).

Senden einer `POST` -Anfrage an den Endpunkt `/networks/resync` .

2.3.2.10.1 Beschreibung

Mit der Resync-Networks-Anfrage veröffentlichen Sie eine Nachricht, um die Netzwerke der aktuellen Organisation neu zu synchronisieren, so als wäre ein Netzwerk bearbeitet worden.

2.3.2.10.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.2.10.3 Anfrage

Um die Netzwerke neu zu synchronisieren, fügen Sie keine zusätzliche Information in den Pfad der Anfrage ein. Ein Request-Body ist nicht erforderlich.

Als Ergebnis erhalten Sie ein Objekt mit einer Bestätigungsmeldung.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`message`	Die Bestätigungsmeldung, die nach dem Auslösen des Resyncs zurückgegeben wird.	`string`

2.3.2.10.4 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
503	Die Anfrage war nicht erfolgreich, da der Dienst vorübergehend nicht verfügbar ist.

2.3.3 Mitigationen

2.3.3.1 Alle Mitigationen der Organisation auflisten

Die Schwellenwert- und Traffic-Kennzahlen — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` sowie (falls die Funktion für den Bericht verworfener Daten aktiviert ist) `dropped_bits` und `dropped_packets` — werden nur für automatische (durch Erkennung ausgelöste) Mitigationen zurückgegeben. Bei manuellen Mitigationen, die keine Erkennungsdaten enthalten, entfallen sie.

SOC-Konten müssen stattdessen eine Organisation explizit über den Endpunkt `/organisations/{organisation}/mitigations` adressieren.

Senden einer `GET` -Anfrage an den Endpunkt `/mitigations`.

2.3.3.1.1 Beschreibung

Mit der List-Mitigations-Anfrage fordern Sie eine Liste aller Mitigationen der Organisation an.

2.3.3.1.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.3.1.3 Anfrage

Um eine Liste aller Mitigationen anzufordern, fügen Sie dem Pfad der Anfrage keine zusätzlichen Informationen hinzu.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `MitigationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Mitigation.	`string`
`organisation`	Die zugehörige Organisation.	`object`
`network`	Das mitigierte Netzwerk oder bei einer Teil-Mitigation eine einzelne IP-Adresse.	`string`

`mitigation_type`	Der Typ der angewendeten Mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`mitigation_cause`	Wie die Mitigation ausgelöst wurde.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	Wann die Mitigation begonnen hat.	`string($date-time)`
`end`	Wann die Mitigation beendet wurde; null, solange sie noch läuft.	`string($date-time)`
`created_at`	Das Erstellungsdatum des Eintrags im ISO-8601-Format.	`string($date-time)`
`updated_at`	Das Datum der letzten Aktualisierung des Eintrags im ISO-8601-Format.	`string($date-time)`
`actual_bw`	Die gemessene Bandbreite zu Beginn der Mitigation.	`number($float)`
`actual_pps`	Die gemessene Paketrate zu Beginn der Mitigation.	`number($float)`
`configured_bw`	Der zu Beginn der Mitigation konfigurierte Bandbreitenschwellenwert.	`number($float)`

Attribut	Beschreibung	Werte
`configured_pps`	Der zu Beginn der Mitigation konfigurierte Paketratenschwellenwert.	`number($float)`
`configured_bw_percentage`	Der Bandbreitenschwellenwert als Prozentsatz der berechneten Baseline.	`number`
`configured_pps_percentage`	Der Paketratenschwellenwert als Prozentsatz der berechneten Baseline.	`number`
`peak_bw`	Die während der Mitigation beobachtete Spitzenbandbreite.	`number($float)`
`peak_pps`	Die während der Mitigation beobachtete Spitzenpaketrate.	`number($float)`
`total_bw`	Die während der Mitigation verarbeiteten Bits insgesamt.	`number($float)`
`total_pps`	Die während der Mitigation verarbeiteten Pakete insgesamt.	`number($float)`
`has_report`	Definiert, ob ein detaillierter Mitigationsbericht verfügbar ist.	`true` `false`
`start_user`	Wer die Mitigation gestartet hat.	`object`
`end_user`	Wer die Mitigation beendet hat; null, solange sie noch läuft.	`object`

2.3.3.1.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "network": "192.0.2.0/24",
      "mitigation_type": "ACTION_MITIGATE_ONPREM",
      "mitigation_cause": "MANUAL_TRIGGER",
```

```
        "start": "2026-01-01T00:00:00+00:00",
        "end": "2026-01-01T00:00:00+00:00",
        "created_at": "2026-01-01T00:00:00+00:00",
        "updated_at": "2026-01-01T00:00:00+00:00",
        "actual_bw": 0,
        "actual_pps": 0,
        "configured_bw": 0,
        "configured_pps": 0,
        "configured_bw_percentage": 0,
        "configured_pps_percentage": 0,
        "peak_bw": 0,
        "peak_pps": 0,
        "total_bw": 0,
        "total_pps": 0,
        "has_report": true,
        "start_user": {
          "id": "pQ7rS8tU9",
          "name": "Max Mustermann"
        },
        "end_user": {
          "id": "pQ7rS8tU9",
          "name": "Max Mustermann"
        }
      }
    ],
    "links": {
      "first": "https://datahub-api.com/api/networks?page=1",
      "last": "https://datahub-api.com/api/networks?page=5",
      "prev": null,
      "next": "https://datahub-api.com/api/networks?page=2"
    },
    "meta": {
      "current_page": 1,
      "from": 1,
      "last_page": 5,
      "links": [
        {
          "url": "https://datahub-api.com/api/networks?page=2",
          "label": "Next »",
          "active": false
        }
      ],
      "path": "https://datahub-api.com/api/networks",
      "per_page": 15,
      "to": 15,
      "total": 64
    }
  }
```

2.3.3.1.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.3.2 Mitigation anhand der ID abrufen

Die Schwellenwert- und Traffic-Werte — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` sowie (wenn die Funktion für den Dropped-Data-Report aktiviert ist) `dropped_bits` und `dropped_packets` — werden nur für automatische (durch Erkennung ausgelöste) Mitigationen zurückgegeben. Bei manuellen Mitigationen, die keine Erkennungsdaten enthalten, entfallen sie. Sie benötigen für den ausgewählten Zeitraum mindestens READ-Berechtigungen.

SOC-Konten müssen eine Organisation stattdessen explizit über den Endpunkt `/organisations/{organisation}/mitigations` adressieren.

Senden einer `GET` -Anfrage an den Endpunkt `/mitigations/{mitigation}`.

2.3.3.2.1 Beschreibung

Mit der Get-Mitigation-Anfrage fordern Sie eine einzelne Mitigation für eine angegebene ID an.

2.3.3.2.2 Voraussetzungen

Werte der Anfrage: **Mitigation-ID** `{mitigation}`

Objekte: keine

2.3.3.2.3 Anfrage

Um eine Mitigation anzufordern, fügen Sie die **Mitigation-ID** `{mitigation}` in den Pfad der Anfrage ein.

Als Ergebnis erhalten Sie ein Objekt `MitigationVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Mitigation.	`string`
`organisation`	Die zugehörige Organisation der Mitigation.	`object`
`network`	Das Netzwerk oder bei einer partiellen Mitigation die spezifische IP-Adresse, die mitigiert wird.	`string`
`mitigation_type`	Der angewendete Mitigationstyp.	`ACTION_BLACKHOLE` `ACTION_MITIGATE_ONPREM` `ACTION_MITIGATE_CLOUD`
`mitigation_cause`	Wie die Mitigation ausgelöst wurde.	`MANUAL_TRIGGER` `AUTO_TRIGGER` `OPS_TRIGGER` `UNKNOWN_TRIGGER`
`start`	Das Startdatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`end`	Das Enddatum der Mitigation im ISO-8601-Format.	`string($date-time)`
`created_at`	Das Erstellungsdatum im ISO-8601-Format.	`string($date-time)`

Attribut	Beschreibung	Werte
`updated_at`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`
`actual_bw`	Die tatsächliche Bandbreite der Mitigation.	`number($float)`
`actual_pps`	Die tatsächlichen Pakete pro Sekunde der Mitigation.	`number($float)`
`configured_bw`	Die konfigurierte Bandbreite der Mitigation.	`number($float)`
`configured_pps`	Die konfigurierten Pakete pro Sekunde der Mitigation.	`number($float)`
`configured_bw_percentage`	Die konfigurierte Bandbreite als Prozentwert.	`number`
`configured_pps_percentage`	Die konfigurierten Pakete pro Sekunde als Prozentwert.	`number`
`peak_bw`	Die Spitzenbandbreite der Mitigation.	`number($float)`
`peak_pps`	Der Spitzenwert der Pakete pro Sekunde der Mitigation.	`number($float)`
`total_bw`	Die Gesamtbandbreite der Mitigation.	`number($float)`
`total_pps`	Die Gesamtzahl der Pakete pro Sekunde der Mitigation.	`number($float)`
`has_report`	Zeigt an, ob für die Mitigation ein Report verfügbar ist.	`true` `false`
`start_user`	Der Nutzende, der die Mitigation gestartet hat.	`object`
`end_user`	Der Nutzende, der die Mitigation beendet hat; null, solange die Mitigation läuft.	`object`
`peaks`	Die Aufschlüsselung des Spitzenverkehrs der Mitigation.	`object`

2.3.3.2.4 Beispiel

Beispiel-Antwort:


```
{
  "id": "string",
  "organisation": {},
  "network": "string",
  "mitigation_type": "ACTION_BLACKHOLE",
  "mitigation_cause": "MANUAL_TRIGGER",
  "start": "2026-01-01T00:00:00+00:00",
  "end": "2026-01-01T00:00:00+00:00",
  "created_at": "2026-01-01T00:00:00+00:00",
  "updated_at": "2026-01-01T00:00:00+00:00",
  "actual_bw": 0,
  "actual_pps": 0,
  "configured_bw": 0,
  "configured_pps": 0,
  "configured_bw_percentage": 0,
  "configured_pps_percentage": 0,
  "peak_bw": 0,
  "peak_pps": 0,
  "total_bw": 0,
  "total_pps": 0,
  "has_report": true,
  "start_user": {},
  "end_user": {},
  "peaks": {}
}
```


2.3.3.2.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.3.3 Grafikdaten einer Mitigation abrufen

> SOC-Konten können diesen Endpunkt nicht mit einem persönlichen Access Token aufrufen. Es gibt kein organisationsbezogenes Token-Äquivalent dazu. Nutzen Sie stattdessen die Zugriffsmöglichkeiten über die Webanwendung (Sitzungsauthentifizierung).

Senden einer `GET` -Anfrage an den Endpunkt `/mitigations/{mitigation}/data/{dataType}/{field}` .

2.3.3.3.1 Beschreibung

Mit der Get-Mitigation-Data-Anfrage fordern Sie die Grafikdaten für eine bestimmte Mitigation an, gefiltert nach Datentyp und Feld.

2.3.3.3.2 Voraussetzungen

Werte der Anfrage: **Mitigations-ID** `{mitigation}` ; **Datentyp** `{dataType}` ; **Feld** `{field}`

Objekte: keine

2.3.3.3.3 Anfrage

Um die Grafikdaten einer Mitigation anzufordern, fügen Sie die **Mitigations-ID** `{mitigation}` , den **Datentyp** `{dataType}` und das **Feld** `{field}` in den Pfad der Anfrage ein.

Datentyp `{dataType}` definiert die Art der abzurufenden Daten, zum Beispiel `bandwidth` oder `protocol` .

Feld `{field}` definiert das abzurufende Feld, zum Beispiel `bits` oder `packets` .

Als Ergebnis erhalten Sie ein Array von Serien für eine grafische Visualisierung.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`name`	Der Name der Serie.	`string`

Attribut	Beschreibung	Werte
`data`	Das Array der Datenpunkte der Serie. Jeder Punkt liefert die Attribute `x` und `y`.	`array`

2.3.3.3.4 Beispiel

Beispiel-Antwort:

```
[
  {
    "data": [
      {
        "x": 0,
        "y": 0
      }
    ],
    "name": "string"
  }
]
```

2.3.3.3.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.3.4 Manuelle Mitigation anhand der ID stoppen

Senden einer `POST`-Anfrage an den Endpunkt `/mitigations/{mitigation}/stop`.

2.3.3.4.1 Beschreibung

Mit der Stop-Mitigation-Anfrage stoppen Sie eine bestimmte manuelle Mitigation anhand ihrer ID.

2.3.3.4.2 Voraussetzungen

Werte der Anfrage: **Mitigation-ID** `{mitigation}`

Objekte: keine

2.3.3.4.3 Anfrage

Um eine manuelle Mitigation zu stoppen, fügen Sie die **Mitigation-ID** `{mitigation}` in den Pfad der Anfrage ein. Weitere Informationen sind nicht erforderlich.

Als Ergebnis erhalten Sie ein Objekt `MitigationVO` mit den Informationen zur gestoppten Mitigation.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Mitigation.	`string`
`organisation`	Die zugehörige Organisation.	`object`
`network`	Das Netzwerk oder bei einer partiellen Mitigation die spezifische IP, die mitigiert wird.	`string`

`mitigation_type`	Der Typ der Mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`mitigation_cause`	Wie die Mitigation ausgelöst wurde.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	Das Startdatum im ISO-8601-Format.	

Attribut	Beschreibung	Werte
		`string($date-time)`
`end`	Das Enddatum im ISO-8601-Format.	`string($date-time)`
`created_at`	Das Erstellungsdatum im ISO-8601-Format.	`string($date-time)`
`updated_at`	Das Datum der letzten Änderung im ISO-8601-Format.	`string($date-time)`
`actual_bw`	Die tatsächliche Bandbreite.	`number($float)`
`actual_pps`	Die tatsächlichen Pakete pro Sekunde.	`number($float)`
`configured_bw`	Die konfigurierte Bandbreite.	`number($float)`
`configured_pps`	Die konfigurierten Pakete pro Sekunde.	`number($float)`
`configured_bw_percentage`	Die konfigurierte Bandbreite in Prozent.	`number`
`configured_pps_percentage`	Die konfigurierten Pakete pro Sekunde in Prozent.	`number`
`peak_bw`	Die Spitzenbandbreite.	`number($float)`
`peak_pps`	Die maximalen Pakete pro Sekunde.	`number($float)`
`total_bw`	Die Gesamtbandbreite.	`number($float)`
`total_pps`	Die gesamten Pakete pro Sekunde.	`number($float)`
`has_report`	Zeigt an, ob für die Mitigation ein Bericht verfügbar ist.	`true` `false`

Attribut	Beschreibung	Werte
`start_user`	Die Person, die die Mitigation gestartet hat.	`object`
`end_user`	Die Person, die die Mitigation beendet hat. Dieser Wert ist null, solange die Mitigation läuft.	`object`

2.3.3.4.4 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
304	Die Ressource wurde seit der letzten Anfrage nicht verändert.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.4 Anomalien

2.3.4.1 Alle Anomalien der Organisation auflisten

> Die Anomaliefunktion muss für die Organisation aktiviert sein. Wenn die Funktion deaktiviert ist, dann antwortet der Endpunkt mit dem Statuscode 403.

> SOC-Konten können diesen Endpunkt nicht mit einem persönlichen Zugriffstoken aufrufen. Nutzen Sie stattdessen den Zugriff über die Web-Anwendung (Sitzungsauthentifizierung).

Senden einer `GET` -Anfrage an den Endpunkt `/anomalies` .

2.3.4.1.1 Beschreibung

Mit der List-Anomalies-Anfrage fordern Sie eine seitenweise Liste aller bisherigen Anomalien der Organisation an.

2.3.4.1.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.4.1.3 Anfrage

Um eine Liste aller Anomalien anzufordern, ist keine zusätzliche Information im Pfad der Anfrage erforderlich. Um die Liste seitenweise auszugeben, zu sortieren und zu filtern, können Sie die folgenden optionalen Abfrageparameter anhängen:

Attribut	Beschreibung	Werte
`page`	Die angeforderte Seite.	`integer` , mindestens `1` , Standardwert `1`
`perPage`	Die Anzahl der Anomalien pro Seite.	`integer` , `1` bis `100` , Standardwert `10`

Attribut	Beschreibung	Werte
`orderBy`	Das Attribut, nach dem sortiert wird.	`started_at` , `last_updated_at` , `ended_at` , `status` , `cidr` , `types` , Standardwert `started_at`
`orderDir`	Die Sortierrichtung.	`asc` , `desc` , Standardwert `desc`
`search`	Die Volltextsuche über die Attribute `cidr` , `status` und `types` .	`string`
`status`	Gibt nur Anomalien mit diesem Status zurück.	`OPEN` , `UPDATE` , `CLOSED`
`type`	Gibt nur Anomalien zurück, die diesen Typ enthalten.	`VOLUMETRIC` , `PROTOCOL` , `AMPLIFICATION`

Als Ergebnis erhalten Sie ein oder mehrere Objekte `AnomalyVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID der Anomalie.	`string`
`cidr`	Das von der Anomalie betroffene Netzwerk oder die betroffene einzelne IP-Adresse in CIDR-Notation.	`string`
`types`	Die erkannten Anomalietypen. Eine Anomalie kann mehr als einen Typ tragen.	`VOLUMETRIC` , `PROTOCOL` , `AMPLIFICATION`
`status`	Der Status der Anomalie.	`OPEN` , `UPDATE` , `CLOSED`
`started_at`	Datum und Uhrzeit des Beginns der Anomalie im ISO-8601-Format.	`string($date-time)`

Attribut	Beschreibung	Werte
`last_updated_at`	Datum und Uhrzeit der letzten Aktualisierung der Anomalie im ISO-8601-Format.	`string($date-time)`
`ended_at`	Datum und Uhrzeit des Endes der Anomalie im ISO-8601-Format. Solange die Anomalie andauert, ist der Wert `null` .	`string($date-time)`
`metadata`	Zusätzliche Informationen zur Anomalie als Liste von Schlüssel-Wert-Paaren.	`array`

Metadaten, die das erkennende System als privat gekennzeichnet hat, werden nie zurückgegeben. Das Attribut `metadata` enthält ausschließlich öffentliche Einträge.

2.3.4.1.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "aB3xY9",
      "cidr": "203.0.113.0/24",
      "types": [
        "VOLUMETRIC"
      ],
      "status": "OPEN",
      "started_at": "2026-01-01T00:00:00+00:00",
      "last_updated_at": "2026-01-01T00:15:00+00:00",
      "ended_at": null,
      "metadata": [
        {
          "key": "attack_vector",
          "value": "UDP_Reflection"
        }
      ]
    }
  ]
}
```

2.3.4.1.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

2.3.5 Mitigationsberichte

2.3.5.1 Mitigationsstatistiken für einen Monat auflisten

> Diese Anfrage steht ausschließlich Super-Admin-Nutzenden zur Verfügung.

Senden einer `GET` -Anfrage an den Endpunkt `/mitigation-statistic-group/{group}` .

2.3.5.1.1 Beschreibung

Mit der Get-Mitigation-Statistics-Anfrage fordern Sie die Mitigationsstatistiken für einen angegebenen Monat der Organisation an.

2.3.5.1.2 Voraussetzungen

Werte der Anfrage: **Monat** `{group}`

Objekte: keine

2.3.5.1.3 Anfrage

Um die Mitigationsstatistiken anzufordern, fügen Sie den **Monat** `{group}` (im Format `YYYY-MM`) dem Pfad der Anfrage hinzu.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `MitigationStatisticVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`org`	Der Name der Organisation.	`string`
`network`	Die IP-Adresse oder das CIDR des mitigierten Netzwerks.	`string`
`start`	Datum und Uhrzeit des Beginns der Mitigation im ISO-8601-Format.	`string($date-time)`
`end`	Datum und Uhrzeit des Endes der Mitigation im ISO-8601-Format.	`string($date-time)`
`trigger`	Der Auslösetyp der Mitigation: `1` manuell gestartet, `2` automatisch gestartet, `3` durch den Betrieb gestartet.	`1` `2`

Attribut	Beschreibung	Werte
		3
`actual_bw`	Die gemessene Bandbreite in Mbps zu Beginn der Mitigation.	`integer`
`configured_bw`	Der konfigurierte Bandbreitenschwellenwert in Mbps.	`integer`
`actual_pps`	Die gemessenen Pakete pro Sekunde zu Beginn der Mitigation.	`integer`
`configured_pps`	Der konfigurierte Paketratenschwellenwert.	`integer`
`peak_bw`	Die während der Mitigation beobachtete Spitzenbandbreite in Mbps.	`integer`
`peak_pps`	Die während der Mitigation beobachtete Spitzen-Paketrate.	`integer`
`total_bw`	Die während der Mitigation empfangene Gesamtbandbreite in Bits.	`integer`
`total_pps`	Die während der Mitigation empfangenen Pakete insgesamt.	`integer`
`dropped_bits`	Die von der Mitigation verworfenen Bits insgesamt.	`integer`
`dropped_packets`	Die von der Mitigation verworfenen Pakete insgesamt.	`integer`

2.3.5.1.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "org": "Test Organisation",
      "network": "172.0.0.1",
      "start": "2026-01-01T00:00:00+00:00",
      "end": "2026-01-01T00:00:00+00:00",
      "trigger": 1,
```

```
        "actual_bw": 100,
        "configured_bw": 200,
        "actual_pps": 1500,
        "configured_pps": 2000,
        "peak_bw": 400,
        "peak_pps": 3000,
        "total_bw": 123456,
        "total_pps": 78910,
        "dropped_bits": 10000,
        "dropped_packets": 2000
      }
    ],
    "links": {
      "first": "https://datahub-api.com/api/networks?page=1",
      "last": "https://datahub-api.com/api/networks?page=5",
      "prev": null,
      "next": "https://datahub-api.com/api/networks?page=2"
    },
    "meta": {
      "current_page": 1,
      "from": 1,
      "last_page": 5,
      "links": [
        {
          "url": "https://datahub-api.com/api/networks?page=2",
          "label": "Next »",
          "active": false
        }
      ],
      "path": "https://datahub-api.com/api/networks",
      "per_page": 15,
      "to": 15,
      "total": 64
    }
  }
```


2.3.5.1.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.5.2 Alle Monate mit Mitigationsstatistiken auflisten

Dieser Endpunkt steht ausschließlich Super-Admin-Nutzenden zur Verfügung.

Senden einer `GET` -Anfrage an den Endpunkt `/mitigation-statistic-groups` .

2.3.5.2.1 Beschreibung

Mit der List-Mitigation-Statistic-Groups-Anfrage fordern Sie eine paginierte Liste aller Monate an, für die Mitigationsstatistiken der Organisation verfügbar sind.

2.3.5.2.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.5.2.3 Anfrage

Um eine Liste aller Monate mit Mitigationsstatistiken anzufordern, ist keine zusätzliche Information im Pfad der Anfrage erforderlich.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `MitigationStatisticGroupVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die Monatskennung des Eintrags im Format `YYYY-MM` .	`string`

2.3.5.2.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "2026-02"
    }
  ],
  "meta": {
    "current_page": 0,
```

```
    "last_page": 0,
    "per_page": 0,
    "total": 0
  }
}
```


2.3.5.2.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.6 Traffic-Berichte

2.3.6.1 Alle Monate mit Traffic-Report-Daten auflisten

Dieser Endpunkt ist nur für Organisationen mit aktivierten Traffic-Reports verfügbar und erfordert Zugriff auf Admin-Ebene.

SOC-Konten können diesen Endpunkt nicht mit einem persönlichen Access Token aufrufen. Es gibt kein organisationsbezogenes Token-Äquivalent dazu. Nutzen Sie stattdessen die Zugriffsmöglichkeiten über die Webanwendung (Sitzungsauthentifizierung).

Senden einer `GET` -Anfrage an den Endpunkt `/traffic-report-groups` .

2.3.6.1.1 Beschreibung

Mit der List-Traffic-Report-Groups-Anfrage fordern Sie eine Liste aller Monate an, für die Traffic-Report-Daten für die aktive Organisation verfügbar sind.

2.3.6.1.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.6.1.3 Anfrage

Um eine Liste aller Monate mit Traffic-Report-Daten anzufordern, fügen Sie keine zusätzlichen Informationen in den Pfad der Anfrage ein.

Als Ergebnis erhalten Sie ein oder mehrere Objekte mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die Monatskennung im Format `YYYY-MM` .	`string`

2.3.6.1.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "id": "2026-04"
    }
  ]
}
```


2.3.6.1.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.6.2 Traffic-Bericht für einen Typ und Zeitraum abrufen

Dieser Endpunkt steht nur Organisationen zur Verfügung, für die Traffic-Berichte aktiviert sind, und erfordert Zugriffsrechte auf Admin-Ebene.

SOC-Konten können diesen Endpunkt nicht mit einem persönlichen Zugriffstoken aufrufen. Es gibt kein entsprechendes organisationsbezogenes Token. Nutzen Sie stattdessen den Zugriff über die Webanwendung (Sitzungsauthentifizierung).

Senden einer `GET` -Anfrage an den Endpunkt `/traffic-reports/{type}/{date}` .

2.3.6.2.1 Beschreibung

Mit der Get-Traffic-Report-Anfrage fordern Sie die Einträge des Traffic-Berichts für einen angegebenen Typ und Zeitraum an.

2.3.6.2.2 Voraussetzungen

Werte der Anfrage: **Berichtstyp** `{type}` ; **Zeitraum** `{date}`

Objekte: keine

2.3.6.2.3 Anfrage

Um den Traffic-Bericht anzufordern, fügen Sie den **Berichtstyp** `{type}` und den **Zeitraum** `{date}` dem Pfad der Anfrage hinzu.

Berichtstyp `{type}` definiert die Granularität des Berichts. Die folgenden Werte stehen zur Verfügung:

Attribut	Beschreibung	Werte
`daily`	Gibt Traffic-Daten aggregiert nach Tag für den angegebenen Monat zurück.	
`monthly`	Gibt Traffic-Daten aggregiert nach Monat für den angegebenen Monat zurück.	

Zeitraum `{date}` definiert den Berichtszeitraum. Der Wert muss für die tägliche Granularität `YYYY-MM-DD` und für die monatliche Granularität `YYYY-MM` lauten.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `TrafficReportVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`ip`	Die IP-Adresse des Hosts.	`string`
`cidr`	Der CIDR-Block, zu dem die IP-Adresse gehört.	`string`
`period_start`	Der Beginn des Berichtszeitraums in UTC.	`string($date)`
`period_end`	Das Ende des Berichtszeitraums in UTC.	`string($date)`

Attribut	Beschreibung	Werte
`traffic`	Der Gesamt-Traffic für den Zeitraum in Bytes.	`number($float)`
`packets`	Die Gesamtzahl der Pakete für den Zeitraum.	`number($float)`

2.3.6.2.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "ip": "192.0.2.1",
      "cidr": "192.0.2.0/24",
      "period_start": "2026-04-01",
      "period_end": "2026-04-01",
      "traffic": 1234567,
      "packets": 8910
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```

2.3.6.2.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
404	Die Anfrage war nicht erfolgreich, da die angeforderte Ressource nicht gefunden wurde.

2.3.7 Audit-Logs

2.3.7.1 Alle Audit-Log-Einträge der Organisation auflisten

> SOC-Konten können diesen Endpunkt nicht mit einem persönlichen Zugriffstoken aufrufen. Es gibt kein organisationsbezogenes Token-Äquivalent. Nutzen Sie stattdessen den Zugriff über die Web-Anwendung (Sitzungsauthentifizierung).

Senden einer `GET` -Anfrage an den Endpunkt `/auditLogs` .

2.3.7.1.1 Beschreibung

Mit der List-Audit-Logs-Anfrage fordern Sie eine Liste aller Audit-Log-Einträge der Organisation an.

2.3.7.1.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.7.1.3 Anfrage

Um eine Liste aller Audit-Log-Einträge anzufordern, ist keine zusätzliche Information im Pfad der Anfrage erforderlich.

Als Ergebnis erhalten Sie ein oder mehrere Objekte `AuditLogVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`event`	Der Typ des protokollierten Ereignisses.	`string`
`resource`	Der Typ der vom Ereignis betroffenen Ressource.	`string`
`resource_identifier`	Die Kennung der betroffenen Ressource.	`string`
`performed_by`		`string`

Attribut	Beschreibung	Werte
	Der Name des Nutzenden, der die Aktion durchgeführt hat.	
`parameters`	Zusätzliche Parameter und Details des protokollierten Ereignisses.	`object`
`created_at`	Datum und Uhrzeit der Protokollierung des Ereignisses im ISO-8601-Format.	`string($date-time)`

2.3.7.1.4 Beispiel

Beispiel-Antwort:


```
{
  "data": [
    {
      "event": "string",
      "resource": "string",
      "resource_identifier": "string",
      "performed_by": "string",
      "parameters": {},
      "created_at": "2026-01-01T00:00:00+00:00"
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```

2.3.7.1.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.

2.3.8 Benutzerverwaltung

2.3.8.1 Kontoinformationen des authentifizierten Nutzenden abrufen

Senden einer `GET` -Anfrage an den Endpunkt `/users/me` .

2.3.8.1.1 Beschreibung

Mit der Get-Logged-User-Anfrage fordern Sie die Kontoinformationen des aktuell authentifizierten Nutzenden an.

2.3.8.1.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.8.1.3 Anfrage

Um die Kontoinformationen des aktuell authentifizierten Nutzenden anzufordern, fügen Sie dem Pfad der Anfrage keine zusätzlichen Informationen hinzu.

Als Ergebnis erhalten Sie ein Objekt `UserVO` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Nutzenden.	`string`
`name`	Der vollständige Name des Nutzenden.	`string`
`email`	Die E-Mail-Adresse des Nutzenden.	`string`
`activeOrganisation`	Der Organisationskontext, in dem das Token verwendet wird.	`object`

2.3.8.1.4 Beispiel

Beispiel-Antwort:


```
{
  "id": "xY9pQ5wR1",
  "name": "Max Mustermann",
  "email": "max@mustermann.de",
  "activeOrganisation": {
    "id": "xY9pQ5wR1",
    "name": "Test Organisation"
  }
}
```


2.3.8.1.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.

2.3.8.2 Benachrichtigungseinstellung des authentifizierten Nutzenden ändern

Die Benachrichtigungseinstellung steht nur für eine Organisation mit aktivierter Anomaliefunktion und nur für Nutzende zur Verfügung, die weder SOC-Administrierende noch SOC-Nutzende sind. SOC-Administrierende und SOC-Nutzende tragen ihre E-Mail-Adresse stattdessen in die Liste der Benachrichtigungsempfänger der jeweiligen Organisation ein.

Senden einer `PATCH` -Anfrage an den Endpunkt `/users/me/notification-preferences` .

2.3.8.2.1 Beschreibung

Mit der Change-Notification-Preferences-Anfrage ändern Sie die Einstellung des authentifizierten Nutzenden für E-Mail-Benachrichtigungen zu Mitigationen und Anomalien.

2.3.8.2.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: `NotificationPreferencesVO`

2.3.8.2.3 Anfrage

Um die Benachrichtigungseinstellung zu ändern, ist keine zusätzliche Information im Pfad der Anfrage erforderlich.

Für die genaue Angabe, welche Informationen zum Ändern der Benachrichtigungseinstellung erforderlich sind, definieren Sie im Body das Objekt `NotificationPreferencesVO` mit den folgenden Attributen:

Attribut	Beschreibung	Werte
`notificationsEnabled`	Zeigt an, ob der Nutzende für E-Mail-Benachrichtigungen zu Mitigationen und Anomalien angemeldet ist.	`true` , `false`

Als Antwort erhalten Sie das Objekt `ApiUser` mit den aktualisierten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
`id`	Die ID des Nutzenden.	`string`
`name`	Der vollständige Name des Nutzenden.	`string`
`email`	Die E-Mail-Adresse des Nutzenden.	`string`
`notificationsEnabled`	Zeigt an, ob der Nutzende für E-Mail-Benachrichtigungen zu Mitigationen und Anomalien angemeldet ist.	`true` , `false`
`activeOrganisation`	Die Organisation, in deren Kontext der Token arbeitet.	`object`

2.3.8.2.4 Beispiel

Beispiel-Request-Body:

```
{
  "notificationsEnabled": true
}
```

2.3.8.2.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da die Authentifizierung fehlerhaft war.
403	Die Anfrage war nicht erfolgreich, da die erforderlichen Berechtigungen fehlen.
422	Die Anfrage war nicht erfolgreich, da die übermittelten Daten nicht verarbeitet werden konnten.

3. Fehlerbehebung

Dieses Kapitel nennt die Meldungen des Myra DataHub-Portals, ihre Ursache und den Weg, sie zu beheben.

Das Portal meldet einen Fehler an drei Stellen:

- **Unter dem Eingabefeld** – solange ein Wert nicht gültig ist. Die Meldung verschwindet, sobald der Wert stimmt.
- **Als Einblendung am Bildrand** – nachdem eine Aktion fehlgeschlagen ist. Sie nennt die fehlgeschlagene Aktion.
- **Als eigene Seite** – wenn die Anwendung die Anfrage gar nicht ausführen kann, etwa bei fehlender Berechtigung.

Erscheint die allgemeine Meldung **Es gab einen unerwarteten Fehler.**, hat der Server die Anfrage nicht beantwortet. Wiederholen Sie die Aktion. Besteht die Meldung fort, notieren Sie Uhrzeit, Ansicht und Aktion, bevor Sie den Fehler melden.

Die Meldungen erscheinen in der Sprache, die im Portal eingestellt ist. Dieses Kapitel zitiert die deutschen Fassungen.

3.1 Anmeldung

Anmeldung schlägt fehl

Die Anmeldemaske prüft E-Mail-Adresse und Passwort gemeinsam. Sie nennt deshalb nicht, welches der beiden Felder falsch ist.

Meldung	Ursache	Abhilfe
Sie konnten nicht eingeloggt werden. Bitte überprüfen Sie Ihre Anmeldedaten.	E-Mail-Adresse oder Passwort stimmen nicht.	Geben Sie beide Angaben erneut ein. Achten Sie auf die Groß- und Kleinschreibung des Passworts und auf eine aktive Feststelltaste.
Diese Anmeldeinformationen stimmen nicht mit einem passenden Benutzerkonto überein.	Zu der E-Mail-Adresse besteht kein Benutzerkonto.	Prüfen Sie die Schreibweise der E-Mail-Adresse. Besteht das Konto noch nicht, lassen Sie es von einer Person mit Administrationsrechten anlegen.
Das angegebene Passwort ist nicht korrekt.	Das Benutzerkonto besteht, das Passwort passt nicht dazu.	Setzen Sie das Passwort über **Passwort vergessen?** zurück.
Die Anzahl der erlaubten Anmeldeversuche wurde überschritten. Bitte versuchen Sie es in n Sekunden erneut.	Pro E-Mail-Adresse und IP-Adresse sind 15 Anmeldeversuche je Minute erlaubt.	Warten Sie die genannte Zeit ab. Die Sperre endet von selbst; ein weiterer Versuch verlängert sie nicht.

Den Ablauf der Anmeldung beschreibt **Anmeldung**.

Zwei-Faktor-Authentifizierung

Meldung	Ursache	Abhilfe
Der Authentifizierungscode ist ungültig.	Der eingegebene Code passt nicht oder ist abgelaufen.	Ein Code gilt nur kurze Zeit. Warten Sie, bis die Authentifizierungs-Anwendung den nächsten Code erzeugt, und geben Sie diesen ein. Prüfen Sie außerdem, ob die Uhrzeit des Geräts stimmt – eine abweichende Uhrzeit erzeugt ungültige Codes.
Der angegebene Zwei-Faktor-Authentifizierungscode war ungültig.	Derselbe Fehler beim nachträglichen Aktivieren im Reiter **Profil**.	Wiederholen Sie die Eingabe mit dem nächsten Code.
Um auf diese Webseite zuzugreifen, ist eine Zwei-Faktor-Authentifizierung erforderlich.	Für dieses Portal ist die Zwei-Faktor-Authentifizierung Pflicht, im Benutzerkonto aber noch nicht eingerichtet.	Richten Sie die Zwei-Faktor-Authentifizierung ein. Ohne sie bleibt das Portal gesperrt.
Die Zwei-Faktor-Authentifizierung wurden nicht aktiviert.	Eine Aktion setzt die Zwei-Faktor-Authentifizierung voraus, etwa das Anzeigen der Notfall-Wiederherstellungs-Codes.	Aktivieren Sie zuerst die Zwei-Faktor-Authentifizierung.

Auch der zweite Faktor ist begrenzt: nach fünf Eingaben je Minute weist das Portal weitere Versuche ab. Warten Sie in diesem Fall eine Minute.

Steht die Authentifizierungs-Anwendung nicht zur Verfügung – etwa nach einem Gerätewechsel –, melden Sie sich über **Wiederherstellungs-Code anwenden** mit einem der Notfall-Wiederherstellungs-Codes an, die Sie bei der Einrichtung gespeichert

haben. Jeder Code gilt einmal. Sind alle Codes verbraucht oder verloren, setzt nur eine Person mit Administrationsrechten das Benutzerkonto zurück.

Passwort zurücksetzen

Über **Passwort vergessen?** fordern Sie eine E-Mail mit einem Rücksetz-Link an.

Meldung	Ursache	Abhilfe
Wir haben Ihre Anfrage zum Zurücksetzen des Passworts erhalten. Sie werden in Kürze eine E-Mail mit weiteren Anweisungen erhalten.	Das Portal hat die Anfrage angenommen.	Öffnen Sie den Link in der E-Mail. Fehlt die E-Mail, sehen Sie im Spam-Ordner nach.
Die angegebene Email ist mit keinem Benutzerkonto verknüpft.	Zu der E-Mail-Adresse besteht kein Benutzerkonto.	Prüfen Sie die Schreibweise. Verwenden Sie die Adresse, an die die Einladung ging.
Bitte warten Sie einen Augenblick mit dem nächsten Versuch.	Sie haben die Anfrage zu kurz nach der vorherigen gestellt.	Warten Sie einen Moment und fordern Sie den Link erneut an.
Der Token (Code) für die Rücksetzung des Passwortes ist nicht mehr gültig.	Der Link ist abgelaufen oder bereits benutzt.	Fordern Sie einen neuen Link an und öffnen Sie ihn unmittelbar nach Erhalt.
Der Token ist abgelaufen. Bitte starten Sie den Prozess neu.	Der Link zum Aktivieren des Kontos oder zum Setzen des Passworts ist abgelaufen.	Beginnen Sie den Vorgang von vorn.

Passwort wird nicht angenommen

Das neue Passwort muss alle folgenden Regeln erfüllen; verletzt es eine, nennt die Maske genau diese.

Meldung	Anforderung
Das Passwort muss mindestens 12 Zeichen lang sein.	mindestens 12 Zeichen
Das Passwort muss mindestens einen Kleinbuchstaben enthalten.	mindestens ein Kleinbuchstabe
Das Passwort muss mindestens einen Großbuchstaben enthalten.	mindestens ein Großbuchstabe
Das Passwort muss mindestens eine Zahl enthalten.	mindestens eine Ziffer
Das Passwort muss mindestens eines dieser Symbole enthalten: ! @#$%^&*	mindestens eines der Zeichen !@#$%^&*
Das Passwort ist ungültig.	Das Passwort erfüllt die Regeln nicht oder stimmt nicht mit der Wiederholung überein.

Zusätzlich prüft das Portal das Passwort gegen bekannte Datenlecks. Das Portal lehnt ein Passwort, das dort auftaucht, auch dann ab, wenn es alle Regeln erfüllt. Wählen Sie in diesem Fall ein anderes Passwort.

Beim Ändern des Passworts im Reiter **Profil** meldet **Falsches Passwort. Bitte versuche Sie es noch einmal.**, dass Sie das aktuelle Passwort falsch eingegeben haben – nicht das neue.

3.2 Zugriff und Anzeige

Das Portal zeigt eine Fehlerseite

Kann das Portal eine Anfrage nicht ausführen, ersetzt es die Ansicht durch eine Fehlerseite mit der Schaltfläche **Zurück zum Dashboard**.

Seite	Meldung	Ursache	Abhilfe
Zugriff verweigert	**Sie haben keinen Zugriff auf diese Seite.**	Das Benutzerkonto besitzt nicht die Rolle, die diese Ansicht voraussetzt, oder die Ansicht gehört zu einem anderen Unternehmen.	Kehren Sie zum Dashboard zurück. Benötigen Sie die Ansicht für Ihre Arbeit, lassen Sie Ihre Rolle von einer Person mit Administrationsrechten prüfen. Welche Rolle welche Ansicht öffnet, steht unter **Rollen und Berechtigungen**.
Seite nicht gefunden	**Die gewünschte Seite existiert nicht oder wurde verschoben.**	Die Adresse ist falsch geschrieben, oder das Objekt dahinter wurde gelöscht – etwa ein Netzwerk, dessen Adresse noch als Lesezeichen gespeichert ist.	Rufen Sie die Ansicht über die Navigation auf statt über ein Lesezeichen.
Internet Serverfehler	**Es ist ein interner Serverfehler aufgetreten.**	Die Anfrage ist auf dem Server gescheitert.	Wiederholen Sie die Aktion nach kurzer Zeit. Bleibt der Fehler, notieren Sie Uhrzeit und Aktion und melden Sie ihn.

Die Sitzung ist abgelaufen

Führt eine Aktion unerwartet zur Anmeldemaske zurück, ist die Sitzung abgelaufen. Ohne Aktivität endet eine Sitzung standardmäßig nach 120 Minuten; der Betreiber des

Portals kann diesen Wert ändern. Das Schließen des Webbrowsers beendet die Sitzung nicht.

- Melden Sie sich erneut an.
- Führen Sie die Aktion noch einmal aus. Eingaben, die Sie vor dem Ablauf gemacht und nicht gespeichert haben, sind verloren.

Im Reiter **Profil** sehen Sie unter **Aktive Sitzungen**, welche Sitzungen noch geöffnet sind, und beenden sie mit **Andere Sitzungen beenden**. Haben Sie den Eindruck, dass Ihr Benutzerkonto kompromittiert wurde, beenden Sie die anderen Sitzungen und ändern Sie umgehend Ihr Passwort.

Eine Ansicht bleibt leer

Eine leere Liste ist kein Fehler: Das Portal zeigt nur die Daten des Unternehmens, in dem Sie gerade angemeldet sind, und nur den ausgewählten Zeitraum.

Meldung	Bedeutung	Abhilfe
Es sind keine Daten verfügbar.	Für den gewählten Zeitraum liegen keine Messwerte vor.	Wählen Sie einen größeren Betrachtungszeitraum.
Keine Netzwerke vorhanden.	Dem Unternehmen ist kein Netzwerk zugeordnet.	Lassen Sie das Netzwerk vom SOC zuordnen.
Keine Mitigationen vorhanden.	Im gewählten Zeitraum wurde keine Mitigation ausgeführt.	Erweitern Sie den Zeitraum.
Keine Traffic-Daten für den ausgewählten Zeitraum gefunden.	Für den gewählten Monat liegt kein Traffic-Bericht vor.	Wählen Sie einen anderen Monat.
Keine Berichte vorhanden.	Es wurde noch kein Mitigationsbericht erzeugt.	Ein Bericht entsteht erst nach einer abgeschlossenen Mitigation.
Keine Audit-Logs vorhanden.	Im gewählten Zeitraum wurde keine	

Meldung	Bedeutung	Abhilfe
	protokollpflichtige Änderung vorgenommen.	Erweitern Sie den Zeitraum oder setzen Sie den Filter zurück.
Keine Anomalien gefunden.	Im gewählten Zeitraum wurde keine Anomalie erkannt.	Erweitern Sie den Zeitraum.

Bleibt eine Ansicht leer, obwohl Daten zu erwarten sind, prüfen Sie zuerst, ob Sie im richtigen Unternehmen angemeldet sind.

3.3 Netzwerke und Mitigationen

Eine manuelle Mitigation lässt sich nicht starten

Meldung	Ursache	Abhilfe
Die Einstellung für die manuelle Mitigation kann nicht geändert werden, solange eine manuelle Mitigation läuft.	Für das Netzwerk läuft bereits eine manuelle Mitigation.	Beenden Sie die laufende Mitigation und ändern Sie die Einstellung danach.
Diese IP-Adresse gehört nicht zum ausgewählten Netzwerk.	Die eingetragene IP-Adresse liegt außerhalb des Adressbereichs des Netzwerks.	Tragen Sie eine Adresse aus dem Bereich des Netzwerks ein. Lassen Sie das Feld leer, um das gesamte Netzwerk zu mitigieren.
Ungültige IP-Adresse.	Die Eingabe ist keine gültige IP-Adresse.	Geben Sie eine vollständige IPv4- oder IPv6-Adresse ohne Leerzeichen ein.
Das Netzwerk oder die IP-Adresse(n) konnte(n) nicht mitigiert werden.	Der Auftrag ist auf dem Server gescheitert.	Wiederholen Sie den Start nach kurzer Zeit. Prüfen Sie zuvor, ob nicht bereits eine Mitigation für das Netzwerk läuft.

Fehlt die Schaltfläche **Mitigation starten** ganz, ist die manuelle Mitigation für dieses Netzwerk nicht freigeschaltet oder Ihr Benutzerkonto besitzt keine Administrationsrechte. Beides ändert nur das SOC.

Eine Mitigation lässt sich nicht beenden

Meldet das Portal **Die Mitigation(en) konnte(n) nicht gestoppt werden.**, hat der Server den Auftrag nicht angenommen. Wiederholen Sie ihn nach kurzer Zeit.

Beenden lassen sich nur manuell gestartete Mitigationen. Eine automatisch ausgelöste Mitigation endet von selbst, sobald der Angriff abklingt.

Ein Netzwerk lässt sich nicht anlegen oder ändern

Die Adresse eines Netzwerks muss als normalisiertes CIDR angegeben sein: die Netzadresse, gefolgt vom Präfix, ohne gesetzte Host-Bits – zum Beispiel `192.0.2.0/24`, nicht `192.0.2.17/24`.

Meldung	Ursache	Abhilfe
Die IP-Adresse muss in einem normalisierten CIDR-Format vorliegen (IPv4 bis /n, IPv6 bis /n).	Das Format stimmt nicht, oder das Präfix ist kleiner als erlaubt.	Übernehmen Sie die in der Meldung genannten Präfixgrenzen. Sie hängen von der Anbindung der Installation ab und stehen deshalb in der Meldung selbst.
Für Cloud-Scrubbing gilt: IPv4: /24 oder kleiner, IPv6: /48 oder kleiner.	Für ein Netzwerk mit Cloud-Scrubbing wurde ein zu kleiner Adressbereich angegeben.	Geben Sie für IPv4 höchstens ein /24 und für IPv6 höchstens ein /48 an.
Beim Hinzufügen des Netzwerks ist ein Fehler aufgetreten. Bitte versuchen Sie es später noch einmal.	Der Server hat das Netzwerk nicht angelegt.	Wiederholen Sie den Vorgang. Prüfen Sie, ob das Netzwerk bereits besteht.
Beim Bearbeiten des Netzwerks ist ein Fehler aufgetreten. Bitte versuchen Sie es später noch einmal.	Der Server hat die Änderung nicht übernommen.	Wiederholen Sie den Vorgang.

Ein Netzwerk lässt sich nicht löschen

Meldet das Portal **Das Netzwerk IP-Adresse kann nicht gelöscht werden, da derzeit eine Mitigation läuft.**, blockiert eine laufende Mitigation das Löschen.

- ► Beenden Sie die Mitigation des Netzwerks.
- ► Löschen Sie das Netzwerk anschließend erneut.

Die Neusynchronisierung schlägt fehl

Meldet das Portal **Beim Auslösen der Neusynchronisierung der Netzwerke ist ein Fehler aufgetreten. Bitte versuchen Sie es in Kürze erneut.**, hat der Server den Auftrag nicht angenommen. Wiederholen Sie ihn nach kurzer Zeit; die Neusynchronisierung ist wiederholbar und ändert nichts an den Netzwerken selbst.

3.4 Benutzerkonten

Ein Konto lässt sich nicht hinzufügen

Meldung	Ursache	Abhilfe
Dieser Benutzer gehört bereits zum Unternehmen.	Zu der E-Mail-Adresse besteht im Unternehmen schon ein Benutzerkonto.	Suchen Sie das Konto in der Liste. Soll es andere Rechte erhalten, ändern Sie die Rolle, statt ein zweites Konto anzulegen.
Der Benutzer konnte nicht zum Unternehmen hinzugefügt werden.	Der Server hat das Konto nicht angelegt.	Prüfen Sie die E-Mail-Adresse und wiederholen Sie den Vorgang.
Dieses Feld ist erforderlich.	Ein Pflichtfeld ist leer.	Füllen Sie das gekennzeichnete Feld aus.
Der Wert darf höchstens 255 Zeichen lang sein.	Die Eingabe ist zu lang.	Kürzen Sie den Wert auf höchstens 255 Zeichen.
Die Änderungen konnten nicht gespeichert werden.	Der Server hat die Änderung nicht übernommen.	Wiederholen Sie den Vorgang. Prüfen Sie danach in der Liste, ob die Änderung angekommen ist.

Den Ablauf beschreibt **Konto hinzufügen**.

Die eingeladene Person erhält keine E-Mail

Ein neu angelegtes Konto bleibt so lange im Status **Ausstehend**, bis die eingeladene Person die Einladung annimmt und ein Passwort setzt.

- Prüfen Sie in der Liste die Schreibweise der E-Mail-Adresse.
- Lassen Sie im Spam-Ordner des Empfängers nachsehen.
- Senden Sie die Einladung über das Symbol **Erneut einladen** noch einmal.

➔ Das Portal bestätigt mit **Die Einladung wurde erfolgreich an den Benutzer gesendet.**

Meldet das Portal stattdessen **Die Einladung konnte nicht erneut an den Benutzer gesendet werden.**, ist der Versand gescheitert. Wiederholen Sie ihn nach kurzer Zeit. Ist der Einladungslink beim Empfänger bereits abgelaufen – erkennbar an der Meldung **Der Token ist abgelaufen. Bitte starten Sie den Prozess neu.** –, senden Sie die Einladung ebenfalls erneut.

Die SIEM-Verbindung lässt sich nicht herstellen

Der Reiter **SIEM-Einstellungen** prüft die Verbindung erst auf Klick.

Meldung	Ursache	Abhilfe
Die Verbindung konnte nicht hergestellt werden.	Host, Port oder API-Token stimmen nicht, oder das Ziel ist vom Portal aus nicht erreichbar.	Prüfen Sie Host und Port. Tragen Sie den API-Token neu ein – ein gespeicherter Token wird nur als **(gespeichert)** angezeigt und lässt sich nicht auslesen. Lassen Sie anschließend prüfen, ob eine Firewall die Verbindung blockiert.
Die Verbindung konnte hergestellt werden.	Die Angaben stimmen.	Speichern Sie die Einstellungen.

Weitere Angaben zum Reiter stehen unter **Reiter SIEM-Einstellungen**.

3.5 Unternehmen

Ein Unternehmen lässt sich nicht anlegen oder ändern

Meldung	Ursache	Abhilfe
Beim Hinzufügen des Unternehmens ist ein Fehler aufgetreten. Bitte versuchen Sie es später noch einmal.	Der Server hat das Unternehmen nicht angelegt.	Wiederholen Sie den Vorgang. Prüfen Sie zuvor in der Liste, ob das Unternehmen bereits besteht.
Beim Bearbeiten des Unternehmens ist ein Fehler aufgetreten. Bitte versuchen Sie es später noch einmal.	Der Server hat die Änderung nicht übernommen.	Wiederholen Sie den Vorgang.
Dieses Feld ist erforderlich.	Ein Pflichtfeld ist leer.	Füllen Sie das gekennzeichnete Feld aus.
Der Wert muss eine positive Zahl sein.	In einem Zahlenfeld steht eine negative Zahl oder eine Null.	Tragen Sie eine positive Zahl ein.

Ein Unternehmen lässt sich nicht löschen

Meldung	Ursache	Abhilfe
Das Netzwerk kann nicht gelöscht werden, da derzeit eine Mitigation läuft. Bitte beenden Sie zuerst die Mitigation und versuchen Sie es erneut.	Für ein Netzwerk des Unternehmens läuft eine Mitigation. Mit dem Unternehmen würden auch seine Netzwerke gelöscht.	Beenden Sie die Mitigation und löschen Sie das Unternehmen anschließend erneut.
Beim Löschen des Unternehmens ist ein Fehler aufgetreten. Bitte versuchen Sie es später noch einmal.	Der Server hat das Unternehmen nicht gelöscht.	Wiederholen Sie den Vorgang.

Mit einem Unternehmen werden auch seine Netzwerke, Benutzerkonten und Daten unwiderruflich gelöscht.

Zusätzliche Kontakte für Benachrichtigungen

Eine zusätzliche Kontaktadresse bleibt so lange **Ausstehend**, bis der Empfänger die Bestätigungs-E-Mail beantwortet. Erst danach erhält sie Benachrichtigungen.

Meldung	Ursache	Abhilfe
Der Kontakt konnte nicht hinzugefügt werden.	Die Adresse wurde nicht angenommen.	Prüfen Sie die Schreibweise. Prüfen Sie, ob die Adresse bereits in der Liste steht.
Die Bestätigungs-E-Mail konnte nicht erneut gesendet werden.	Der Versand ist gescheitert, oder die Grenze ist erreicht.	Pro Kontakt sind fünf Bestätigungs-E-Mails je Stunde erlaubt. Warten Sie und senden Sie danach erneut.
Der Kontakt konnte nicht entfernt werden.	Der Server hat den Kontakt nicht gelöscht.	Wiederholen Sie den Vorgang.

Bleibt ein Kontakt trotz gesendeter E-Mail auf **Ausstehend**, ist der Bestätigungslink nicht geöffnet worden oder abgelaufen. Senden Sie die Bestätigungs-E-Mail erneut.

3.6 API-Zugriff

Ein API-Token lässt sich nicht erstellen

Meldung	Ursache	Abhilfe
Muss eine ganze Zahl zwischen 1 und 90 sein.	Die Gültigkeitsdauer liegt außerhalb des erlaubten Bereichs.	Tragen Sie eine ganze Zahl zwischen 1 und 90 Tagen ein.
Dieses Feld ist erforderlich.	Der Name des Tokens fehlt.	Vergeben Sie einen Namen, an dem Sie den Token später wiedererkennen.
Beim Erstellen des Tokens ist ein Fehler aufgetreten. Bitte versuchen Sie es erneut.	Der Server hat den Token nicht angelegt.	Wiederholen Sie den Vorgang.
Beim Löschen des Tokens ist ein Fehler aufgetreten. Bitte versuchen Sie es erneut.	Der Server hat den Token nicht gelöscht.	Wiederholen Sie den Vorgang.

> **Bitte kopieren Sie Ihren neuen API-Token. Aus Sicherheitsgründen wird er nicht erneut angezeigt.** Haben Sie den Token nicht kopiert, bevor Sie den Dialog geschlossen haben, lässt er sich nicht nachträglich auslesen. Löschen Sie ihn und erstellen Sie einen neuen.

Den Ablauf beschreibt **API-Token erstellen**.

Die API weist eine Anfrage ab

Antwort	Ursache	Abhilfe
`400 Bad Request`	Die Anfrage ist unvollständig oder enthält einen ungültigen Wert.	Das zurückgegebene Objekt `ViolationVO` nennt das Feld und den Grund. Korrigieren Sie

Antwort	Ursache	Abhilfe
		den Wert und senden Sie die Anfrage erneut.
`401 Unauthorized`	Der Bearer-Token fehlt, ist falsch geschrieben oder abgelaufen.	Prüfen Sie den Kopf `Authorization: Bearer <Token>` . Ein Token gilt höchstens 90 Tage; danach erstellen Sie einen neuen.
`403 Forbidden`	Dem Benutzerkonto hinter dem Token fehlt die Berechtigung für diesen Endpunkt – oder die Kennung im Pfad besteht nicht bzw. gehört zu einem anderen Unternehmen. Beides beantwortet die API gleich, damit sie keine fremden Kennungen preisgibt.	Prüfen Sie zuerst die Kennung im Pfad, danach die Rolle des Benutzerkontos.
`429 Too Many Requests`	Es sind 240 Anfragen je Minute erlaubt, gezählt je Benutzerkonto.	Verteilen Sie die Anfragen über die Zeit. Werten Sie den Kopf `Retry-After` der Antwort aus und wiederholen Sie die Anfrage danach.

Die vollständige Liste steht unter **Mögliche Antworten auf eine Anfrage**.

Ein SOC-Konto erhält keinen Zugriff über seinen API-Token

Weist die API eine Anfrage mit **SOC accounts cannot access organisation-scoped data with a personal access token.** ab, ist das kein Fehler, sondern eine Absicherung: Ein SOC-Konto besitzt keine eigenen Netzwerke. Über einen persönlichen API-Token würde es die Daten desjenigen Unternehmens liefern, in das es zuletzt gewechselt ist.

- Sprechen Sie das Unternehmen im Pfad ausdrücklich an: Verwenden Sie die Endpunkte unter `/organisations/{organisation}/…` statt der Endpunkte ohne Unternehmen im Pfad.

4. Referenz

4.1 Darstellungsmittel

Auszeichnung	Beschreibung
Text in Fett	Kennzeichnet Bildschirmzitate der grafischen Benutzeroberfläche.
Links	Kennzeichnet Verweise auf Kapitel und Abschnitte innerhalb des Handbuchs sowie externe Quellen.
`Dicktenglei ch`	Kennzeichnet Kommandos, Code und Eingaben.
`<ABC>`	Kennzeichnet Platzhalter, die vom Kunden oder vom System ausgefüllt werden.
☑	Kennzeichnet Voraussetzungen, die die Nutzenden vor der Ausführung eines Arbeitsschrittes erfüllen müssen.
▶	Kennzeichnet Arbeitsschritte, die die Nutzenden ausführen sollen.
▷	Kennzeichnet untergeordnete Arbeitsschritte, die die Nutzenden ausführen sollen.
↳	Kennzeichnet das Zwischenergebnis zur Kontrolle nach Ausführung eines oder mehrerer Arbeitsschritte.
➔	Kennzeichnet das Ergebnis, das nach der Ausführung mehrerer Arbeitsschritte vorliegen soll.
ⓘ Text	Kennzeichnet wichtige Hinweise, die die Nutzenden unterstützen sollen.
ⓘ Text	Kennzeichnet besonders wichtige Informationen, die bei Nichtbeachtung zu Fehleinstellungen oder dem Verlust von Daten führen können.
★ Text	Kennzeichnet Beispiele, die die Nutzenden unterstützen sollen.

4.2 Glossar

Element	Beschreibung
Scrubbing	Scrubbing bezeichnet den Vorgang, Internet-Traffic, insbesondere auf OSI-Layer ¾, derart zu filtern, dass valider Clean-Traffic von schädlichem Angriffs-Traffic unterschieden wird.
Scrubbing Center	Ein Scrubbing Center ist ein hochperformanter Internetknoten (Point of Presence / PoP) bestehend aus Hardware, Software und breitbandiger Anbindung, der durch Myra-Technologie in der Lage ist, Scrubbing effizient durchzuführen.
Myra Partner	Ein ISP ist ein Kunde von Myra, der das Myra-Produkt Network DDoS Protection (on-prem) einsetzt und innerhalb seines eigenen Netzwerkes implementiert hat.
Endkunde	Ein Endkunde ist der Kunde eines Myra Partners, der die Dienstleistung volumetrischer DDoS-Schutz für OSI-Layer ¾ **powered by Myra** bezieht.
Network DDoS Protection (cloud)	Cloud Scrubbing ist eine Dienstleistung von Myra, in Form von Security-as-a-Service (SaaS), die das Netzwerk des Myra Partner vor volumetrischen DDoS-Angriffen auf OSI-Layer ¾ schützt. **Funktionalität:** Sobald im Vorfeld definierte Parameter überschritten werden, wird der (Angriffs-)Traffic kurzfristig mittels Border-Gateway-Protocol (BGP)-Rerouting in ein Cloud-Scrubbing-Center umgeleitet und dort vom unerwünschten Traffic **reingewaschen**, um nur Clean-Traffic über eine gesicherte Verbindung an den Empfänger weiterzuleiten. **Vorteile:** Mit Network DDoS Protection (cloud) können DDoS-Angriffe mit einer Bandbreite von mehreren TBit/s zuverlässig abgewehrt werden. Diese Abwehrbandbreite steht dem Myra Partner immer zur Verfügung, auch wenn Sie die gesamte Leitungskapazität (Bandbreite) der eigenen physischen

Element	Beschreibung
	Anbindung des Myra Partners übersteigt. Dabei ist es unerheblich, ob die gesamte Leitungskapazität des Myra Partners physisch durch einen Leitungsanbieter oder durch mehrere (Multi-Vendor-Strategie) realisiert wird. Dieser DDoS-Schutz bleibt auch erhalten, wenn der Myra Partner zukünftig einen Leitungsanbieter wechselt oder weitere dazunimmt. **Einschränkung:** Der Schutz durch Network DDoS Protection (cloud) kann technisch bedingt nur für einzelne /24-Präfixe bei IPv4 bzw. /48-Präfixe bei IPv6 erfolgen. Aufgrund der im Allgemeinen im öffentlichen Internet geltenden Beschränkung auf eben diese Größen können kleinere Netzwerke als /24 bzw. /48 nicht über Cloud Scrubbing geschützt werden.
Network DDoS Protection (on-prem)	Myra stellt seinem Partner ein oder mehrere physische Scrubbing Center zur Verfügung, die in die Netzwerkinfrastruktur des Myra Partner integriert werden. So wird gewährleistet, dass sämtliche Router, die am für das Scrubbing relevanten Routing beteiligt sind, von Myra oder dem Myra Partner kontrolliert werden. Dadurch können auch gültige Routen für kleinere Präfixe (d. h. kleinere Netzwerke als /24 bzw. /48) definiert werden, ohne dass es dadurch zu Problemen beim öffentlichen Routing kommt.
Network DDoS Protection (hybrid)	Network DDoS Protection (hybrid) ist die Kombination aus den Network-DDoS-Schutzlösungen OnPrem und Cloud. Überschreitet die Bandbreite einer DDoS-Attacke die Leitungskapazität (von einer oder auch mehreren physischen Anbindungen) des Myra Partners, kann – im Sinne einer zweiten Verteidigungslinie – auf die Ressourcen von Myra zurückgegriffen und von Network DDoS Protection (on-prem) auf Network DDoS Protection (cloud) umgeschaltet werden, um auch volumetrische DDoS-Attacken auf OSI-Layer ¾ mit Bandbreiten von mehreren TBit/s zuverlässig abzuwehren. So kann der Myra Partner sicherstellen, dass seine eigenen Server und Netze sowie die seiner Endkunden auch während DDoS-Attacken mit extrem großen Bandbreiten erreichbar bleiben.
Myra	Die Myra Flow-Application ist eine Anwendung, die anhand der von den Edge-Routern des Myra Partners gelieferten Daten und zuvor definierter

Element	Beschreibung
Flow-Application	Schwellenwerte DDoS-Attacken erkennt. Das Flow-Monitoring meldet erkannte Angriffe an nachgelagerte Instanzen, um automatisch Gegenmaßnahmen einzuleiten. Die Anwendung wird in der Netzwerkinfrastruktur des Myra Partners betrieben, üblicherweise auf einer virtuellen Maschine.
Uplink	Ein Uplink ist ein dedizierter Kanal für die Rückleitung des gereinigten Traffics an den Myra Partner nach erfolgtem Scrubbing. Dieser Kanal ist notwendig, um einen Routing-Loop zu vermeiden. Uplinks können als Direct Connect (physisch) sowie als VLAN, IPsec, GRE (virtuell) redundant aufgebaut werden.
On Demand	On Demand bedeutet, dass die Filterung des Traffics erst aktiviert wird, sobald ein Angriff die festgelegten Schwellenwerte überschreitet. Normalerweise fließt der Traffic nicht über das Scrubbing-Center. Bei automatischer Angriffserkennung wird das Routing umgestellt und der Datenverkehr dort verarbeitet. Nach 24 Stunden wird das reguläre Routing wiederhergestellt – ein Zeitraum, den Myra empfiehlt, um unnötiges Route-Flapping zu verhindern.
Route-Flapping	Das Route-Flapping bezeichnet den Zustand von unterschiedlichen im Internet bekannt gegebenen Routen (announced routes) zum selben Zeitpunkt. Dies ist gefährlich und hat weitreichende negative Folgen auf das Routing im öffentlichen Internet.
Myra App	Die Myra App ist eine webbasierte Benutzeroberfläche zur Steuerung und Konfiguration der Schutzsysteme.
Myra DataHub	Der Myra DataHub ist eine webbasierte Benutzeroberfläche (WebGUI) für Myra Partner zur Übersicht der Endkunden. Darauf sind die Endkunden mit den aufgeschalteten Netzen, sowie deren angelegten Konten dargestellt. Dem Endkunden werden innerhalb dieser WebGUI die Übersicht zum Traffic-Verlauf, die aufgeschalteten Netze, sowie die gesammelten Mitigationsreports präsentiert. Innerhalb der Darstellung des Traffic-Verlaufs ist eine Filterung zwischen Bandbreite und Paketrate, sortiert nach Ziel-IP, Übersicht zu Quell-Ländern, ASN sowie den Paketraten nach Port möglich. Zusätzlich können verschiedene Betrachtungszeiträume bis zu 24 Stunden definiert werden. Die gesetzten Schwellenwerte sind über die WebGUI

Element	Beschreibung
	ebenfalls einsehbar. Darüber hinaus umfasst die Funktionalität des Myra DataHub die Möglichkeit zur Einleitung der manuellen Mitigation sowie zur Konfiguration der definierten Unternehmen, Netzwerke und User durch den Myra Partner.