

Myra DataHub

SOC-Handbuch (Versatel)

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 • Neue Abschnitte • Kleinere Korrekturen Aktualisierte Abschnitte: • Ansicht Netzwerke • Netzwerk ansehen • Netzwerk hinzufügen • Netzwerk ändern • Netzwerk löschen • Manuelle Mitigationen starten • Manuelle Mitigationen beenden • Konto hinzufügen • Konto ändern • Konto löschen • Reiter API-Token • Aktive Webbrowser-Sitzungen beenden • Unternehmensmanagement • Ansicht Dashboard Neue Abschnitte: • Ansicht Anomalieverlauf • Reiter Benachrichtigungen • Alle Anomalien der Organisation auflisten • Benachrichtigungseinstellung des authentifizierten Nutzens ändern • Benachrichtigungsadresse zur Organisation hinzufügen

Version	Datum	Änderungsgrund
		• Benachrichtigungsadresse aus der Organisation löschen • 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	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
V1.4	08/2025	Aktualisierte Abschnitte • Detailansicht Monatsbericht

Version	Datum	Änderungsgrund
V1.3	07/2025	Kleinere Korrekturen
V1.2	05/2025	Aktualisierte Abschnitte • Neue Abschnitte 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	16
1.1 Beschreibung	16
1.1.1 Was ist der Myra DataHub?	16
1.1.2 Zielgruppe	17
1.2 Erste Schritte	18
1.2.1 Konto aktivieren	18
1.2.2 Anmeldung	20
1.3 DataHub-Portal	22
1.3.1 Übersicht Myra DataHub-Portal	22
1.3.1.1 Ansicht Unternehmenskonten	23
1.3.1.1.1 Unternehmen ändern	26
1.3.1.2 Ansicht Bericht	28
1.3.1.2.1 Detailansicht Monatsbericht	29
1.3.1.3 Ansicht Audit-Log	31
1.3.1.4 Ansicht Versionsverlauf	32
1.3.2 Unternehmensmanagement	33
1.3.2.1 Ansicht Dashboard	35
1.3.2.2 Ansicht Netzwerke	38
1.3.2.2.1 Netzwerk ansehen	40
1.3.2.2.2 Netzwerk hinzufügen	43
1.3.2.2.3 Netzwerk ändern	46
1.3.2.2.4 Netzwerk löschen	48
1.3.2.2.5 Manuelle Mitigationen starten	48
1.3.2.2.6 Manuelle Mitigationen beenden	52
1.3.2.3 Ansicht Mitigationsverlauf	54
1.3.2.3.1 Mitigationsberichte öffnen	55
1.3.2.3.2 Ansicht Mitigationsberichte	56
1.3.2.4 Ansicht Anomalieverlauf	58
1.3.2.4.1 Dialog Anomaliedetails	61

1.3.2.5 Ansicht Audit-Log	62
1.3.3 Benutzerverwaltung	64
1.3.3.1 Ansicht Benutzerverwaltung	65
1.3.3.2 Reiter Benutzerverwaltung	65
1.3.3.2.1 Konto hinzufügen	65
1.3.3.2.2 Konto ändern	66
1.3.3.2.3 Konto löschen	67
1.3.3.3 Reiter SIEM-Einstellungen	69
1.3.3.4 Reiter Benachrichtigungen	71
1.3.3.4.1 Bereich Benachrichtigungen	71
1.3.3.4.2 Bereich Zusätzliche Kontakte	72
1.3.4 Persönliches Konto	74
1.3.4.1 Reiter Profil	74
1.3.4.1.1 Benutzernamen ändern	75
1.3.4.1.2 Passwort aktualisieren	75
1.3.4.1.3 Zwei-Faktor-Authentifizierung aktivieren	75
1.3.4.1.4 Aktive Webbrowser-Sitzungen beenden	80
1.3.4.2 Reiter Benachrichtigungen	81
1.3.4.3 Reiter API-Token	82
1.3.4.3.1 Bereich API-Token erstellen	83
1.3.4.3.2 Bereich API-Tokens verwalten	83
1.4 Berechtigungen	85
1.4.1 Rollen und Berechtigungen	85
2. API	88
2.1 Verwendung der Myra API	88
2.2 Allgemein	89
2.2.1 Zugriff zur Myra API erhalten	89
2.2.2 Authentifizierung mittels Bearer-Token	90
2.2.2.1 API-Token erstellen	90
2.2.2.2 Anfrage mittels Bearer-Token an die API stellen	91

2.2.3	Verwendete API-Methoden	93
2.2.4	Mögliche Antworten auf eine Anfrage	94
2.2.4.1	Mögliche Statuscodes	94
2.2.4.2	Verwendete Objekte	95
2.3	API-Endpunkte	96
2.3.1	Organisationsverwaltung	97
2.3.1.1	Organisation löschen	97
2.3.1.1.1	Beschreibung	97
2.3.1.1.2	Voraussetzungen	97
2.3.1.1.3	Anfrage	97
2.3.1.1.4	Antworten	98
2.3.1.2	SIEM-Konfiguration einer Organisation löschen	98
2.3.1.2.1	Beschreibung	98
2.3.1.2.2	Voraussetzungen	98
2.3.1.2.3	Anfrage	98
2.3.1.2.4	Antworten	99
2.3.1.3	Organisationen mit Netzwerk- und Mitigationsdetails auflisten	99
2.3.1.3.1	Beschreibung	99
2.3.1.3.2	Voraussetzungen	99
2.3.1.3.3	Anfrage	99
2.3.1.3.4	Beispiel	100
2.3.1.3.5	Antworten	102
2.3.1.4	Alle Organisationen des Nutzens auflisten	102
2.3.1.4.1	Beschreibung	102
2.3.1.4.2	Voraussetzungen	102
2.3.1.4.3	Anfrage	103
2.3.1.4.4	Beispiel	103
2.3.1.4.5	Antworten	104
2.3.1.5	Organisation anhand der ID abrufen	104
2.3.1.5.1	Beschreibung	105
2.3.1.5.2	Voraussetzungen	105
2.3.1.5.3	Anfrage	105
2.3.1.5.4	Beispiel	106
2.3.1.5.5	Antworten	107

2.3.1.6 Alle Mitigationen einer Organisation auflisten	107
2.3.1.6.1 Beschreibung	107
2.3.1.6.2 Voraussetzungen	107
2.3.1.6.3 Anfrage	108
2.3.1.6.4 Beispiel	110
2.3.1.6.5 Antworten	111
2.3.1.7 Alle Netzwerke einer Organisation auflisten	112
2.3.1.7.1 Beschreibung	112
2.3.1.7.2 Voraussetzungen	112
2.3.1.7.3 Anfrage	112
2.3.1.7.4 Beispiel	113
2.3.1.7.5 Antworten	115
2.3.1.8 Alle Nutzenden einer Organisation auflisten	115
2.3.1.8.1 Beschreibung	115
2.3.1.8.2 Voraussetzungen	115
2.3.1.8.3 Anfrage	115
2.3.1.8.4 Beispiel	116
2.3.1.8.5 Antworten	117
2.3.1.9 Einstellungen einer Organisation ändern	117
2.3.1.9.1 Beschreibung	117
2.3.1.9.2 Voraussetzungen	117
2.3.1.9.3 Anfrage	117
2.3.1.9.4 Beispiel	118
2.3.1.9.5 Antworten	119
2.3.1.10 SIEM-Konfiguration einer Organisation ändern	119
2.3.1.10.1 Beschreibung	119
2.3.1.10.2 Voraussetzungen	119
2.3.1.10.3 Anfrage	120
2.3.1.10.4 Beispiel	121
2.3.1.10.5 Antworten	121
2.3.1.11 Nutzende innerhalb einer Organisation ändern	122
2.3.1.11.1 Beschreibung	122
2.3.1.11.2 Voraussetzungen	122
2.3.1.11.3 Anfrage	122
2.3.1.11.4 Beispiel	123
2.3.1.11.5 Antworten	124

2.3.1.12	Organisation hinzufügen	124
2.3.1.12.1	Beschreibung	124
2.3.1.12.2	Voraussetzungen	124
2.3.1.12.3	Anfrage	124
2.3.1.12.4	Beispiel	125
2.3.1.12.5	Antworten	125
2.3.1.13	Bestätigungs-E-Mail für eine Benachrichtigungsadresse erneut senden	126
2.3.1.13.1	Beschreibung	126
2.3.1.13.2	Voraussetzungen	126
2.3.1.13.3	Anfrage	127
2.3.1.13.4	Beispiel	127
2.3.1.13.5	Antworten	127
2.3.1.14	Nutzende zur Organisation hinzufügen	128
2.3.1.14.1	Beschreibung	128
2.3.1.14.2	Voraussetzungen	128
2.3.1.14.3	Anfrage	128
2.3.1.14.4	Beispiel	129
2.3.1.14.5	Antworten	129
2.3.1.15	Nutzenden aus einer Organisation entfernen	130
2.3.1.15.1	Beschreibung	130
2.3.1.15.2	Voraussetzungen	130
2.3.1.15.3	Anfrage	130
2.3.1.15.4	Beispiel	131
2.3.1.15.5	Antworten	131
2.3.1.16	Benachrichtigungsadresse zur Organisation hinzufügen	131
2.3.1.16.1	Beschreibung	132
2.3.1.16.2	Voraussetzungen	132
2.3.1.16.3	Anfrage	132
2.3.1.16.4	Beispiel	133
2.3.1.16.5	Antworten	133
2.3.1.17	Benachrichtigungsadresse aus der Organisation löschen	133
2.3.1.17.1	Beschreibung	134
2.3.1.17.2	Voraussetzungen	134
2.3.1.17.3	Anfrage	134
2.3.1.17.4	Antworten	134
2.3.2	Netzwerke	135

2.3.2.1 Netzwerk aus der Organisation löschen	135
2.3.2.1.1 Beschreibung	135
2.3.2.1.2 Voraussetzungen	135
2.3.2.1.3 Anfrage	135
2.3.2.1.4 Antworten	135
2.3.2.2 Alle Netzwerke mit ihrem Mitigationsstatus auflisten	136
2.3.2.2.1 Beschreibung	136
2.3.2.2.2 Voraussetzungen	136
2.3.2.2.3 Anfrage	136
2.3.2.2.4 Beispiel	138
2.3.2.2.5 Antworten	139
2.3.2.3 Alle Netzwerke der Organisation auflisten	139
2.3.2.3.1 Beschreibung	139
2.3.2.3.2 Voraussetzungen	139
2.3.2.3.3 Anfrage	140
2.3.2.3.4 Beispiel	141
2.3.2.3.5 Antworten	142
2.3.2.4 Netzwerk anhand der ID abrufen	142
2.3.2.4.1 Beschreibung	143
2.3.2.4.2 Voraussetzungen	143
2.3.2.4.3 Anfrage	143
2.3.2.4.4 Beispiel	144
2.3.2.4.5 Antworten	145
2.3.2.5 Alle Mitigationen eines Netzwerks auflisten	145
2.3.2.5.1 Beschreibung	146
2.3.2.5.2 Voraussetzungen	146
2.3.2.5.3 Anfrage	146
2.3.2.5.4 Beispiel	148
2.3.2.5.5 Antworten	149
2.3.2.6 Einstellungen eines Netzwerks ändern	150
2.3.2.6.1 Beschreibung	150
2.3.2.6.2 Voraussetzungen	150
2.3.2.6.3 Anfrage	150
2.3.2.6.4 Beispiel	155
2.3.2.6.5 Antworten	155
2.3.2.7 Netzwerk zur Organisation hinzufügen	156

2.3.2.7.1 Beschreibung	156
2.3.2.7.2 Voraussetzungen	156
2.3.2.7.3 Anfrage	157
2.3.2.7.4 Beispiel	159
2.3.2.7.5 Antworten	160
2.3.2.8 Manuelle Mitigation für ein Netzwerk starten	160
2.3.2.8.1 Beschreibung	161
2.3.2.8.2 Voraussetzungen	161
2.3.2.8.3 Anfrage	161
2.3.2.8.4 Beispiel	163
2.3.2.8.5 Antworten	163
2.3.2.9 Aktive manuelle Mitigation eines Netzwerks stoppen	164
2.3.2.9.1 Beschreibung	164
2.3.2.9.2 Voraussetzungen	164
2.3.2.9.3 Anfrage	164
2.3.2.9.4 Beispiel	166
2.3.2.9.5 Antworten	166
2.3.2.10 Resync der Netzwerke der Organisation auslösen	167
2.3.2.10.1 Beschreibung	167
2.3.2.10.2 Voraussetzungen	167
2.3.2.10.3 Anfrage	167
2.3.2.10.4 Antworten	168
2.3.3 Mitigationen	169
2.3.3.1 Alle Mitigationen der Organisation auflisten	169
2.3.3.1.1 Beschreibung	169
2.3.3.1.2 Voraussetzungen	169
2.3.3.1.3 Anfrage	169
2.3.3.1.4 Beispiel	171
2.3.3.1.5 Antworten	173
2.3.3.2 Mitigation anhand der ID abrufen	173
2.3.3.2.1 Beschreibung	173
2.3.3.2.2 Voraussetzungen	174
2.3.3.2.3 Anfrage	174
2.3.3.2.4 Beispiel	176
2.3.3.2.5 Antworten	177
2.3.3.3 Grafikdaten einer Mitigation abrufen	177

2.3.3.3.1 Beschreibung	177
2.3.3.3.2 Voraussetzungen	177
2.3.3.3.3 Anfrage	177
2.3.3.3.4 Beispiel	178
2.3.3.3.5 Antworten	178
2.3.3.4 Manuelle Mitigation anhand der ID stoppen	179
2.3.3.4.1 Beschreibung	179
2.3.3.4.2 Voraussetzungen	179
2.3.3.4.3 Anfrage	179
2.3.3.4.4 Antworten	181
2.3.4 Anomalien	182
2.3.4.1 Alle Anomalien der Organisation auflisten	182
2.3.4.1.1 Beschreibung	182
2.3.4.1.2 Voraussetzungen	182
2.3.4.1.3 Anfrage	182
2.3.4.1.4 Beispiel	184
2.3.4.1.5 Antworten	185
2.3.5 Mitigationsberichte	186
2.3.5.1 Mitigationsstatistiken für einen Monat auflisten	186
2.3.5.1.1 Beschreibung	186
2.3.5.1.2 Voraussetzungen	186
2.3.5.1.3 Anfrage	186
2.3.5.1.4 Beispiel	187
2.3.5.1.5 Antworten	188
2.3.5.2 Alle Monate mit Mitigationsstatistiken auflisten	189
2.3.5.2.1 Beschreibung	189
2.3.5.2.2 Voraussetzungen	189
2.3.5.2.3 Anfrage	189
2.3.5.2.4 Beispiel	189
2.3.5.2.5 Antworten	190
2.3.6 Country-Packet-Reports	191
2.3.6.1 Den Country-Packet-Report des aktuellen Monats abrufen	191
2.3.6.1.1 Beschreibung	191
2.3.6.1.2 Voraussetzungen	191
2.3.6.1.3 Anfrage	191

2.3.6.1.4 Beispiel	192
2.3.6.1.5 Antworten	193
2.3.6.2 Den Country-Packet-Report eines bestimmten Monats abrufen	193
2.3.6.2.1 Beschreibung	193
2.3.6.2.2 Voraussetzungen	193
2.3.6.2.3 Anfrage	194
2.3.6.2.4 Beispiel	194
2.3.6.2.5 Antworten	194
2.3.6.3 Den Country-Packet-Report des aktuellen Tages abrufen	195
2.3.6.3.1 Beschreibung	195
2.3.6.3.2 Voraussetzungen	195
2.3.6.3.3 Anfrage	195
2.3.6.3.4 Beispiel	196
2.3.6.3.5 Antworten	197
2.3.6.4 Den Country-Packet-Report eines bestimmten Tages abrufen	197
2.3.6.4.1 Beschreibung	197
2.3.6.4.2 Voraussetzungen	197
2.3.6.4.3 Anfrage	198
2.3.6.4.4 Beispiel	198
2.3.6.4.5 Antworten	199
2.3.7 Audit-Logs	200
2.3.7.1 Alle Audit-Log-Einträge der Organisation auflisten	200
2.3.7.1.1 Beschreibung	200
2.3.7.1.2 Voraussetzungen	200
2.3.7.1.3 Anfrage	200
2.3.7.1.4 Beispiel	201
2.3.7.1.5 Antworten	202
2.3.8 Benutzerverwaltung	203
2.3.8.1 Kontoinformationen des authentifizierten Nutzens abrufen	203
2.3.8.1.1 Beschreibung	203
2.3.8.1.2 Voraussetzungen	203
2.3.8.1.3 Anfrage	203
2.3.8.1.4 Beispiel	204
2.3.8.1.5 Antworten	204
2.3.8.2 Benachrichtigungseinstellung des authentifizierten Nutzens ändern	204

2.3.8.2.1 Beschreibung	205
2.3.8.2.2 Voraussetzungen	205
2.3.8.2.3 Anfrage	205
2.3.8.2.4 Beispiel	206
2.3.8.2.5 Antworten	206
3. Fehlerbehebung	207
3.1 Anmeldung	208
3.2 Zugriff und Anzeige	212
3.3 Netzwerke und Mitigationen	215
3.4 Benutzerkonten	217
3.5 Unternehmen	219
3.6 API-Zugriff	221
4. Referenz	223
4.1 Darstellungsmittel	223
4.2 Konfiguration über YAML	224
4.3 Glossar	230

1. Myra DataHub

1.1 Beschreibung

1.1.1 Was ist der Myra DataHub?

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 Paketrage, sortiert nach Ziel-IP, Übersicht zu Quell-Ländern, ASN 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.

1.1.2 Zielgruppe

Das Handbuch richtet sich ausschließlich an interne Nutzende des SOC-Modus und ist nicht für die Anwendung durch externe Nutzende gedacht.

1.2 Erste Schritte

1.2.1 Konto aktivieren

Bevor Sie sich im Myra DataHub anmelden können, muss ein Admin Ihnen ein Konto im Myra DataHub anlegen. Sobald Ihr neues Konto angelegt wurde, erhalten Sie eine Einladungs-E-Mail.



Bitte beachten Sie, dass diese E-Mail von der Adresse **noc@myrasecurity.com** versendet wird.

Um das Konto zu aktivieren, gehen Sie wie folgt vor:

- Öffnen Sie die Einladungs-E-Mail.

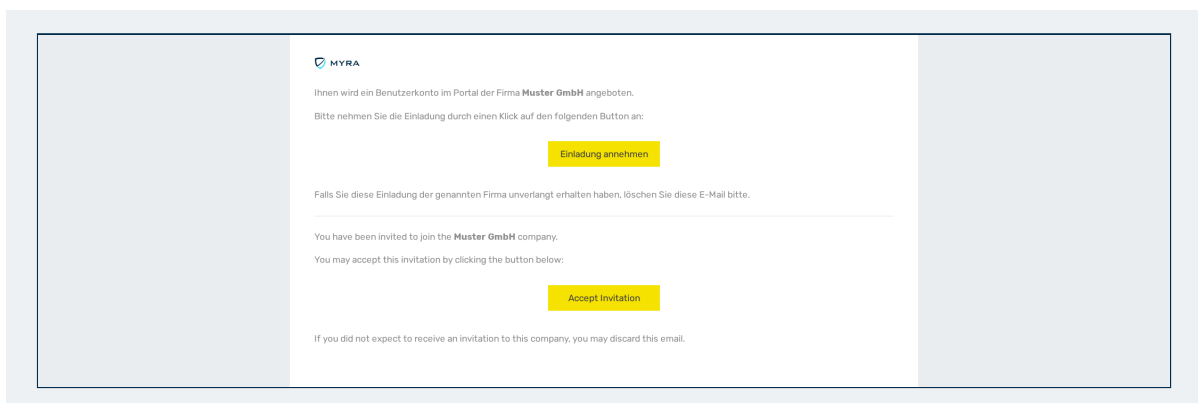


Abbildung 1: Einladungs-E-Mail

- Klicken Sie auf die Schaltfläche **Account aktivieren** in der Einladungs-E-Mail.
 - ↳ Die Webseite des Myra DataHub öffnet sich.



Abbildung 2: Dialog zum Ändern des Passwortes

- Geben Sie Ihr neues Passwort ein.



Das Passwort muss mindestens 12 Zeichen lang sein und mindestens je einen Großbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.

- Bestätigen Sie Ihr neues Passwort.
- Klicken Sie auf die Schaltfläche **Speichern**.
- Ihr neues Konto ist nun aktiviert.

1.2.2 Anmeldung

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

- ▶ Öffnen Sie die Website.
- ▶ Geben Sie in der Anmeldemaske die folgenden Daten ein:
 - **E-Mail-Adresse**
 - **Passwort**

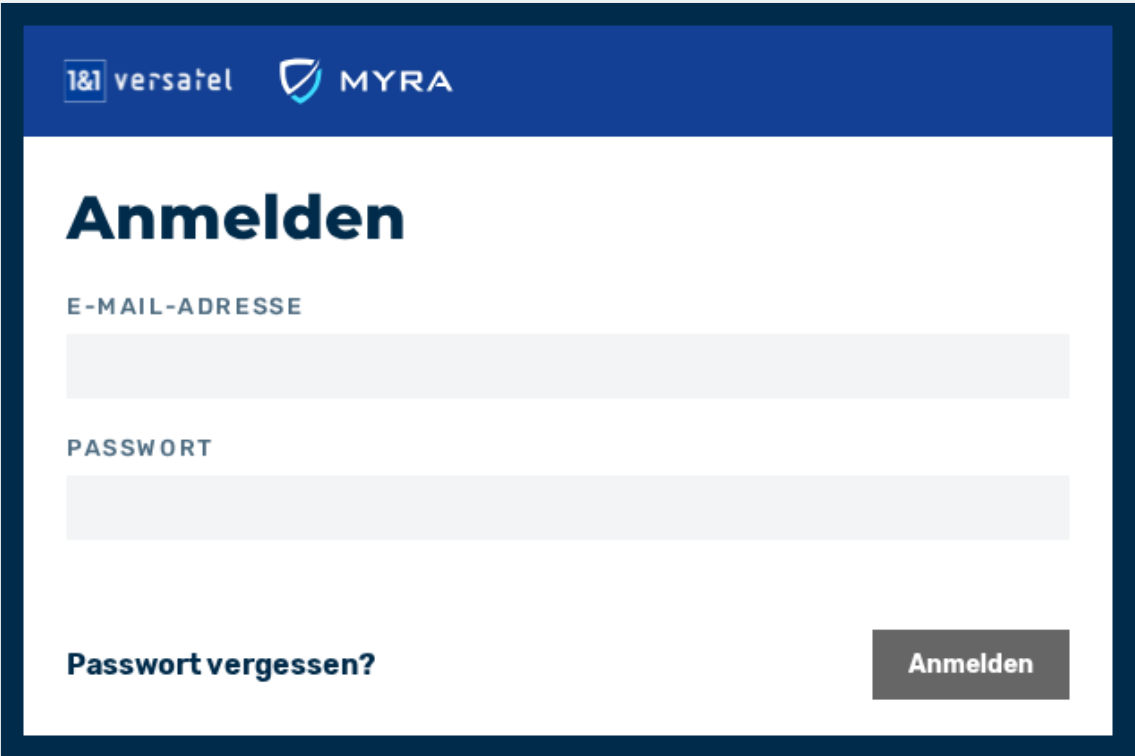


Abbildung 3: Dialog Anmelden

- ▶ Klicken Sie auf die Schaltfläche **Anmelden**.

The screenshot shows a login dialog for MYRA. At the top, there is a dark blue header bar with the '1&1 versatel' logo on the left and the 'MYRA' logo on the right. Below the header, the title 'Zwei-Faktor-Authentifizierung (2FA)' is displayed in a large, bold, black font. Underneath the title, a paragraph of text reads: 'Bitte geben Sie den von Ihrer Authentifizierungsanwendung generierten Verifizierungscode ein. Wenn Sie keinen Zugriff auf Ihre Authentifizierungsanwendung haben, können Sie einen Ihrer Backup-Codes verwenden.' Below this text is a label 'VERIFIZIERUNGSCODE' followed by a wide, light gray rectangular input field. In the bottom right corner of the dialog, there is a dark gray button with the white text 'Anmeldung verifizieren'.

Abbildung 4: Dialog Zwei-Faktor-Authentifizierung (2FA) - Anmeldung

- ▶ Geben Sie Ihren 2FA-Code ein.
- ▶ Klicken Sie auf die Schaltfläche **Anmeldung verifizieren**.
- Die Startseite **Unternehmenskonten** öffnet sich.



Die Zwei-Faktor-Authentifizierung (2FA) ist nur verfügbar, wenn diese vorher im Konto aktiviert wurde. Weitere Informationen finden Sie unter [Zwei-Faktor-Authentifizierung aktivieren](#).

1.3 DataHub-Portal

1.3.1 Übersicht Myra DataHub-Portal

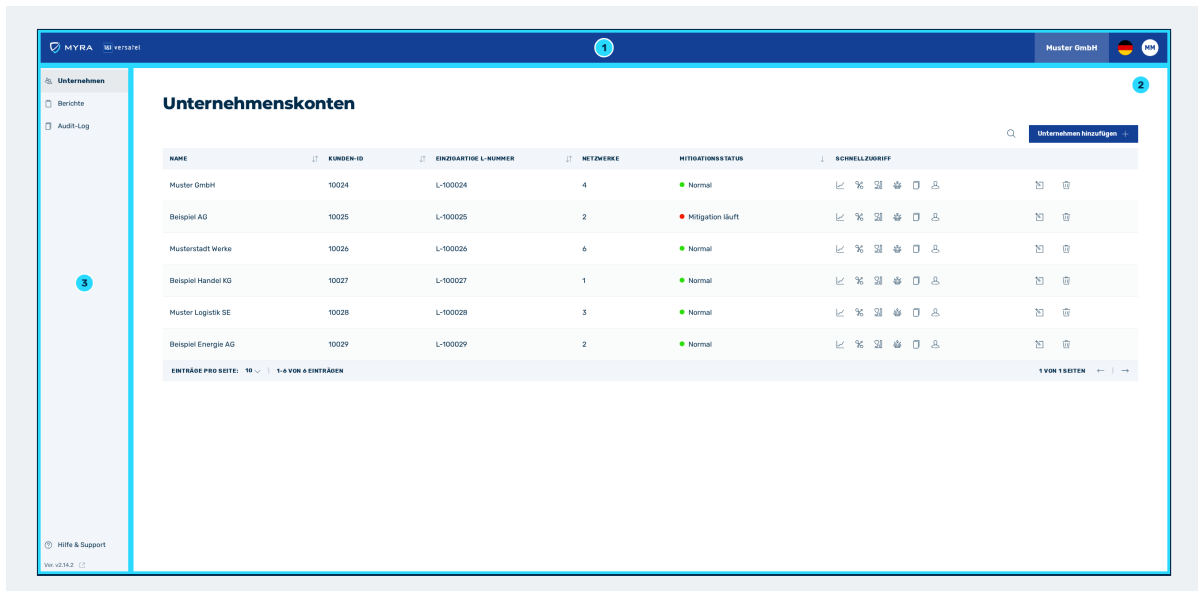


Abbildung 5: Übersicht Startseite

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

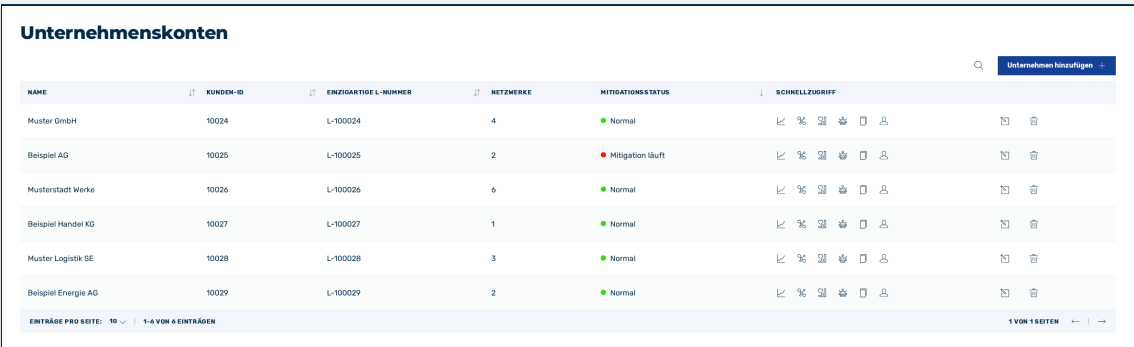
Auf der Startseite können Sie die folgenden Informationen finden:

- Obere Menüleiste mit Zugriff auf die folgenden Schaltflächen (1):
 - Schaltfläche mit dem Namen des Unternehmens für den Zugriff auf die Benutzerverwaltung
 - Schaltfläche mit Flaggsymbol 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
- Hilfe & Support zum Öffnen der Online-Hilfe
- Anzeige der aktuellen Versionsnummer mit Symbol  zum Öffnen der Ansicht **Changelog**

1.3.1.1 Ansicht Unternehmenskonten



NAME	KUNDEN-ID	ENZIGARTIGE L-NUMMER	NETZWERKE	MITIGATIONSSTATUS	SCHNELLZUGRIFF
Muster GmbH	10024	L-100024	4	Normal	   
Beispiel AG	10025	L-100025	2	Mitigation läuft	   
Musterstadt Werke	10026	L-100026	6	Normal	   
Beispiel Handel KG	10027	L-100027	1	Normal	   
Muster Logistik SE	10028	L-100028	3	Normal	   
Beispiel Energie AG	10029	L-100029	2	Normal	   

Abbildung 6: 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 neue Unternehmen hinzufügen sowie vorhandene Unternehmen verwalten und ändern.

Folgende Informationen werden Ihnen in einer Tabelle angezeigt:

Element	Beschreibung
Name	Der Name des Kunden.
Kunden-ID	Die individuelle ID des Kunden.
Einzigartige L-Nummer	Die eindeutige Kundennummer für die Internetleitung über die die Kunden bei Versatel angebunden werden.
Netzwerke	Die eingetragenen IP-Adressen des Kunden.

Element	Beschreibung
Mitigationsstatus	Der Mitigationsstatus für das entsprechende Unternehmen. Mitigation läuft : Eine oder mehrere Mitigationen wurden gestartet. 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.
Unternehmen hinzufügen	Die Schaltfläche Unternehmen hinzufügen öffnet den Dialog Neues Unternehmen hinzufügen, über den Sie neue Unternehmen hinzufügen können.  Um ein Unternehmen hinzuzufügen, zu ändern oder zu löschen, benötigen Sie SOC-Administrationsrechte.
	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 .

Element	Beschreibung
	Das Symbol öffnet die Ansicht Benutzerverwaltung des jeweiligen Unternehmens. Hier können die Einstellungen für Konten eingesehen und geändert werden.
	Das Symbol öffnet den Dialog Unternehmen bearbeiten zur Bearbeitung des Namens und der Kunden-ID. Siehe <u>Unternehmen ändern</u>. Um ein Unternehmen hinzuzufügen, zu ändern oder zu löschen, benötigen Sie SOC-Administrationsrechte.
	Das Symbol öffnet den Dialog Unternehmen löschen zum Löschen des Kundenkontos. Um ein Unternehmen hinzuzufügen, zu ändern oder zu löschen, 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. Sie befinden sich im SOC-Modus für: Muster GmbH Zurück zur Übersicht

1.3.1.1.1 Unternehmen ändern



Um ein Unternehmen hinzuzufügen, zu ändern oder zu löschen, benötigen Sie SOC-Administrationsrechte.

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



Abbildung 7: Schaltfläche zum Bearbeiten eines Unternehmens

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

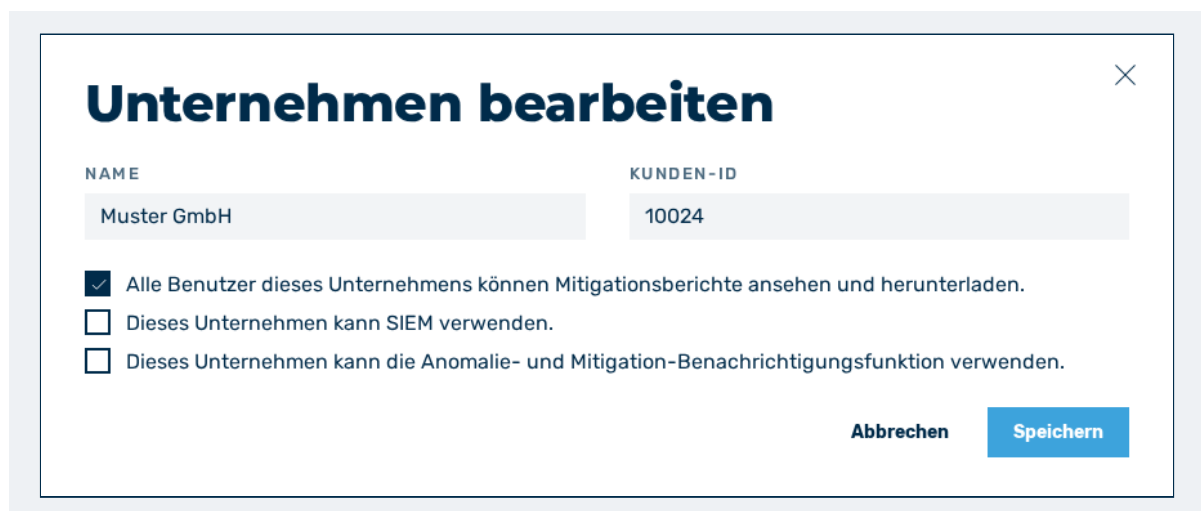


Abbildung 8: Dialog Unternehmen bearbeiten

- Geben Sie ins Feld unter **Name** den neuen Namen des Unternehmens ein.
- Geben Sie ins Feld unter **Kunden-ID** die neue ID 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 Paketrage (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 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.

Berichte	
NAME	BERICHT
Monatlicher Mitigationsbericht - Mai 2026	
Monatlicher Mitigationsbericht - April 2026	
Monatlicher Mitigationsbericht - März 2026	
Monatlicher Mitigationsbericht - Februar 2026	
Monatlicher Mitigationsbericht - Januar 2026	
Monatlicher Mitigationsbericht - Dezember 2025	
Monatlicher Mitigationsbericht - November 2025	
Monatlicher Mitigationsbericht - Oktober 2025	
Monatlicher Mitigationsbericht - September 2025	
Monatlicher Mitigationsbericht - August 2025	
EINTRÄGE PRO SEITE: 10 1-10 VON 16 EINTRÄGEN 1 VON 2 SEITEN	

Abbildung 9: 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

Monatlicher Mitigationsbericht												
NAME	NETZWERK	STARTDATUM	BEENDET	RAUSGEHTEN-SCHWELLENWERT (BYTES)	RAUSGEHTEN-SCHWELLENWERT (PACKETS)	HAUPTLICHE RAUSGEHTEN-SCHWELLENWERT (BYTES)	HAUPTLICHE RAUSGEHTEN-SCHWELLENWERT (PACKETS)	DATENVOLUMEN (BYTES)	PACKETS UMSATZ	VERKÜRZTE BITS (BYTES)	VERKÜRZTE PACKETS	AUSLÖSER-TYP
Muster GmbH	XXX.XXX.XXX.XXX/24	02.05.2020 11:04	02.05.2020 11:52	4.000 / 3.884	500.000 / 486.210	8.412	912.880	24.180.540	2.104.882.311	6.204.118	584.309.772	Automatisch
Muster GmbH	XXX.XXX.XXX.XXX/24	07.05.2020 03:18	07.05.2020 04:06	4.000 / 3.912	500.000 / 491.075	6.037	784.219	17.902.114	1.685.401.905	3.918.446	402.771.038	Automatisch
Muster GmbH	XXX.XXX.XXX.XXX/24	14.05.2020 20:41	14.05.2020 21:12	4.000 / 4.000	500.000 / 500.000	5.219	612.714	9.844.702	1.032.556.760	1.204.877	118.640.215	Manuell
Muster GmbH	XXXXXXX.XXX.XXX/48	21.05.2020 08:55	21.05.2020 09:47	10.000 / 9.740	800.000 / 782.640	12.804	1.204.311	38.412.907	3.518.229.664	11.882.503	1.096.884.310	Automatisch
Muster GmbH	XXX.XXX.XXX.XXX/24	28.05.2020 16:12	28.05.2020 16:58	4.000 / 4.000	500.000 / 500.000	4.740	528.905	10.288.415	1.147.330.038	902.715	94.336.507	Manuell
EINTRÄGE PRO SEITE: 10 1-5 VON 5 EINTRÄGEN												
1 VON 1 SEITE												

Abbildung 10: 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.

Element	Beschreibung
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 Paketrage (Pakete/s)	Die höchste Anzahl an Paketen pro Sekunde während der Mitigation.
Datenvolumen (MBit)	Die Gesamtauslastung der Bandbreite während der Mitigation.
Pakete gesamt	Die Summe aller Pakete während der Mitigation.
Verworfen Bits (MBit)	Das Datenvolumen, das während der Mitigation verworfen wurde.
Verworfen Pakete	Die Anzahl der Pakete, die während der Mitigation verworfen wurden.
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

Audit-Log

CSV herunterladen

ERSTELLT	UNTERNEHMEN	AUSGEFÜHRT DURCH	EVENT	RESSOURCE	RESSOURCEN-ID	PARAMETER
12.05.2026 09:14:22	Muster GmbH	max.mustermann@example.com	UPDATED	Netzwerk	XXXXXXXXXX/24	bw_limit: 4000
12.05.2026 09:02:47	Muster GmbH	max.mustermann@example.com	CREATED	Netzwerk	XXXXXXXXXX/24	pps_limit: 500000
11.05.2026 17:36:05	Beispiel AG	erika.musterfrau@example.com	UPDATED	Benutzer	erika.musterfrau@example.com	role: user
11.05.2026 16:20:31	Beispiel AG	erika.musterfrau@example.com	CREATED	Benutzer	jan.beispiel@example.com	role: admin
11.05.2026 14:58:12	Musterstadt Werke	jan.beispiel@example.com	DELETED	Netzwerk	XXXXXXXXXX/48	-
11.05.2026 11:41:09	Musterstadt Werke	jan.beispiel@example.com	UPDATED	Netzwerk	XXXXXXXXXX/24	type: ACTION_BLACKHOLE
10.05.2026 18:07:53	Beispiel Handel KG	lena.sommer@example.com	CREATED	Unternehmen	10027	name: Beispiel Handel KG
10.05.2026 15:22:40	Muster Logistik SE	tobias.winter@example.com	UPDATED	Netzwerk	XXXXXXXXXX/24	duration: 14400
10.05.2026 12:15:18	Muster Logistik SE	tobias.winter@example.com	DELETED	Benutzer	lena.sommer@example.com	-
09.05.2026 08:49:02	Beispiel Energie AG	max.mustermann@example.com	CREATED	Netzwerk	XXXXXXXXXX/24	nettype: RIPE [P]

EINTRÄGE PRO SEITE: 10

1-10 VON 37 EINTRÄGEN

1 VON 4 SEITEN

Abbildung 11: 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.
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 Website des Myra DataHub.
- ▶ Loggen Sie sich ein.
 - ↳ Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.
- ▶ Klicken Sie auf den Namen des gewünschten Unternehmens.
- Die Startseite des Myra DataHub mit den Unternehmenskonten öffnet sich.

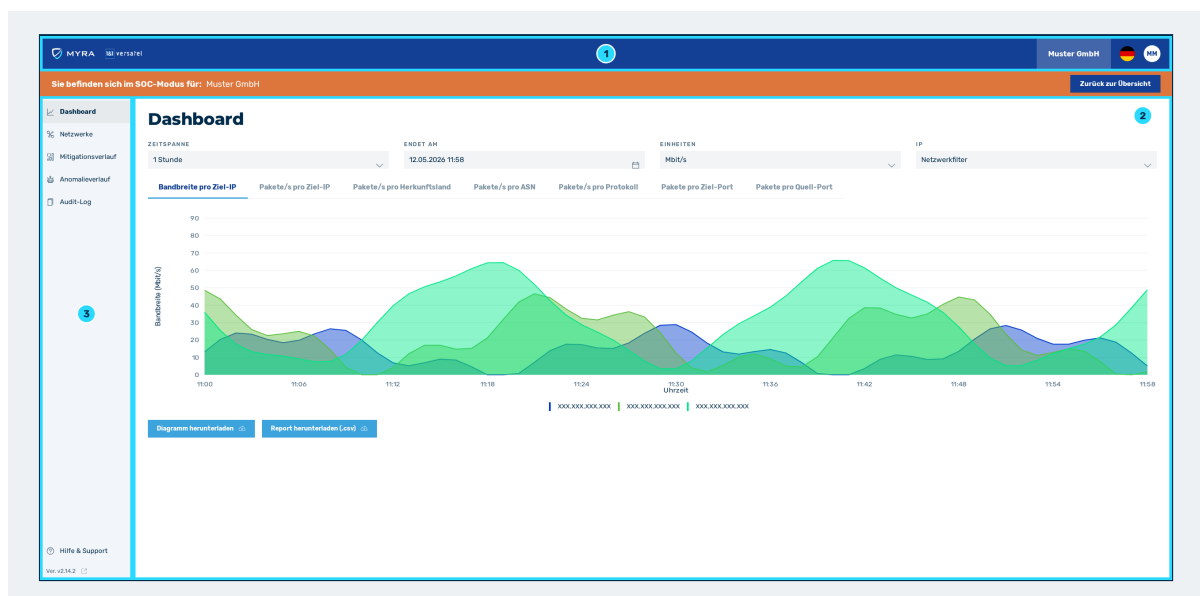


Abbildung 12: Startseite für Unternehmen

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 Nutzens 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
 -  Audit-Log
 - 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.

Sie befinden sich im SOC-Modus für: Muster GmbH

Zurück zur Übersicht

1.3.2.1 Ansicht Dashboard



Abbildung 13: 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 Herkunftsland	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde, aufgeschlüsselt nach Herkunftsland, an. Die Herkunftsländer der Pakete werden dabei mit Ihrem internationalen Ländercode angegeben, z. B. DE für Deutschland oder GB für Großbritannien.
Pakete /s pro ASN	Dieses Diagramm zeigt, wie viele Pakete pro Sekunde von einer bestimmten Quell-ASN (Autonomous System Number) empfangen wurden. In der Legende unterhalb des Diagramms finden Sie die zugehörigen Namen der ASNs.
Pakete /s pro	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde, gruppiert nach dem Übertragungsprotokoll, an. In der Legende unterhalb

Element	Beschreibung
Protokoll	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.
Legendenfiter	Zusätzlich zu den Filtern oberhalb der Diagramme gibt es Diagrammspezifische 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 Herkunftsland: Pakete/s pro Herkunftsland ASN: Pakete/s pro ASN Protokoll: Pakete/s pro Protokoll Port: Pakete pro Ziel-Port und Pakete pro Quell-Port



Abbildung 14: 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.

Element	Beschreibung
	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.

NAME	IP-ADRESSE	BANDBREITEN-SCHWELLENWERT (MBit/s)	PAKETRATEN-SCHWELLENWERT (PAKETE/s)	STATUS DER AUTOMATISCHEN MITIGATION	STATUS DER MANUELLEN MITIGATION	MANUELLE MITIGATION STARTEN
Network 1	XXX.XXX.XXX.XXX/24	4000	500000	Normal	Mitigation läuft	Mitigation beenden
Network 2	XXX.XXX.XXX.XXX/24	4000	500000	Deaktiviert	Normal	Mitigation starten
Network 3	XXX.XXX.XXX.XXX/48	10000	800000	Normal	Normal	Mitigation starten

EINTRÄGE PRO SEITE: 10 | 1-3 VON 3 EINTRÄGEN | 1 VON 1 SEITE

Abbildung 15: 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.
Paketraten-Schwellenwert (Pakete/s)	Die maximal erlaubte Anzahl von Paketen pro Sekunde, die für das Netzwerk erlaubt sind.

Element	Beschreibung
	 Wenn der Schalter für den Netzwerkschutz unter Automatische Aktionen deaktiviert ist, erscheinen alle vor der Deaktivierung definierten Werte ausgegraut.
Status der automatisch en Mitigation	Zeigt den Status der Mitigation an: Deaktiviert : Die automatische Mitigation ist deaktiviert. Mitigation läuft : Eine Mitigation wurde gestartet. Teilweise mitigiert : Eine Mitigation läuft nur für einen Teil des Netzwerkes.  Sie können die aktuell mitigierte IP-Adressen einsehen, indem Sie den Mauszeiger über den Statusindikator bewegen. Normal : Die Mitigation wurde beendet.
Status der manuellen Mitigation	Zeigt den Status der manuellen Mitigation an: Mitigation läuft : Eine manuelle Mitigation wurde gestartet. Teilweise mitigiert : Eine manuelle Mitigation läuft nur für einen Teil des Netzwerkes. 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 Paketrage.
	Das Symbol ermöglicht die Sortierung einzelner Spalten.
Netzwerk hinzufügen	Die Schaltfläche öffnet den Dialog Neues Netzwerk hinzufügen zum Hinzufügen eines neuen Netzwerkes.

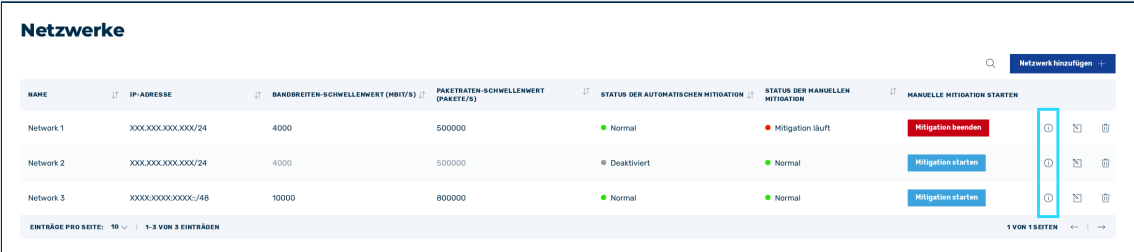
Element	Beschreibung
	Das Symbol öffnet den Dialog Informationen über <Netzwerkname> zum Einsehen aller gesetzten Einstellungen des ausgewählten Netzwerkes.
	Das Symbol öffnet den Dialog Netzwerk bearbeiten zum Bearbeiten der Einstellungen des ausgewählten Netzwerkes.
	Das Symbol öffnet den Dialog Netzwerk 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:



NAME	IP-ADRESSE	BANDBREITEN-SCHWELLENWERT (MBIT/S)	PAKETRATEN-SCHWELLENWERT (PAKETE/S)	STATUS DER AUTOMATISCHEN MITIGATION	STATUS DER MANUELLEN MITIGATION	MANUELLE MITIGATION STARTEN	
Network 1	XXX.XXX.XXX.XXX/24	4000	500000	Normal	Mitigation läuft	Mitigation beenden	
Network 2	XXX.XXX.XXX.XXX/24	4000	500000	Deaktiviert	Normal	Mitigation starten	
Network 3	XXX.XXX.XXX.XXX/48	10000	800000	Normal	Normal	Mitigation starten	

EINTRÄGE PRO SEITE: 50 | 1-3 VON 3 EINTRÄGEN

1 VON 1 SEITE

Abbildung 16: Symbol zum Ansehen des Netzwerkes

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

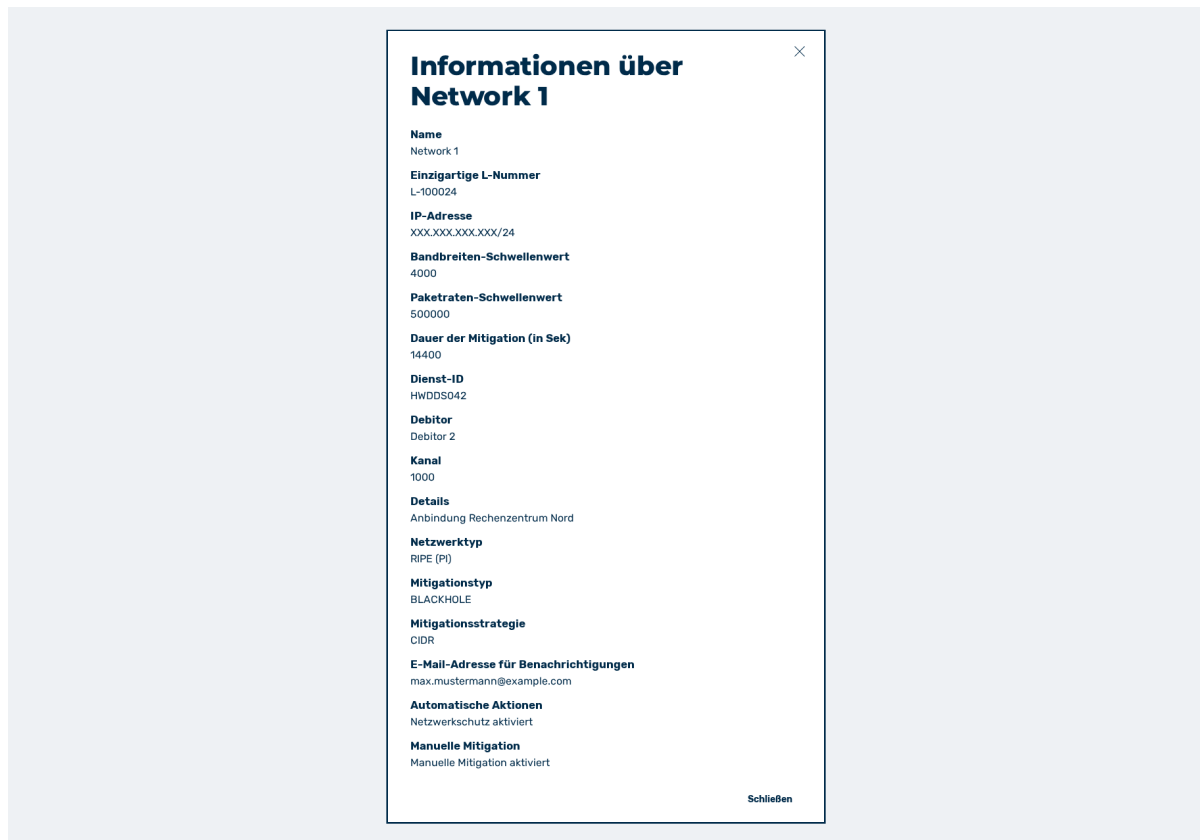


Abbildung 17: Dialog Informationen über Netzwerk

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.
Paketraten-Schwellenwert (Pakete/s)	Der Schwellenwert für die maximale Anzahl der erlaubten Pakete pro Sekunde.
Dienst-ID	Ein Versatel-spezifischer Wert.
Kanal	Ein Versatel-spezifischer Wert.
Netzwerktyp	Der Netzwerktyp für das entsprechende Netzwerk. Die folgenden Werte sind verfügbar: RIPE: Nutzt das Regional Internet Registry for Europe (RIPE) als Netzwerktyp.

Element	Beschreibung
	RIPE (PI): Nutzt den Provider Independent Address Space (PI-Adressraum) als Netzwerktyp. RIPE (LIR): Nutzt das Local Internet Registry (LIR) als Netzwerktyp. RIPE (AS8881): Nutzt das autonome System (AS) von Versatel als Netzwerktyp. SUBNET: Nutzt einen selbstdefinierten IP-Adressbereich als Netzwerktyp.
Einzigartige L-Nummer	Die eindeutige Kundennummer für die Internetleitung, über die die Kunden angebunden werden.
Bandbreiten-Schwellenwert (MBit/s)	Der Schwellenwert für die maximale Höhe der möglichen Bandbreite.
Dauer der Mitigation (in Sek)	Die Dauer der Mitigation in Sekunden, nachdem der Datenverkehr unterhalb der Schwellwerte gefallen ist.
Debitor	Ein Versatel-spezifischer Wert.
Details	Ein individueller Kommentar zur Beschreibung des Netzwerkes.
Mitigationstyp	Die Art und Weise, wie die Mitigation durchgeführt wird. Die folgenden Werte sind verfügbar: BLACKHOLE: Bei Überschreitung des Schwellenwertes wird der komplette Traffic verworfen. ONPREM: Bei Überschreitung des Schwellenwertes wird der Traffic über die internen Server bereinigt. 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.

Element	Beschreibung
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.

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:

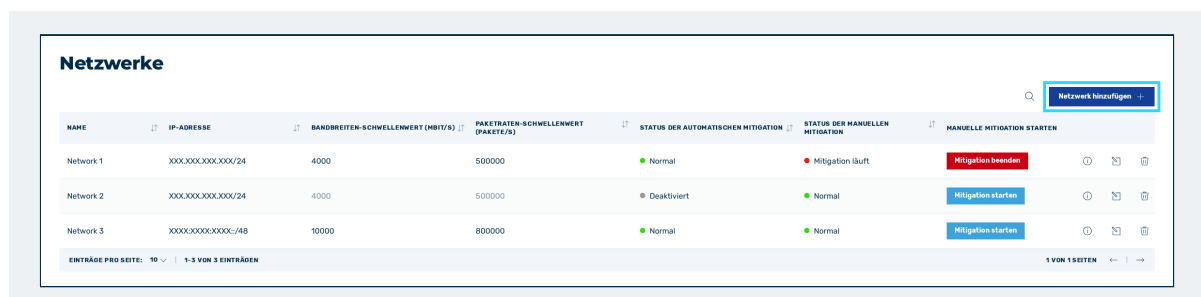


Abbildung 18: Schaltfläche zum Hinzufügen eines Netzwerkes

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

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



Abbildung 19: 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 **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 **Dienst-ID** den entsprechenden Wert ein.
- ▶ Geben Sie ins Feld unter **Kanal** den entsprechenden Wert ein.

- ▶ Wählen Sie in der Drop-down-Liste unter **Netzwerktyp** den entsprechenden Wert aus. Die folgenden Werte sind verfügbar:
 - **RIPE**: Nutzt das Regional Internet Registry for Europe (RIPE) als Netzwerktyp.
 - **RIPE (PI)**: Nutzt den Provider Independent Address Space (PI-Adressraum) als Netzwerktyp.
 - **RIPE (LIR)**: Nutzt das Local Internet Registry (LIR) als Netzwerktyp.
 - **RIPE (AS8881)**: Nutzt das autonome System (AS) von Versatel als Netzwerktyp.
 - **SUBNET**: Nutzt einen selbstdefinierten IP-Adressbereich als Netzwerktyp.
- ▶ 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, geben Sie ins Feld unter **Einzigartige L-Nummer** die eindeutige Kundennummer des Unternehmens 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 **Dauer der Mitigation (in Sek)** die Dauer der Mitigation in Sekunden, nachdem der Datenverkehr unterhalb der Schwellenwerte gefallen ist, an.
- ▶ Falls erforderlich, geben Sie ins Feld unter **Debitor** den entsprechenden Wert ein.
- ▶ Falls erforderlich, geben Sie ins Feld unter **Details** einen individuellen Kommentar zur Beschreibung des Netzwerkes ein.
- ▶ Wählen Sie in der Drop-down-Liste unter **Mitigationstyp** die entsprechende Mitigationsvariante aus. Die folgenden Werte sind verfügbar:
 - ↳ **BLACKHOLE**: Bei Überschreitung des Schwellenwertes wird der komplette Traffic verworfen.
 - ↳ **ONPREM**: Bei Überschreitung des Schwellenwertes wird der Traffic über die internen Server bereinigt.

- ↳ **CLOUD:** Bei Überschreitung des Schwellenwertes wird der Traffic über das Myra-Rechenzentrum bereinigt.
- ▶ 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.

- ▶ 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.

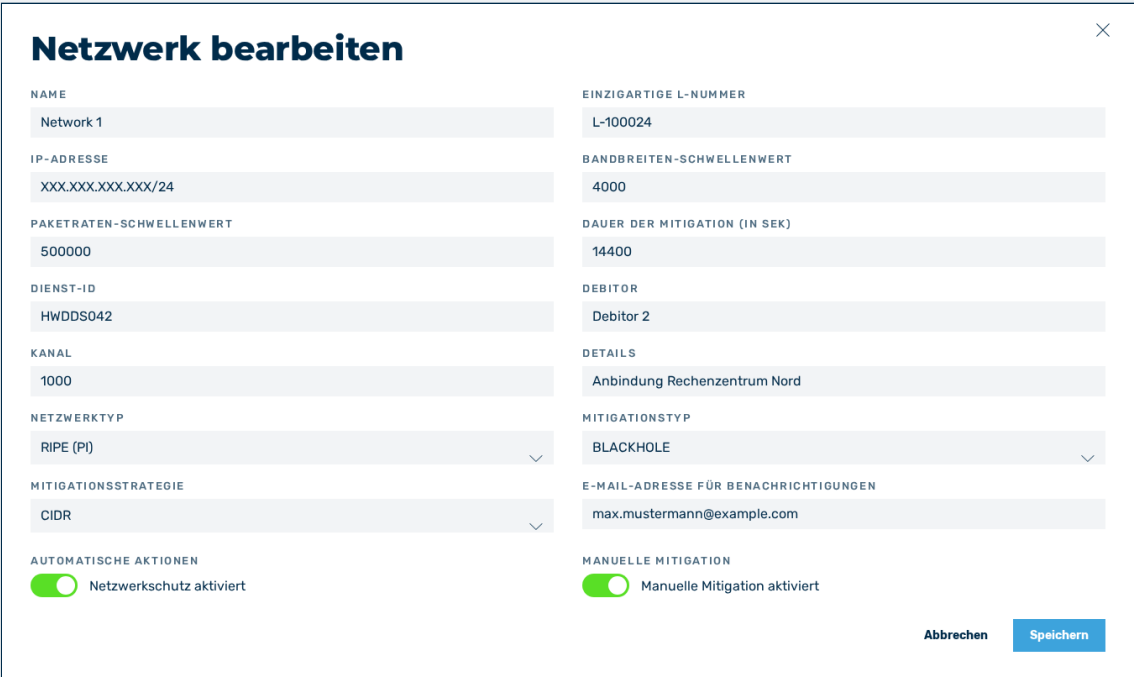
Um ein vorhandenes Netzwerk zu ändern, gehen Sie wie folgt vor:



NAME	IP-ADRESSE	BANDBREITEN-SCHWELLENWERT (MBIT/S)	PAKETRATEN-SCHWELLENWERT (PAKETE/S)	STATUS DER AUTOMATISCHEN MITIGATION	STATUS DER MANUELLEN MITIGATION	MANUELLE MITIGATION STARTEN
Network 1	XXX.XXX.XXX.XXX/24	4000	500000	Normal	Mitigation läuft	Mitigation beenden
Network 2	XXX.XXX.XXX.XXX/24	4000	500000	Deaktiviert	Normal	Mitigation starten
Network 3	XXX.XXX.XXX.XXX/48	10000	800000	Normal	Normal	Mitigation starten

Abbildung 20: Symbol zum Bearbeiten des Netzwerkes

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



Netzwerk bearbeiten

NAME

Network 1

IP-ADRESSE

XXX.XXX.XXX.XXX/24

PAKETRATEN-SCHWELLENWERT

500000

DIENTST-ID

HWDDS042

KANAL

1000

NETZWERKTYP

RIPE (PI)

MITIGATIONSSTRATEGIE

CIDR

AUTOMATISCHE AKTIONEN

☒ Netzwerkschutz aktiviert

EINZIGARTIGE L-NUMMER

L-100024

BANDBREITEN-SCHWELLENWERT

4000

DAUER DER MITIGATION (IN SEK)

14400

DEBITOR

Debitor 2

DETAILS

Anbindung Rechenzentrum Nord

MITIGATIONSTYP

BLACKHOLE

E-MAIL-ADRESSE FÜR BENACHRICHTIGUNGEN

max.mustermann@example.com

MANUELLE MITIGATION

☒ Manuelle Mitigation aktiviert

Abbrechen

Speichern

Abbildung 21: 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:

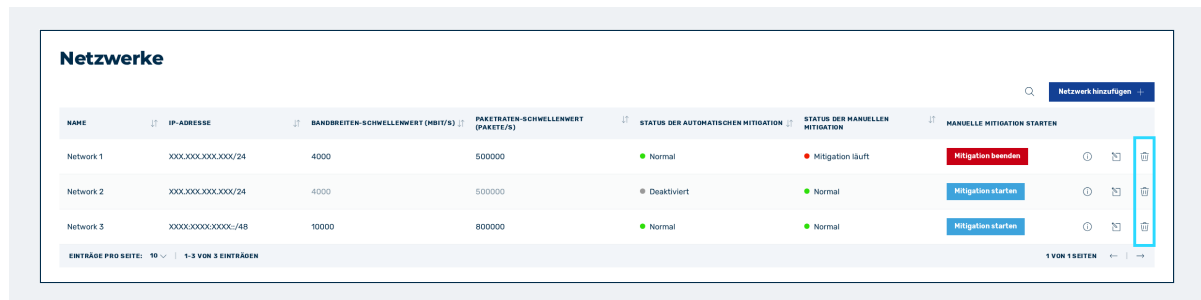


Abbildung 22: Dialog zum Löschen des Netzwerkes

- Klicken Sie auf das Symbol .
- ↳ Die Ansicht **Netzwerk löschen** öffnet sich.

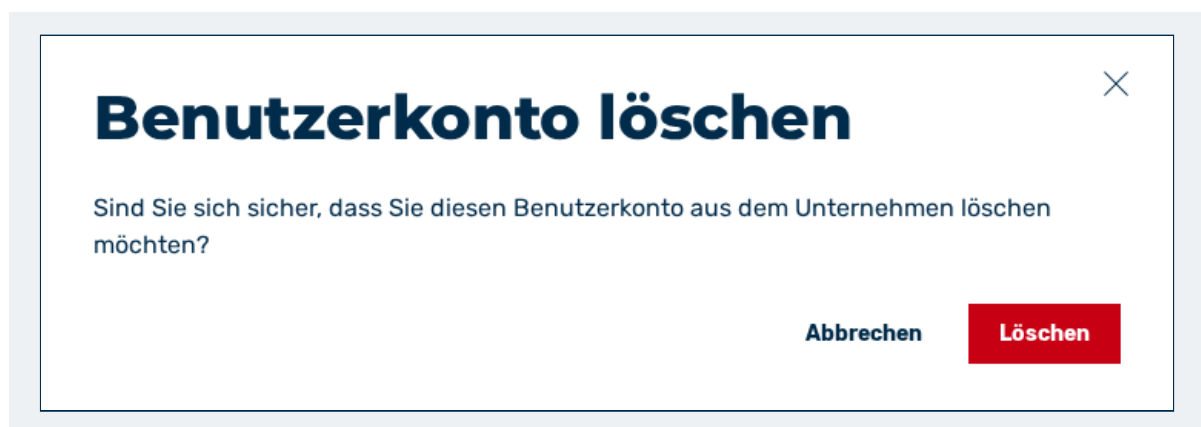


Abbildung 23: Dialog Netzwerk löschen

- 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



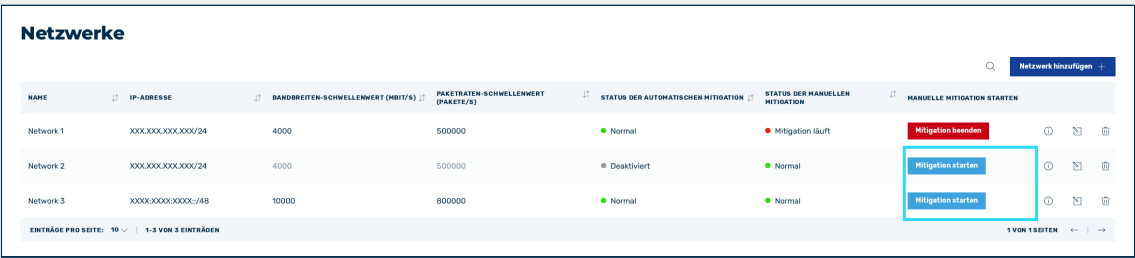
Mitigationen sind für das gesamte Netzwerk oder einzelne bzw. mehrere IP-Adressen möglich.



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:



NAME	IP-ADRESSE	BANDBREITEN-SCHWELLENWERT (MBIT/S)	PAKETRATEN-SCHWELLENWERT (PAKETE/S)	STATUS DER AUTOMATISCHEN MITIGATION	STATUS DER MANUELLEN MITIGATION	MANUELLE MITIGATION STARTEN
Network 1	XXX.XXX.XXX.XXX/24	4000	500000	Normal	Mitigation läuft	Mitigation beenden
Network 2	XXX.XXX.XXX.XXX/24	4000	500000	Deaktiviert	Normal	Mitigation starten
Network 3	XXX.XXX.XXX.XXX/48	10000	800000	Normal	Normal	Mitigation starten

Abbildung 24: Schaltflächen für den Start einer Mitigation

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

- Je nach Art des Netzwerkes wird Ihnen eine von zwei verschiedenen Ansichten angezeigt:



Abbildung 25: Dialog Netzwerk oder IP-Adresse(n) mitigieren– Variante 1

- Bei Netzwerken mit IPv4 mit /32 und IPv6 mit /128 wird Ihnen nur die IP-Adresse des Netzwerkes angezeigt.



Abbildung 26: Dialog Netzwerk oder IP-Adresse(n) mitigieren– Variante 2

- Bei allen anderen Netzwerken können Sie im rechten Feld eine spezifische IP-Adresse eintragen, um die Mitigation nur für die IP-Adresse auszuführen. Über das Symbol  können Sie weitere spezifische IP-Adressen hinzufügen.

Wenn Sie das Feld leer lassen, dann wird die Mitigation für das gesamte Netzwerk gestartet.



Bei Eingabe einer spezifischen IP-Adresse prüft das System automatisch, ob diese IP-Adresse auch zu dem ausgewählten Netzwerk gehört.

- 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
- **Teilweise mitigiert:** Die manuelle Mitigation wurde nur für einen Teil des Netzwerkes gestartet.



Wenn Sie eine Mitigation für eine spezifische IP-Adresse gestartet haben, können Sie den Vorgang auch für weitere IP-Adressen jederzeit wiederholen.

Klicken Sie dazu auf die Schaltfläche **Weitere Mitigation**, um den Dialog für die manuelle Mitigation wieder zu öffnen.



Nach dem erfolgreichen Start einer Migration ändern sich in der Spalte **MANUELLE MITIGATION STARTEN** die Schaltflächen:

- Bei Start einer Mitigation für ein ganzes Netzwerk: Statt der Schaltfläche **Mitigation starten** erscheint die Schaltfläche **Mitigation beenden**.
- Bei Start einer Mitigation für eine spezifische IP-Adresse: Neben der Schaltfläche **Mitigation starten** erscheint eine zusätzliche Schaltfläche **(X) Mitigation(en) beenden**. Wobei das **X** in der Klammer die Anzahl der IP-Adresse anzeigt, für die eine Mitigation eingeleitet wurde.



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 Mitigationssymbol 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 27: 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.

- Prüfen Sie, welcher Fall vorliegt, und gehen Sie dann wie folgt vor:

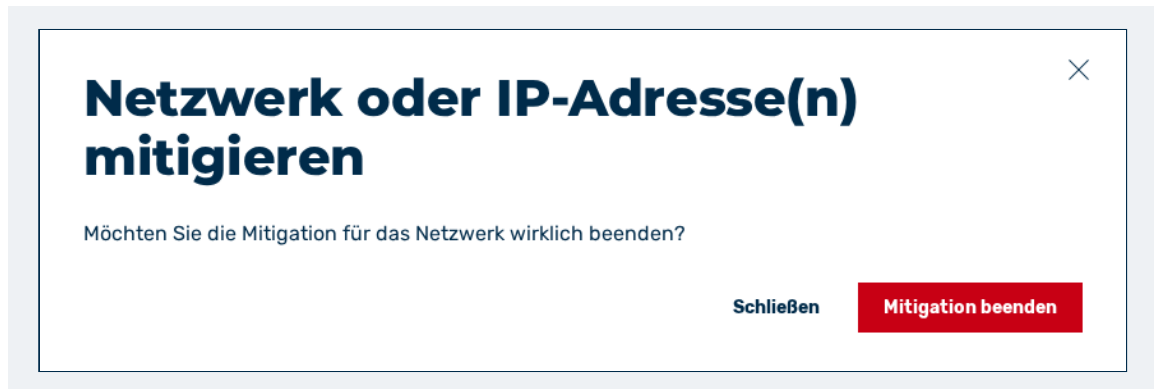


Abbildung 28: Dialog zum Beenden einer Mitigation – gesamtes Netzwerk

- Bei der Mitigation eines ganzen Netzwerkes, klicken Sie auf die Schaltfläche **Mitigation beenden**.



Abbildung 29: Dialog zum Beenden einer Mitigation – einzelne IP-Adressen

- Um die Mitigation für alle IP-Adressen zu beenden, klicken Sie auf die Schaltfläche **Alle Mitigationen beenden**.
- Um die Mitigation für einzelne IP-Adressen zu beenden, klicken Sie jeweils auf die Schaltfläche **Mitigation beenden** neben dem Eintrag und dann auf die Schaltfläche **Schließen**.



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

1.3.2.3 Ansicht Mitigationsverlauf

Mitigationsverlauf								
NETZWERK	GESTARTET	BEENDET	GESTARTET VON	BEENDET VON	BANDBREITEN-SCHWELLENWERT (MBit/s)	PAKETRATEN-SCHWELLENWERT (PAKETE/S)	AUSLÖSERTYP	BERICHT
XXX.XXX.XXX.XXX/24	02.05.2026 11:04	02.05.2026 11:52	Myra	Myra	4.000 / 3.884	500.000 / 486.210	Automatisch	📄
XXX.XXX.XXX.XXX/24	07.05.2026 03:18	07.05.2026 04:06	Myra	Myra	4.000 / 3.912	500.000 / 491.075	Automatisch	📄
XXX.XXX.XXX.XXX/24	14.05.2026 20:41	14.05.2026 21:12	max.mustermann@example.com	max.mustermann@example.com	4.000 / 4.000	500.000 / 500.000	Manuell	📄
XXX.XXX.XXX.XXX/48	21.05.2026 08:55	21.05.2026 09:47	Myra	Myra	10.000 / 9.740	800.000 / 782.640	Automatisch	📄
XXX.XXX.XXX.XXX/24	28.05.2026 16:22	28.05.2026 16:58	erika.musterfrau@example.com	erika.musterfrau@example.com	4.000 / 4.000	500.000 / 500.000	Manuell	📄
EINTRÄGE PRO SEITE: 10 1-5 VON 5 EINTRÄGEN 1 VON 1 SEITEN								

Abbildung 30: 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.

Element	Beschreibung
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	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

Bericht - Network 1 (Muster GmbH)		Bericht herunterladen
DETAILS		
Netzwerk	XXX.XXX.XXX.XXX/24	
Mitigationzeitraum	02.05.2026 11:04 - 02.05.2026 11:52	
Auslösertyp	Automatisch	
BANDBREITE (MBIT/S)		
Konfigurierter Schwellenwert	4.000	
Maximal	8.412	
Gesamt	24.180.560	
Verworfen Bits	19.442.108	
PAKETE (PAKETE/S)		
Konfigurierter Schwellenwert	500.000	
Maximal	912.480	
Gesamt	2.104.882.311	
Verworfen Pakete	1.788.104.225	

Abbildung 31: 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.
Bandbreite – Verworfen Bits	Zeigt die Anzahl der herausgefilterten Bits an.
Pakete – Konfigurierter Schwellenwert	Zeigt den konfigurierten Paketraten-Schwellenwert an, bei dem die automatische Mitigation ausgelöst wird.

Element	Beschreibung
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.
Pakete – Verworfen Pakete	Zeigt die Anzahl der herausgefilterten Pakete 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 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 Herkunftsland	Dieses Diagramm zeigt die Anzahl der empfangenen Pakete pro Sekunde, aufgeschlüsselt nach Herkunftsland, an. Die Herkunftsländer der Pakete werden dabei mit Ihrem internationalen Ländercode angegeben, z. B. DE für Deutschland oder GB für Großbritannien.
Pakete /s pro ASN	Dieses Diagramm zeigt, wie viele Pakete pro Sekunde von einer bestimmten Quell-ASN (Autonomous System Number) empfangen wurden. In der Legende unterhalb des Diagramms finden Sie die zugehörigen Namen der ASNs.

Element	Beschreibung
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.
Legend enfilter	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 Herkunftsland: Pakete/s pro Herkunftsland ASN: Pakete/s pro ASN 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](#)).

Anomalieverlauf						
BEGINN	LETZTE AKTUALISIERUNG	TYP	NETZWERK	STATUS	ENDE	
22.05.2026 14:08	22.05.2026 14:26	Volumetrisch	XXX.XXX.XXX.XXX/24	Offen		①
21.05.2026 08:55	21.05.2026 09:47	Amplifikation	XXXX.XXXX.XXXX/48	Geschlossen	21.05.2026 09:47	①
19.05.2026 22:15	19.05.2026 22:41	Protokoll	XXX.XXX.XXX.XXX/24	Aktualisierung		①
14.05.2026 20:41	14.05.2026 21:12	Volumetrisch	XXX.XXX.XXX.XXX/24	Geschlossen	14.05.2026 21:12	①
07.05.2026 03:18	07.05.2026 04:06	Amplifikation	XXX.XXX.XXX.XXX/24	Geschlossen	07.05.2026 04:06	①
02.05.2026 11:04	02.05.2026 11:52	Volumetrisch	XXX.XXX.XXX.XXX/24	Geschlossen	02.05.2026 11:52	①
EINTRÄGE PRO SEITE: 10 1-6 VON 6 EINTRÄGEN						1 VON 1 SEITEN

Abbildung 32: 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

Anomaliedetails

Beginn
22.05.2026 14:08

Ende
–

Netzwerk
XXX.XXX.XXX.XXX/24

Letzte Aktualisierung
22.05.2026 14:26

Typ
Volumetrisch

Status
Offen

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.

Zusätzliche Informationen

Maximale Bandbreite
8.412 MBit/s

Ziel-IP
XXX.XXX.XXX.XXX

Maximale Paketrate
912.480 Pakete/s

Protokoll
UDP

Schließen

Abbildung 33: 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 Audit-Log

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

Audit-Log						
ERSTELLT	AUSGEFÜHRT DURCH	EVENT	RESSOURCE	RESSOURCEN-ID	PARAMETER	
12.05.2026 09:14:22	max.mustermann@example.com	UPDATED	Netzwerk	XXXXXXX/24	bw_limit: 4000	
12.05.2026 09:02:47	max.mustermann@example.com	CREATED	Netzwerk	XXXXXXX/24	pps_limit: 500000	
11.05.2026 17:36:05	erika.musterfrau@example.com	UPDATED	Benutzer	erika.musterfrau@example.com	role: user	
11.05.2026 16:20:31	erika.musterfrau@example.com	CREATED	Benutzer	jan.beispiel@example.com	role: admin	
11.05.2026 14:58:12	jan.beispiel@example.com	DELETED	Netzwerk	XXXXXXX/48	—	
11.05.2026 11:41:09	jan.beispiel@example.com	UPDATED	Netzwerk	XXXXXXX/24	type: ACTION_BLACKHOLE	
10.05.2026 18:07:53	lena.sommer@example.com	CREATED	Netzwerk	XXXXXXX/24	bw_limit: 1000	
10.05.2026 15:22:40	tobias.winter@example.com	UPDATED	Netzwerk	XXXXXXX/24	duration: 14400	
10.05.2026 12:15:18	tobias.winter@example.com	DELETED	Benutzer	lena.sommer@example.com	—	
09.05.2026 08:49:02	max.mustermann@example.com	CREATED	Netzwerk	XXXXXXX/24	nettype: RIPE (P)	
EINTRÄGE PRO SEITE: 10 1-10 VON 37 EINTRÄGEN 1 VON 4 SEITEN						

Abbildung 34: 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.
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.

Element	Beschreibung
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 35: 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 36: 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

1.3.3.2.1 Konto hinzufügen

Um ein Konto hinzuzufügen, gehen Sie wie folgt vor:

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

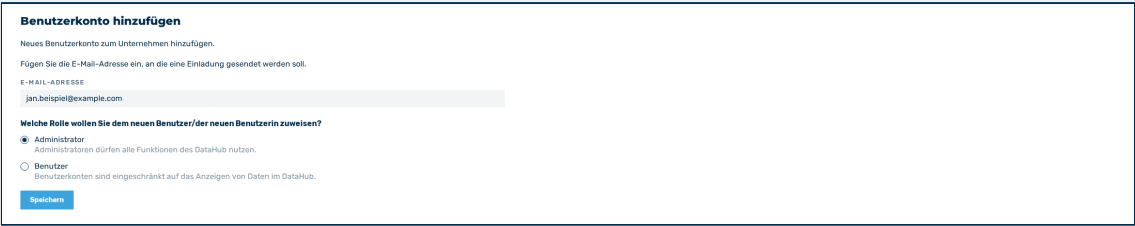


Abbildung 37: Bereich Benutzerkonto hinzufügen

- Geben Sie unter **E-Mail-Adresse** die E-Mail des neuen Nutzenden ein.



Beim Hinzufügen eines neuen Nutzenden wird der Name vor dem @-Symbol als Name des Nutzenden im System hinterlegt.

Der Name kann nachträglich von Nutzenden mit der Rolle **Administrator** (siehe **Konto ändern**) oder von den Nutzenden selbst (siehe **Benutzernamen ändern**) angepasst werden.

- Wählen Sie unter **Welche Rolle wollen Sie dem neuen Benutzer/der neuen Benutzerin zuweisen?** die entsprechende Rechtegruppe aus.

Sie haben zwei Rechtegruppen zur Auswahl:

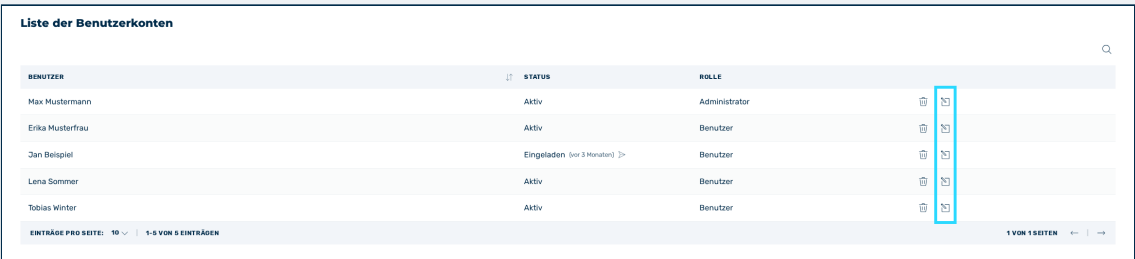
- ↳ **Administrator:** Nutzende mit der Rolle **Administrator** dürfen jede Portalfunktion nutzen.
- ↳ **Benutzer:** Nutzende mit der Rolle **Benutzer** sind eingeschränkt und dürfen nur Daten einsehen.
- Klicken Sie auf die Schaltfläche **Speichern**.
- Eine Meldung bestätigt das erfolgreiche Anlegen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

Neue Nutzende erhalten eine Einladungs-E-Mail mit einem Aktivierungslink.

1.3.3.2.2 Konto ändern

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

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



BENUTZER	STATUS	ROLLE
Max Mustermann	Aktiv	Administrator
Erika Musterfrau	Aktiv	Benutzer
Jan Beispiel	Eingeladen (vor 5 Minuten) >	Benutzer
Lena Sommer	Aktiv	Benutzer
Tobias Winter	Aktiv	Benutzer

EINTRÄGE PRO SEITE: 10 | 1-5 VON 5 EINTRÄGEN

1 VON 1 SEITE

Abbildung 38: Bereich Liste der Benutzerkonten

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

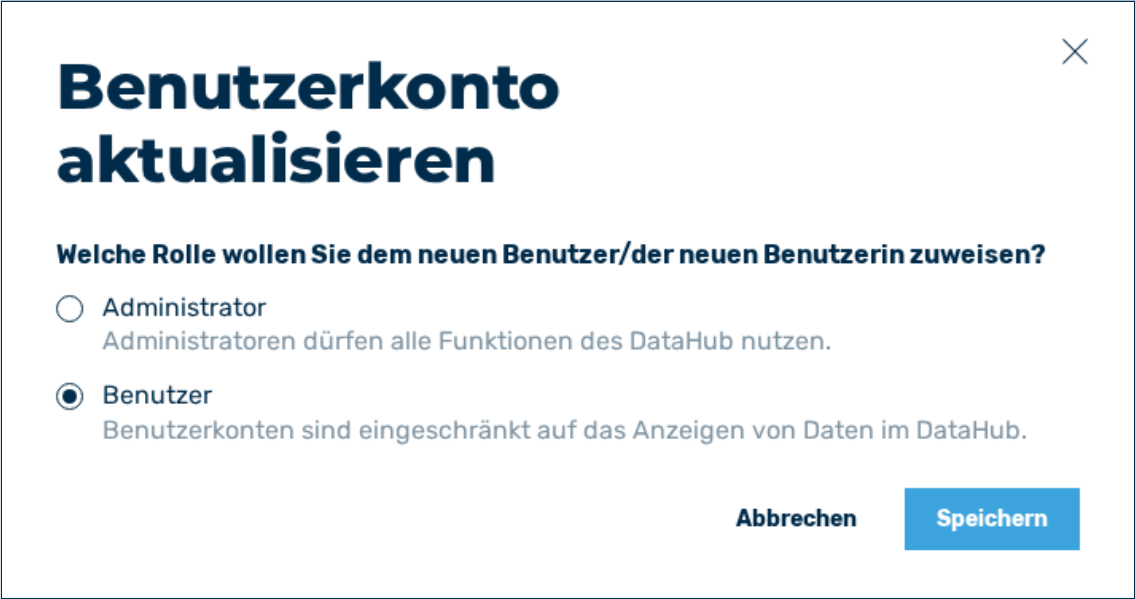


Abbildung 39: Dialog Benutzerkonto aktualisieren

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

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.

1.3.3.2.3 Konto löschen



Das Entfernen eines Kontos ist endgültig und gelöschte Konten können nicht wiederhergestellt werden. Um ein gelöschtes Konto wieder hinzufügen zu können, müssen Sie dieses neu anlegen.



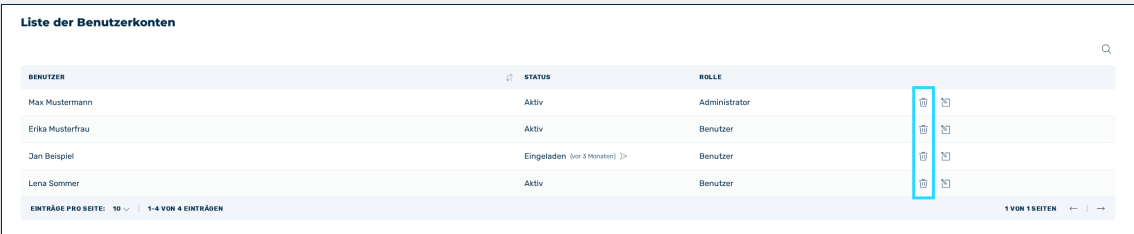
Als SOC-User haben Sie die Rechte für Unternehmen alle Benutzer zu löschen.

Als SOC-Admin können Sie zudem Konten von Nutzenden mit den Rollen **Benutzer** und **Administrator** löschen.

Als SOC-User mit Rolle **Benutzer** können Sie nur die Konten von SOC-User derselben Rolle löschen.

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

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



BENUTZER	STATUS	ROLLE
Max Mustermann	Aktiv	Administrator
Erika Musterfrau	Aktiv	Benutzer
Jan Beispiel	Eingeladen (vor 3 Monaten) >	Benutzer
Lena Sommer	Aktiv	Benutzer

EINTRÄGE PRO SEITE: 10 | 1-4 VON 4 EINTRÄGEN

1 VON 1 SEITE

Abbildung 40: Bereich Liste der Benutzerkonten

- Klicken Sie in der Spalte **Löschen** auf das Symbol .
- ↳ Der Dialog **Benutzerkonto löschen** öffnet sich.

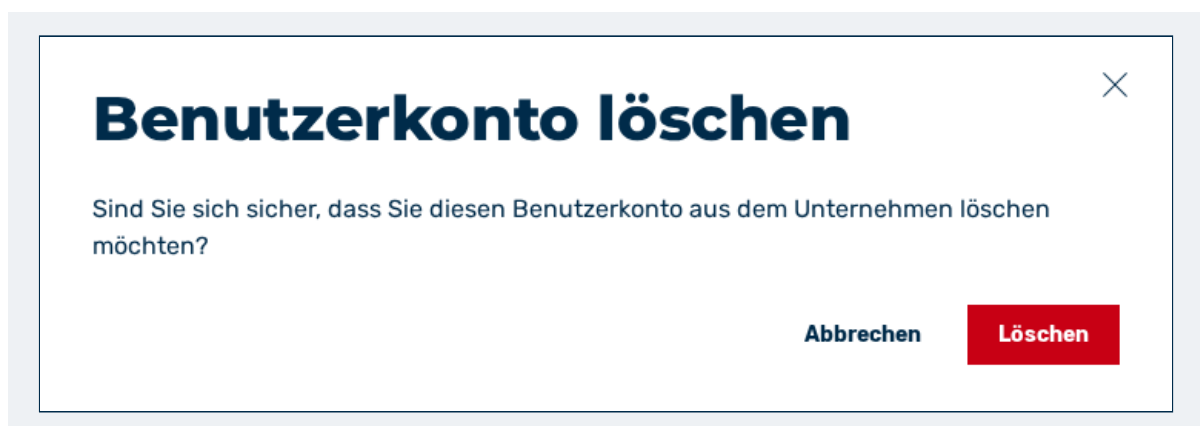


Abbildung 41: Dialog Benutzerkonto löschen

- Klicken Sie auf die Schaltfläche **Entfernen**.
- Eine Meldung bestätigt das Löschen des Kontos. Der Eintrag ist nicht länger in der Liste der Konten sichtbar.

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.

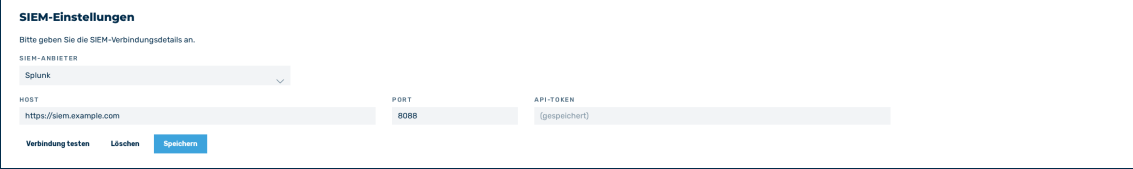


Abbildung 42: Reiter SIEM-Einstellungen

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

Funktion	Event
Mitigation	Netzwerk bearbeiten
	Netzwerk löschen
	Automatische Mitigation gestartet
	Automatische Mitigation beendet
	Manuelle Mitigation starten
Benutzerverwaltung	Manuelle Mitigation beenden
	Konto hinzufügen
	Konto löschen
	E-Mail verifizieren
	Passwort zurücksetzen
	2FA aktivieren und deaktivieren

Die folgenden Informationen werden nicht im SIEM-Log angezeigt:

Funktion	Event
Unternehmen	Unternehmen bearbeiten
	Unternehmen löschen
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



BENUTZER	E-MAIL-ADRESSE	ROLLE	E-MAIL-BENACHRICHTIGUNGEN
Max Mustermann	max.mustermann@example.com	Administrator	✓ Aktiviert
Erika Mustermann	erika.mustermann@example.com	Benutzer	✓ Aktiviert
Jan Beispiel	jan.beispiel@example.com	Benutzer	✗ Deaktiviert
Lena Sommer	lena.sommer@example.com	Benutzer	✓ Aktiviert
Tobias Winter	tobias.winter@example.com	Benutzer	✗ Deaktiviert

Abbildung 43: 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:

Element	Beschreibung
	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



Zusätzliche Kontakte

Fügen Sie Personen, Systeme und gemeinsame Postfächer hinzu, die keine Nutzenden der Anwendung sind, damit diese E-Mail-Benachrichtigungen erhalten.

E-MAIL-ADRESSE
reports@example.com Kontakt hinzufügen

E-MAIL-ADRESSE	STATUS	AKTIONEN
noc@example.com	Bestätigt	
alerts@example.com	Bestätigt	
soc@example.com	Ausstehend	

Abbildung 44: 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.
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.

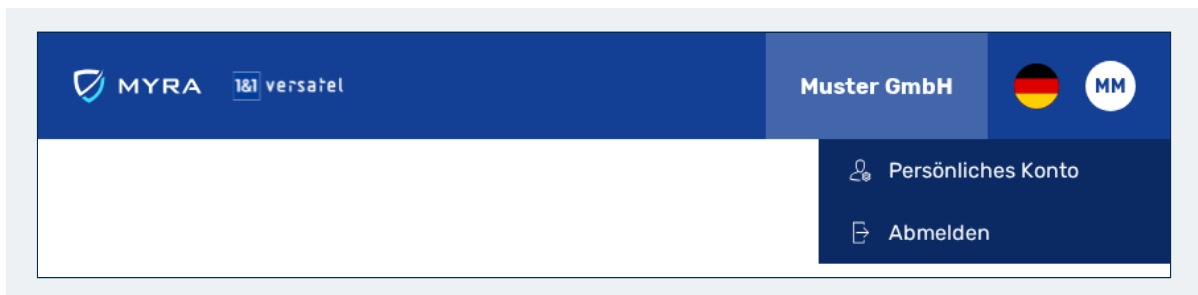


Abbildung 45: Optionen unter dem Profilbild

- ▶ 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
- **Passwort ändern:** Einstellungen zum Setzen eines neuen Passwortes
- **Zwei-Faktor-Authentifizierung (2FA):** Einstellung zur Konfiguration der Zwei-Faktor-Authentifizierung
- **Aktive Sitzungen:** Überblick über alle Sitzungen des Nutzers

1.3.4.1.1 Benutzernamen ändern

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

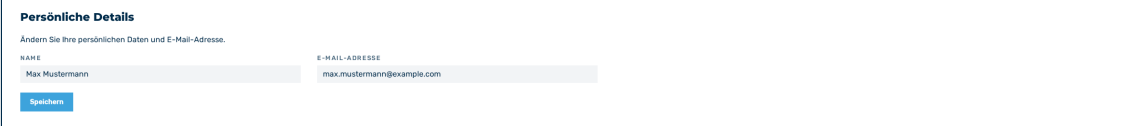


Abbildung 46: Bereich Persönliches Konto

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 Passwort aktualisieren

Im Bereich **Passwort ändern** der Ansicht **Persönliches Konto** können Sie Ihr Passwort ändern.



Abbildung 47: Bereich Passwort ändern

Um Ihr Passwort zu ändern, gehen Sie wie folgt vor:

- ▶ Geben Sie im Textfeld **Aktuelles Passwort** das aktuelle Passwort ein.
- ▶ Geben Sie im Textfeld **Neues Passwort** das neue Passwort ein.
- ▶ Geben Sie im Textfeld **Neues Passwort bestätigen** erneut das neue Passwort ein.
- ▶ Klicken Sie auf die Schaltfläche **Speichern**.
- Eine Meldung bestätigt das erfolgreiche Aktualisieren des Passwortes.

1.3.4.1.3 Zwei-Faktor-Authentifizierung aktivieren



Beim ersten Login auf den Myra DataHub ist die Zwei-Faktor-Authentifizierung noch deaktiviert und muss händisch aktiviert werden.

Im Bereich **Zwei-Faktor-Authentifizierung (2FA)** in der Ansicht **Persönliches Konto** können Sie für Ihr Konto die Zwei-Faktor-Authentifizierung verwalten.

Um die Zwei-Faktor-Authentifizierung zu aktivieren, gehen Sie wie folgt vor:

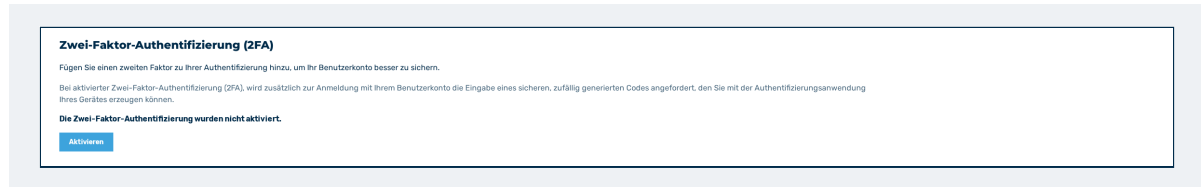


Abbildung 48: Bereich Zwei-Faktor-Authentifizierung (2FA)

- Klicken Sie auf die Schaltfläche **Aktivieren**.
- ↳ Der Dialog **Neues Passwort bestätigen** öffnet sich.



Abbildung 49: Dialog Neues Passwort bestätigen

- Geben Sie ins Feld unter **Passwort** Ihr aktuelles Passwort ein.
- Klicken Sie auf die Schaltfläche **Bestätigen**.
- ↳ Der Dialog **Aktivierung der Zwei-Faktor-Authentifizierung abschließen**, mit einem QR-Code öffnet sich.

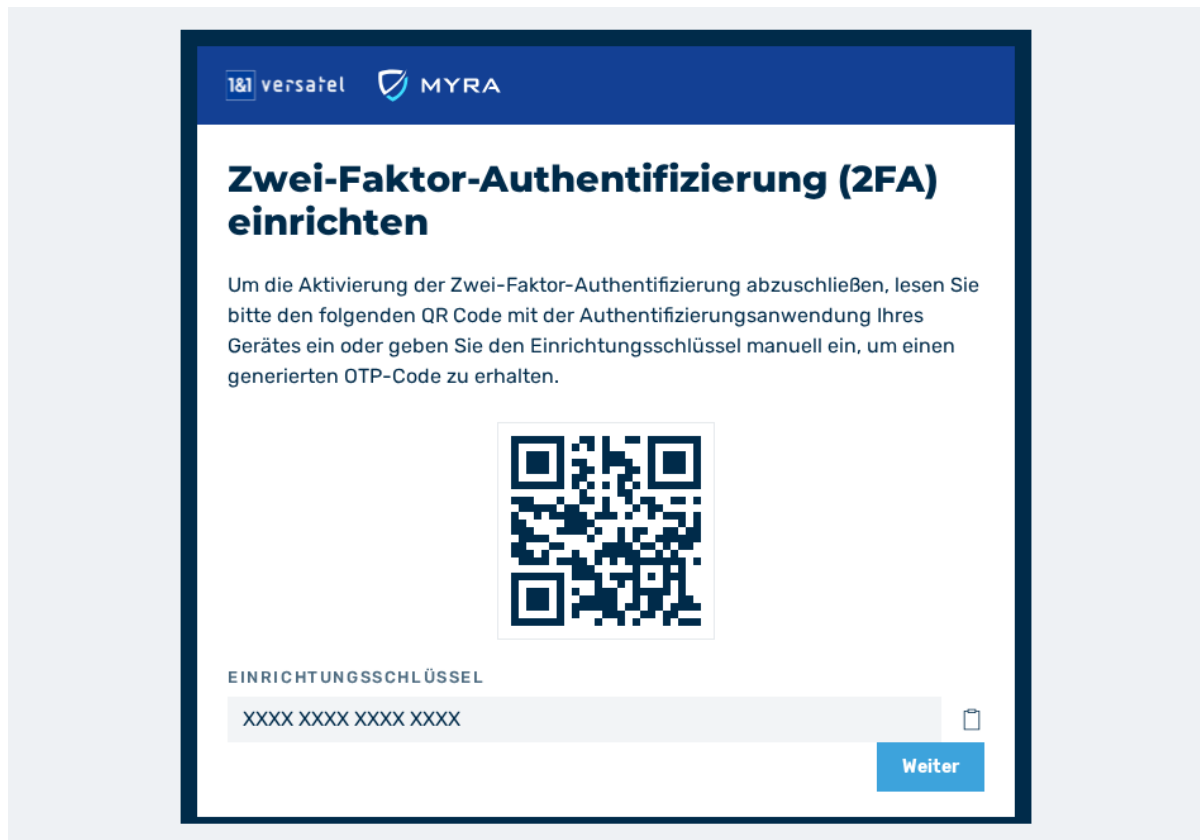


Abbildung 50: Dialog Aktivierung der Zwei-Faktor-Authentifizierung abschließen.

- Scannen Sie den QR-Code mit einem TOTP-fähigen Gerät oder Programm (z. B. Authenticator-Apps). Alternativ können Sie auch den Einrichtungsschlüssel verwenden.
- Klicken Sie auf die Schaltfläche **Weiter**.

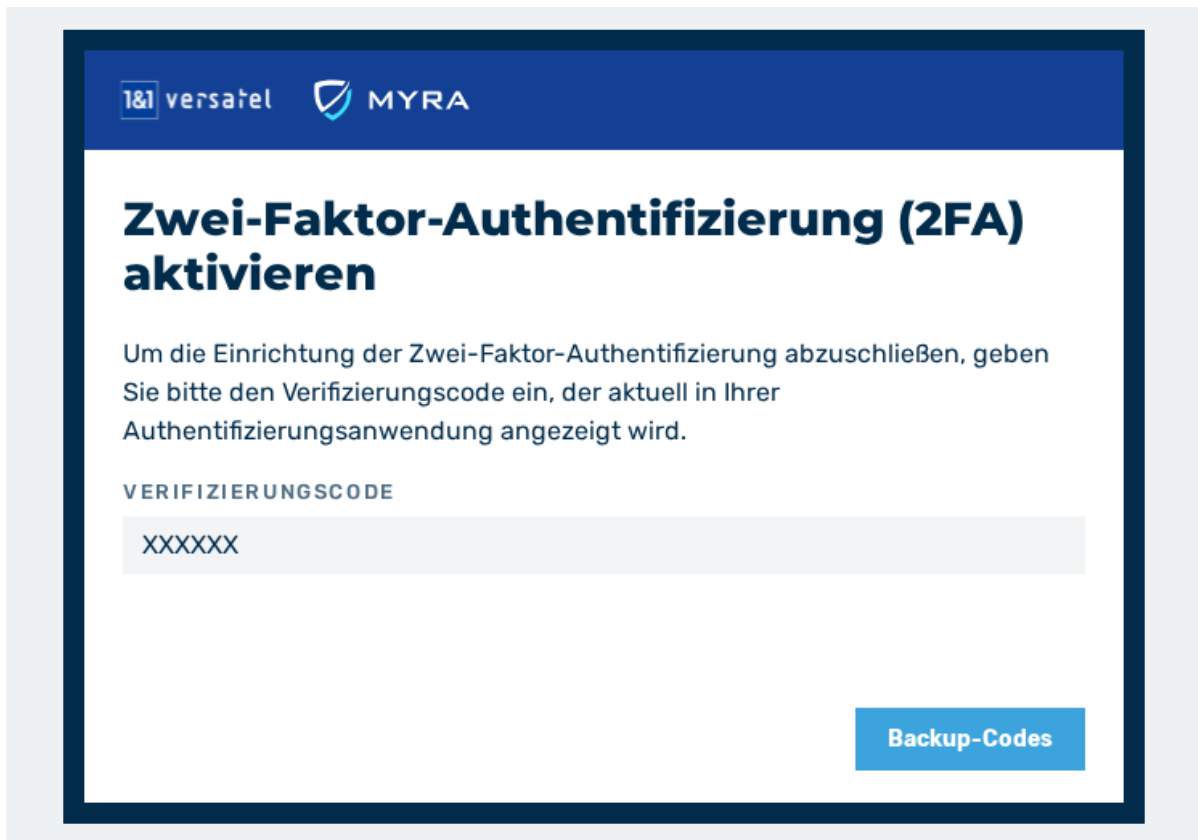


Abbildung 51: Dialog Zwei-Faktor-Authentifizierung (2FA) aktivieren

- Klicken Sie auf die Schaltfläche **Backup-Codes**.
 - ↳ Der Dialog **Backup-Codes** öffnet sich.

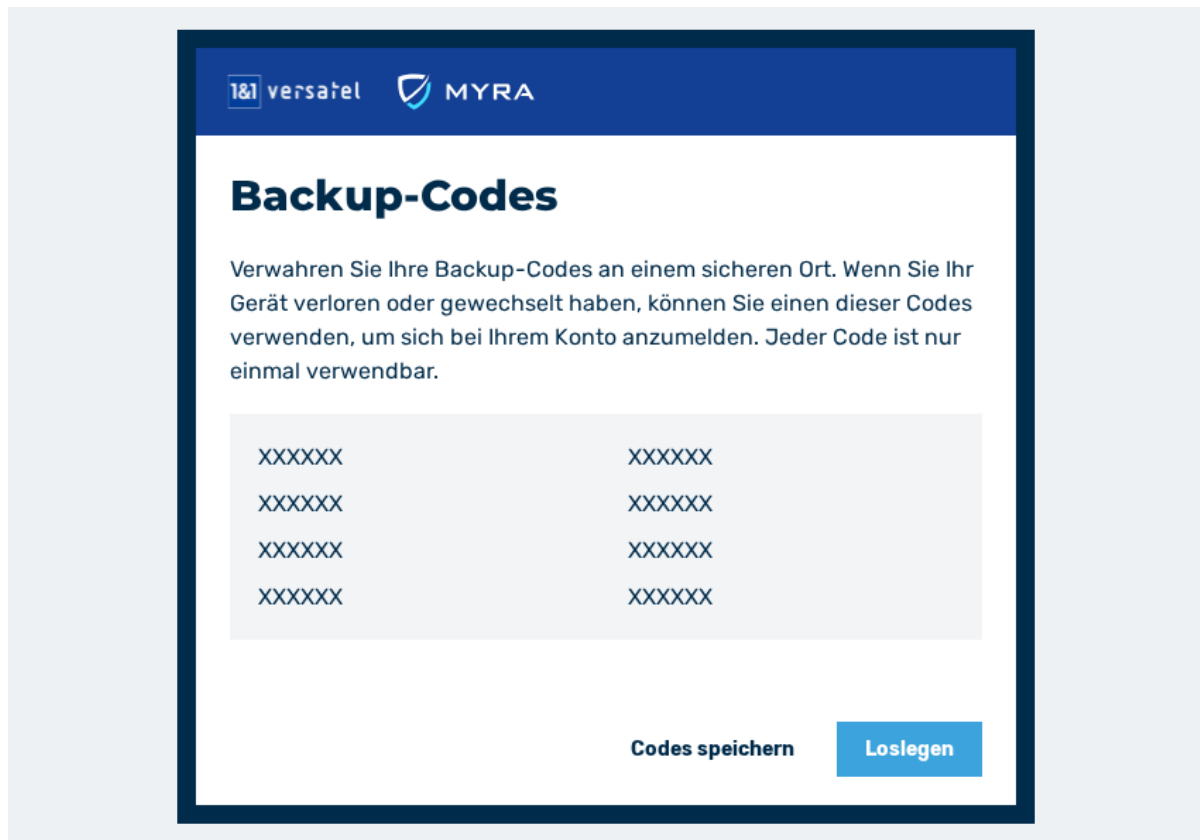


Abbildung 52: Dialog Backup-Codes anzeigen

- ▶ Sie haben zwei Möglichkeiten:
 - Klicken Sie auf das Symbol , um die Backup-Codes in den Zwischenspeicher zu kopieren und diese abzuspeichern.
 - Laden Sie sich eine Backup-Datei herunter.
 - ▷ Geben Sie ins Feld unter **Verifizierungscode** Ihren 6-stelligen Verifizierungscode ein.
 - ▷ Klicken Sie auf die Schaltfläche **Codes speichern**.
 - Eine HTML-Datei mit den Backup-Codes wird heruntergeladen.
- ▶ Klicken Sie auf das **X** oben rechts, um den Dialog zu schließen.
- Die Zwei-Faktor-Authentifizierung ist eingerichtet.



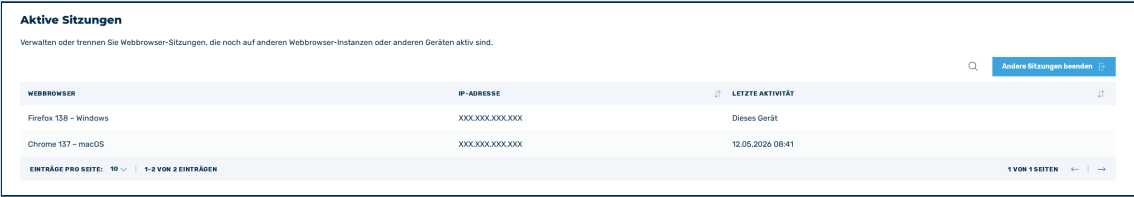
Speichern oder verwahren Sie die Wiederherstellungscodes an einem sicheren Ort. Ohne diese Codes können Sie im Fall des Verlusts Ihres 2FA-Geräts nicht mehr auf Ihr Konto zugreifen.

Sie können jederzeit neue Notfall-Wiederherstellungscodes generieren lassen, indem Sie die Schaltfläche **Neue Codes erzeugen** wählen. Sie erhalten dann acht neue Einmalcodes.

Sollten Sie die 2FA ausschalten wollen, können Sie dies jederzeit über die Schaltfläche **Deaktivieren** im Abschnitt **Zwei-Faktor-Authentifizierung (2FA)** des Profilbereichs tun.

1.3.4.1.4 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.



WEBBROWSER	IP-ADRESSE	LETZTE AKTIVITÄT
Firefox 158 - Windows	XXXXXX.XXX.XXX	Dieses Gerät
Chrome 157 - macOS	XXXXXX.XXX.XXX	12.05.2026 08:41

Abbildung 53: 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](#)).

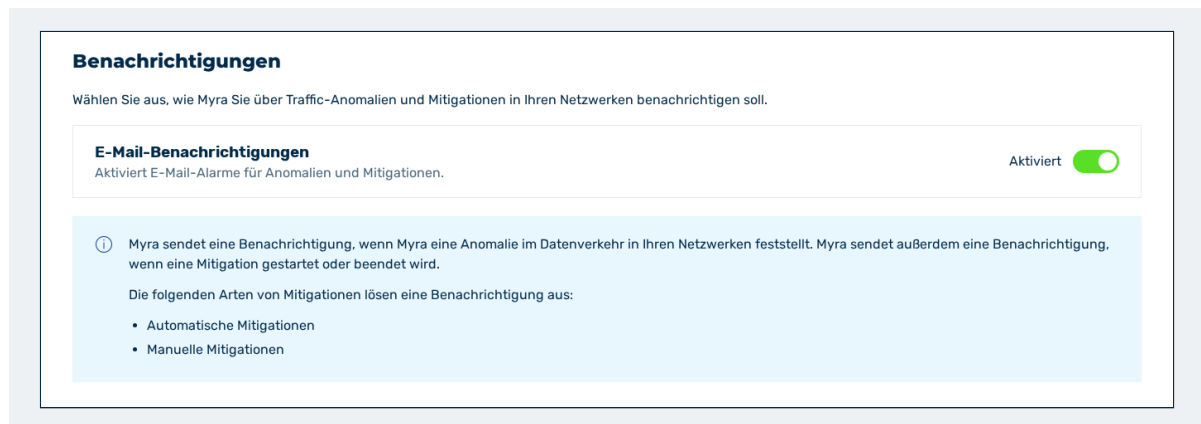


Abbildung 54: Reiter Benachrichtigungen

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.

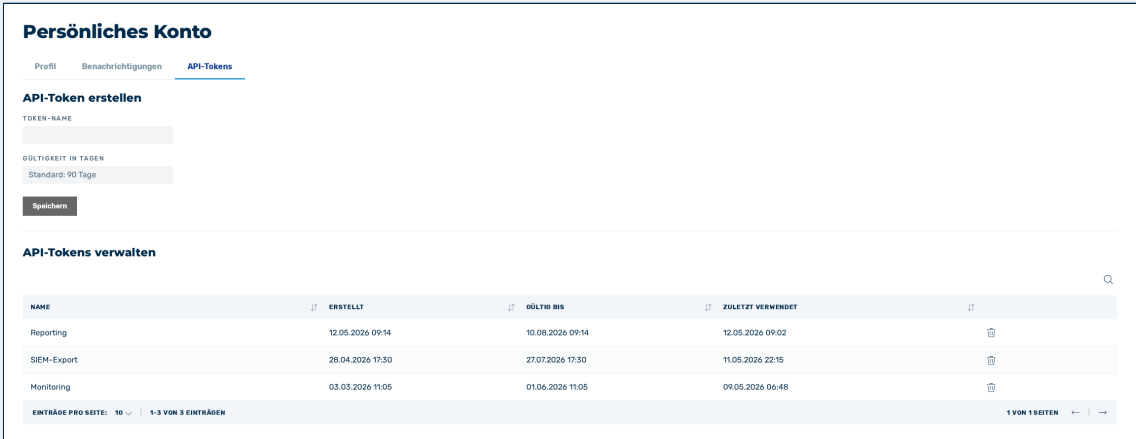
Um die E-Mail-Benachrichtigungen zu aktivieren, gehen Sie wie folgt vor:

- 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



Persönliches Konto

Profil Benachrichtigungen **API-Tokens**

API-Token erstellen

TOKEN-NAMEN

GÜLTIGKEIT IN TAGEN

Standard: 90 Tage

Speichern

API-Tokens verwalten

NAME	ERSTELLT	GÜLTIG BIS	ZULETZT VERWENDET	
Reporting	12.05.2026 09:14	10.08.2026 09:14	12.05.2026 09:02	
SIEM-Export	28.04.2026 17:30	27.07.2026 17:30	11.05.2026 22:15	
Monitoring	03.03.2026 11:05	01.06.2026 11:05	09.05.2026 06:48	

EINTRÄGE PRO SEITE: 10 | 1-3 VON 3 EINTRÄGEN

1 VON 1 SEITEN

Abbildung 55: 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
Unternehmensmanagement	Unternehmen hinzufügen	Nein	Nein	Nein	Ja
	Unternehmen ändern	Nein	Nein	Nein	Ja
	Unternehmen löschen	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

Seiten	Optionen	Unternehmen		SOC	
		User	Admin	User	Admin
	Audit-Log herunterladen	Nein	Nein	Ja	Ja
SOC-Mode	SOC-Mode	Nein	Nein	Ja	Ja
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

Seiten	Optionen	Unternehmen		SOC	
		User	Admin	User	Admin
	Manuelle Mitigation starten/beenden	Nein	Ja	Ja	Ja
	Netzwerk hinzufügen	Nein	Nein	Nein	Ja
	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://versatel.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**.

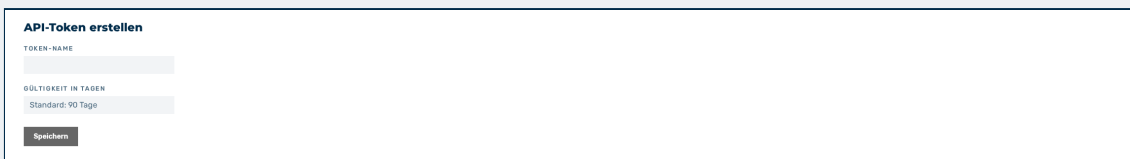


Abbildung 56: Namen und Gültigkeit für den API-Token eingeben

- ▶ 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 57: 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://versatel.myracloud.com/domains/1234`

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



```
-H „Authorization: Bearer MY_API_TOKEN“
```

- 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://versatel.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 <code>id</code> , <code>modified</code> 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

Status code	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 <code>QueryVO</code> wird zurückgegeben, wenn eine Liste von Objekten aus einer GET-Anfrage empfangen wird.
ResultVO	Bei erfolgreichen POST-, PUT- und DELETE-Anfragen wird ein Objekt <code>ResultVO</code> zurückgegeben.
ViolationVO	Bei fehlerhaften Anfragen wird ein Objekt <code>ViolationVO</code> 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 der Swagger-Dokumentation Ihrer Installation unter dem Pfad `/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 `OrganisationV0` 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 `OrganisationV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

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

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,
    "customer_id": "abc",
    "cidrs": "127.0.0.1/32, 10.0.0.0/24",
    "under_mitigation": false,
    "customer_reference": "abc"
  }
],
"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 Nutzers 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 `OrganisationV0` 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 `OrganisationV0` 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
customer_id	Die Kennung der Kundenreferenz.	string
customer_reference	Die gruppierte Kundenreferenz.	string

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,
  "customer_id": "abc",
  "cidrs": "127.0.0.1/32, 10.0.0.0/24",
  "under_mitigation": false,
}
```

```
"customer_reference": "abc"
}
```

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	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 `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 `MitigationV0` 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_BLOCKHOLE ACTION_MITIGATION_PREM ACTION_MITIGATION_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)
Das Erstellungsdatum im ISO-8601-Format.		

Attribut	Beschreibung	Werte
created_at		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)
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)
dropped_bits	Die während der Mitigation verworfenen Bits insgesamt.	integer
dropped_packets	Die während der Mitigation verworfenen Pakete insgesamt.	integer

Attribut	Beschreibung	Werte
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,
      "dropped_bits": 0,
      "dropped_packets": 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 `NetworkV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
<code>id</code>	Die ID des Netzwerks.	<code>string</code>
<code>organisation</code>	Die zugehörige Organisation, referenziert über ID und Name.	<code>object</code>
<code>name</code>	Der Name des Netzwerks.	<code>string</code>
<code>cidr</code>	Der CIDR-Bereich des Netzwerks.	<code>string</code>
<code>enabled</code>	Zeigt an, ob die automatische Mitigation aktiviert ist.	<code>true</code> <code>false</code>

Attribut	Beschreibung	Werte
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
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,
  "mitigation_type": "ACTION_BLACKHOLE",
  "auto_mitigation_strategy": "IP",
  "duration": 0,
  "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	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 `UserV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
id	Die ID der Nutzenden.	string

Attribut	Beschreibung	Werte
name	Der vollständige Name der Nutzenden.	string
email	Die E-Mail-Adresse der Nutzenden.	string
role	Die Rolle der Nutzenden innerhalb der Organisation.	admin editor
status	Der aktuelle Status des Benutzerkontos.	string
invited Since	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
customer_id	Eine eindeutige Kundenreferenz für die 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

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

2.3.1.9.4 Beispiel

Beispiel-Request-Body:

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

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: `OrganisationV0`

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 `OrganisationV0` 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 `OrganisationV0` 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
customer_id	Die Kennung der Kundenreferenz.	string
customer_referen ce	Die gruppierte Kundenreferenz.	string

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
<code>id</code>	Die ID des Nutzenden.	<code>string</code>
<code>modified</code>	Das Datum der letzten Änderung im ISO-8601-Format.	<code>string(\$date-time)</code>

Die folgenden Attribute sind optional:

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

2.3.11.4 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: `OrganisationV0`

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 `OrganisationV0` 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
customer_id	Eine eindeutige Kundenreferenz für die Organisation.	string
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 `OrganisationV0` mit den Informationen zum neuen Eintrag zurück.

2.3.12.4 Beispiel

Beispiel-Request-Body:

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

2.3.12.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.

STATUSCODE	BESCHREIBUNG
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.

2.3.1.13 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: `UserV0`

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 `UserV0` mit den folgenden Attributen definiert werden:

Attribut	Beschreibung	Werte
<code>userEmail</code>	Die E-Mail-Adresse der Nutzenden.	<code>string</code>
<code>userRole</code>	Die Rolle der Nutzenden.	<code>admin</code> <code>editor</code>

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

2.3.14.4 Beispiel

Beispiel-Request-Body:

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

2.3.14.5 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 Nutzens zurückgegeben wird.	string

2.3.15.4 Beispiel

Beispiel-Request-Body:

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

2.3.15.5 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)

2.3.16.4 Beispiel

Beispiel-Request-Body:

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

2.3.16.5 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.

2.3.17 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
mitigation_type	Der Mitigationstyp des Netzwerks.	ACTION_BLACK HOLE ACTION_MITIG ATE_ONPREM ACTION_MITIG ATE_CLOUD
auto_mitigation_strategy	Die Strategie der automatischen Mitigation des Netzwerks.	string
duration	Die Dauer der automatischen Mitigation.	integer
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
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

Attribut	Beschreibung	Werte
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,
      "mitigation_type": "ACTION_BLACKHOLE",
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "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
<code>id</code>	Die ID des Netzwerks.	<code>string</code>
<code>organisation</code>	Die zugehörige Organisation, referenziert durch <code>id</code> und <code>name</code> .	<code>object</code>
<code>name</code>	Der Name des Netzwerks.	<code>string</code>
<code>cidr</code>	Der IP-Bereich des Netzwerks in CIDR-Notation.	<code>string</code>
<code>enabled</code>	Definiert, ob die automatische Mitigation aktiviert ist.	<code>true</code> <code>false</code>
<code>mitigation_type</code>	Die Art der Mitigation, die bei Überschreitung der Schwellenwerte angewendet wird.	<code>ACTION_BLACK_HOLE</code> <code>ACTION_MITIGATE_ONPREM</code> <code>ACTION_MITIGATE_CLOUD</code>
<code>auto_mitigation_strategy</code>	Die Strategie für die automatische Mitigation.	<code>string</code>
<code>duration</code>	Die Dauer der automatischen Mitigation in Sekunden.	<code>integer</code>
<code>pps_limit</code>	Das konfigurierte PPS-Limit.	<code>integer</code>
<code>bw_limit</code>	Das konfigurierte Bandbreitenlimit.	<code>integer</code>
<code>autoStatus</code>	Zeigt an, ob sich das Netzwerk aktuell in automatischer Mitigation befindet.	<code>true</code> <code>false</code>
<code>manualStatus</code>		<code>true</code>

Attribut	Beschreibung	Werte
	Zeigt an, ob sich das Netzwerk aktuell in manueller Mitigation befindet.	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,
      "mitigation_type": "ACTION_BLACKHOLE",
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "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 `NetworkV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
<code>id</code>	Die ID des Netzwerks.	<code>string</code>
<code>organisation</code>	Die zugehörige Organisation.	<code>object</code>
<code>name</code>	Der Name des Netzwerks.	<code>string</code>
<code>cidr</code>	Der CIDR-Bereich des Netzwerks.	<code>string</code>
<code>enabled</code>	Definiert, ob die automatische Mitigation aktiviert ist.	<code>true</code> <code>false</code>
<code>mitigation_type</code>	Der Mitigationstyp des Netzwerks.	<code>ACTION_BLACK_HOLE</code> <code>ACTION_MITIGATE_ONPREM</code> <code>ACTION_MITIGATE_CLOUD</code>

Attribut	Beschreibung	Werte
auto_mitigation_strategy	Die Strategie der automatischen Mitigation des Netzwerks.	string
duration	Die Dauer der automatischen Mitigation.	integer
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
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,
  "mitigation_type": "ACTION_BLACKHOLE",
  "auto_mitigation_strategy": "IP",
  "duration": 0,
  "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 `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 `MitigationV0` 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_BLACK_HOLE ACTION_MITIGATE_ONPREM ACTION_MITIGATE_CLOUD
mitigation_cause	Die Art, 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 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)
dropped_bits		integer

Attribut	Beschreibung	Werte
	Die während der Mitigation verworfenen Bits insgesamt.	
dropped_packets	Die während der Mitigation verworfenen Pakete insgesamt.	integer
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,
      "dropped_bits": 0,
      "dropped_packets": 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
<code>id</code>	Die ID des Netzwerks.	<code>string</code>
<code>modified</code>	Das Datum der letzten Änderung im ISO-8601-Format.	<code>string(\$date-time)</code>
<code>cidr</code>	Der CIDR-Bereich des Netzwerks.	<code>string</code>
<code>enabled</code>	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.	<code>true</code> <code>false</code>
<code>pps_limit</code>	Der PPS-Schwellenwert.	<code>integer</code>
<code>bw_limit</code>	Der Bandbreiten-Schwellenwert in Mbps.	<code>integer</code>

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
<code>name</code>	Der Name des Netzwerks.	<code>string</code>
<code>pps_limit_calculated</code>	Der berechnete PPS-Schwellenwert.	<code>integer</code>
<code>bw_limit_calculated</code>	Der berechnete Bandbreiten-Schwellenwert.	<code>integer</code>
<code>team_id</code>	Die ID der Organisation, zu der dieses Netzwerk gehört.	<code>string</code>

Attribut	Beschreibung	Werte
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
active_partial_auto_mitigations	Die aktiven partiellen automatischen Mitigationen.	array
country_blocks	Die aktiven Länderblockierungen.	array
extra	Zusätzliche Informationen zum Netzwerk.	object
mitigation_type	Der konfigurierte Mitigationstyp.	string
network_type	Der Typ des Netzwerks.	string
customer_reference	Die Kundenreferenz-Kennung.	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 `NetworkV0` 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.	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

Attribut	Beschreibung	Werte
		false
active_partial_mitigations	Die aktiven partiellen manuellen Mitigationen.	array
active_partial_auto_mitigations	Die aktiven partiellen automatischen Mitigationen.	array
country_blocks	Die aktiven Länderblockierungen.	array
extra	Zusätzliche Informationen zum Netzwerk.	object
mitigation_type	Der konfigurierte Mitigationstyp.	string
network_type	Der Typ des Netzwerks.	string
customer_reference	Die Kundenreferenz-Kennung.	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": [
    {}
  ],
  "allow_manual_mitigation": true,
  "extra": {},
  "mitigation_type": "string",
  "network_type": "string",
  "customer_reference": "abc",
  "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	

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.

2.3.2.7 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:

Attr ibut	Beschreibung	Wert e
<code>cidr</code>	Der IP-Bereich in CIDR-Notation. Muss innerhalb der Organisation eindeutig sein.	string
<code>enabled</code>	Definiert, ob die automatische Mitigation für das Netzwerk aktiviert ist. Bei <code>false</code> werden keine automatischen Mitigationen ausgelöst; manuelle und Ops-Mitigationen sind davon nicht betroffen.	true false
<code>pps_limit</code>	Der absolute PPS-Schwellenwert. Erforderlich, falls <code>pps_limit_percentage</code> nicht angegeben ist.	integer
<code>bw_limit</code>	Der absolute Bandbreiten-Schwellenwert in Mbps. Erforderlich, falls <code>bw_limit_percentage</code> nicht angegeben ist.	integer

Die folgenden Attribute sind optional:

Attribut	Beschreibung	Werte
<code>name</code>	Der Name des Netzwerks.	string
<code>team_id</code>	Die ID der Organisation, zu der das Netzwerk hinzugefügt wird.	string
<code>pps_limit_calculated</code>	Der berechnete PPS-Schwellenwert.	integer
<code>bw_limit_calculated</code>	Der berechnete Bandbreiten-Schwellenwert.	integer

true

Attribut	Beschreibung	Werte
autoStatus	Zeigt an, ob sich das Netzwerk aktuell in automatischer Mitigation befindet.	false
manualStatus	Zeigt an, ob sich das Netzwerk aktuell in manueller Mitigation befindet.	true false
active_parti al_mitigatio ns	Die aktiven partiellen manuellen Mitigationen.	array
active_parti al_auto_miti gations	Die aktiven partiellen automatischen Mitigationen.	array
country_bloc ks	Die aktiven Ländersperren.	array
allow_manual _mitigation	Zeigt an, ob für das Netzwerk manuelle Mitigationen gestartet werden können. Der Standardwert ist true , falls das Attribut fehlt.	true false
extra	Zusätzliche benutzerdefinierte Felder der Organisation.	object
mitigation_t ype	Der anzuwendende Mitigationstyp.	ACTION_BL ACKHOLE ACTION_MI TIGATE_ON PREM ACTION_MI TIGATE_CL LOUD
network_type	Der Registrierungstyp des Netzwerks.	string
customer_ref erence	Die Kennung der Kundenreferenz.	string
emails	Die E-Mail-Adressen, die bei Start oder Ende einer Mitigation benachrichtigt werden.	array
duration	Die maximale Mitigationsdauer in Sekunden (Minimum 300).	integer

Attribut	Beschreibung	Werte
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 <code>NetworkV0</code> -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": [
    {}
  ],
  "allow_manual_mitigation": true,
  "extra": {},
  "mitigation_type": "string",
  "network_type": "string",
  "customer_reference": "abc",
  "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 `MitigationV0` 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_BLACK_HOLE ACTION_MITIGATE_ONPREM

Attribut	Beschreibung	Werte
		ACTION_MITIG ATE_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(\$datetime)
end	Das Enddatum der Mitigation im ISO-8601-Format.	string(\$datetime)
created_at	Das Erstellungsdatum im ISO-8601-Format.	string(\$datetime)
updated_at	Das Datum der letzten Änderung im ISO-8601-Format.	string(\$datetime)
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)

Attribut	Beschreibung	Werte
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
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.

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.

2.3.2.9 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	Wert
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 `MitigationV0` 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
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)

Attribut	Beschreibung	Werte
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	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.

STATUSCODE	BESCHREIBUNG
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.

2.3.2.10 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 `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 `MitigationV0` 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(\$datetime)
end	Wann die Mitigation beendet wurde; null, solange sie noch läuft.	string(\$datetime)
created_at	Das Erstellungsdatum des Eintrags im ISO-8601-Format.	string(\$datetime)
updated_at	Das Datum der letzten Aktualisierung des Eintrags im ISO-8601-Format.	string(\$datetime)
actual_bw	Die gemessene Bandbreite zu Beginn der Mitigation.	number(\$float)
actual_pps	Die gemessene Paketrage 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)
dropped_bits	Die während der Mitigation verworfenen Bits insgesamt.	integer
dropped_packets	Die während der Mitigation verworfenen Pakete insgesamt.	integer
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,
    "dropped_bits": 0,
    "dropped_packets": 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 `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 `MitigationV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

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

Attribut	Beschreibung	Werte
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)
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)
dropped_bits	Die Gesamtzahl der während der Mitigation verworfenen Bits.	integer
dropped_packets	Die Gesamtzahl der während der Mitigation verworfenen Pakete.	integer
has_report		true false

Attribut	Beschreibung	Werte
	Zeigt an, ob für die Mitigation ein Report verfügbar ist.	
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,
  "dropped_bits": 0,
  "dropped_packets": 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
data	Das Array der Datenpunkte der Serie. Jeder Punkt liefert die Attribute <code>x</code> und <code>y</code> .	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.

STATUSCODE	BESCHREIBUNG
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 `MitigationV0` 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_BLACK HOLE ACTION_MITIG ATE_ONPREM

Attribut	Beschreibung	Werte
		ACTION_MITIG ATE_CLOUD
mitigation_cause	Wie die Mitigation ausgelöst wurde.	MANUAL_TRIGGER AUTO_TRIGGER OPS_TRIGGER UNKNOWN_TRIGGER
start	Das Startdatum im ISO-8601-Format.	string(\$datetime)
end	Das Enddatum im ISO-8601-Format.	string(\$datetime)
created_at	Das Erstellungsdatum im ISO-8601-Format.	string(\$datetime)
updated_at	Das Datum der letzten Änderung im ISO-8601-Format.	string(\$datetime)
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)

Attribut	Beschreibung	Werte
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
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
orderByDir	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 `AnomalyV0` 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 <code>null</code> .	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 `MitigationStatisticV0` 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 mitigierte 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 `MitigationStatisticGroupV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
<code>id</code>	Die Monatskennung des Eintrags im Format <code>YYYY-MM</code> .	<code>string</code>

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 Country-Packet-Reports

2.3.6.1 Den Country-Packet-Report des aktuellen Monats abrufen



Dieser Endpunkt verwendet nicht die reguläre DataHub-API-Authentifizierung. Die Authentifizierung erfolgt über ein separates statisches Token (Konfigurationswert `COUNTRY_STATS_API_TOKEN`), das als Bearer-Token im `Authorization`-Header übermittelt wird.

Senden einer `GET`-Anfrage an den Endpunkt `/country-packet-reports`.

2.3.6.1.1 Beschreibung

Mit der `List-Country-Packet-Reports`-Anfrage fordern Sie den aggregierten Country-Packet-Report des aktuellen Monats an. Der Report enthält pro Land die Summe der Pakete aus den im Berichtsmonat beendeten Mitigationen, absteigend nach Paketanzahl sortiert.

Das System aggregiert die Daten stündlich neu. Die Aggregation setzt das Feature-Flag `COUNTRY_STATS_ENABLED` voraus; andernfalls bleibt der Report leer.

2.3.6.1.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.6.1.3 Anfrage

Um den Report des aktuellen Monats anzufordern, ist keine zusätzliche Information im Pfad der Anfrage erforderlich.

Als Ergebnis erhalten Sie in `data` eine Liste von Länder-Einträgen sowie ein Objekt `meta` mit Angaben zum Berichtszeitraum.

Die Länder-Einträge liefern die folgenden Informationen:

Attribut	Beschreibung	Werte
<code>country</code>	Der ISO-Ländercode des Landes.	<code>string</code>

Attribut	Beschreibung	Werte
packets	Die aggregierte Anzahl der Pakete für das Land im Berichtsmonat.	integer

Das Objekt `meta` liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
period_start	Der erste Tag des Berichtsmonats im Format YYYY-MM-DD .	string(\$date)
period_end	Der letzte Tag des Berichtsmonats im Format YYYY-MM-DD .	string(\$date)
last_updated_at	Datum und Uhrzeit der letzten Aggregation im ISO-8601-Format; null , wenn noch keine Daten aggregiert wurden.	string(\$date-time)

2.3.6.1.4 Beispiel

Beispiel-Antwort:

```
{
  "data": [
    {
      "country": "DE",
      "packets": 3023924
    },
    {
      "country": "US",
      "packets": 953069
    },
    {
      "country": "NL",
      "packets": 561701
    }
  ],
  "meta": {
    "period_start": "2026-06-01",
    "period_end": "2026-06-30",
    "last_updated_at": "2026-06-30T23:05:00+00:00"
  }
}
```

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 der <code>Authorization</code> -Header fehlt oder kein Bearer-Token enthält.
403	Die Anfrage war nicht erfolgreich, da das übermittelte Token ungültig ist.

2.3.6.2 Den Country-Packet-Report eines bestimmten Monats abrufen



Dieser Endpunkt verwendet nicht die reguläre DataHub-API-Authentifizierung. Die Authentifizierung erfolgt über ein separates statisches Token (Konfigurationswert `COUNTRY_STATS_API_TOKEN`), das als Bearer-Token im `Authorization` -Header übermittelt wird.

Senden einer `GET` -Anfrage an den Endpunkt `/country-packet-reports/{period}` .

2.3.6.2.1 Beschreibung

Mit der `Get-Country-Packet-Report`-Anfrage fordern Sie den aggregierten Country-Packet-Report eines bestimmten Monats an. Der Report enthält pro Land die Summe der Pakete aus den im Berichtsmonat beendeten Mitigationen, absteigend nach Paketanzahl sortiert.

2.3.6.2.2 Voraussetzungen

Werte der Anfrage: **Monat** {period}

Objekte: keine

2.3.6.2.3 Anfrage

Um den Report eines bestimmten Monats anzufordern, fügen Sie den **Monat** {period} im Format YYYY-MM in den Pfad der Anfrage ein. Ein Wert in einem anderen Format führt zu einem 404-Fehler.

Als Ergebnis erhalten Sie in `data` eine Liste von Länder-Einträgen sowie ein Objekt `meta` mit Angaben zum Berichtszeitraum. Der Aufbau der Antwort entspricht der Anfrage für den aktuellen Monat. Siehe [Den Country-Packet-Report des aktuellen Monats abrufen](#).

Für Monate ohne aggregierte Daten enthält die Antwort eine leere Liste `data` ; `last_updated_at` ist in diesem Fall `null` .

2.3.6.2.4 Beispiel

Beispiel-Antwort:

```
{
  "data": [
    {
      "country": "DE",
      "packets": 3023924
    },
    {
      "country": "FR",
      "packets": 529490
    }
  ],
  "meta": {
    "period_start": "2026-05-01",
    "period_end": "2026-05-31",
    "last_updated_at": "2026-06-01T00:35:00+00:00"
  }
}
```

2.3.6.2.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	

STATUSCODE	BESCHREIBUNG
	Die Anfrage war nicht erfolgreich, da der Authorization -Header fehlt oder kein Bearer-Token enthält.
403	Die Anfrage war nicht erfolgreich, da das übermittelte Token ungültig ist.
404	Die Anfrage war nicht erfolgreich, da der angegebene Monat kein gültiges Format hat.

2.3.6.3 Den Country-Packet-Report des aktuellen Tages abrufen



Dieser Endpunkt verwendet nicht die reguläre DataHub-API-Authentifizierung. Die Authentifizierung erfolgt über ein separates statisches Token (Konfigurationswert `COUNTRY_STATS_API_TOKEN`), das als Bearer-Token im Authorization -Header übermittelt wird.

Senden einer GET -Anfrage an den Endpunkt `/country-packet-daily-reports`.

2.3.6.3.1 Beschreibung

Mit der List-Country-Packet-Reports-Anfrage fordern Sie den aggregierten Country-Packet-Report des aktuellen Tages an. Der Report enthält pro Land die Summe der Pakete aus den am Berichtstag beendeten Mitigationen, absteigend nach Paketanzahl sortiert.

Das System aggregiert die Daten stündlich neu. Die Aggregation setzt das Feature-Flag `COUNTRY_STATS_ENABLED` voraus; andernfalls bleibt der Report leer.

2.3.6.3.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: keine

2.3.6.3.3 Anfrage

Um den Report des aktuellen Tages anzufordern, ist keine zusätzliche Information im Pfad der Anfrage erforderlich.

Als Ergebnis erhalten Sie in `data` eine Liste von Tages-Einträgen. Jeder Eintrag enthält das Datum sowie in `countries` die Länder-Einträge.

Die Einträge liefern die folgenden Informationen:

Attribut	Beschreibung	Werte
<code>date</code>	Der Tag, für den der Bericht erstellt wird.	<code>string(\$date)</code>
<code>country</code>	Der ISO-Ländercode des Landes.	<code>string</code>
<code>packets</code>	Die aggregierte Anzahl der Pakete für das Land am Berichtstag.	<code>integer</code>

2.3.6.3.4 Beispiel

Beispiel-Antwort:

```
{
  "data": [
    {
      "date": "2026-06-08",
      "countries": [
        {
          "country": "DE",
          "packets": 3023924
        },
        {
          "country": "US",
          "packets": 953069
        },
        {
          "country": "NL",
          "packets": 561701
        }
      ]
    }
  ]
}
```

2.3.6.3.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da der <code>Authorization</code> -Header fehlt oder kein Bearer-Token enthält.
403	Die Anfrage war nicht erfolgreich, da das übermittelte Token ungültig ist.

2.3.6.4 Den Country-Packet-Report eines bestimmten Tages abrufen



Dieser Endpunkt verwendet nicht die reguläre DataHub-API-Authentifizierung. Die Authentifizierung erfolgt über ein separates statisches Token (Konfigurationswert `COUNTRY_STATS_API_TOKEN`), das als Bearer-Token im `Authorization` -Header übermittelt wird.

Senden einer `GET` -Anfrage an den Endpunkt `/country-packet-daily-reports/{period}`.

2.3.6.4.1 Beschreibung

Mit der `Get-Country-Packet-Report`-Anfrage fordern Sie den aggregierten Country-Packet-Report eines bestimmten Tages an. Der Report enthält pro Land die Summe der Pakete aus den am Berichtstag beendeten Mitigationen, absteigend nach Paketanzahl sortiert.

2.3.6.4.2 Voraussetzungen

Werte der Anfrage: **Tag** {period}

Objekte: keine

2.3.6.4.3 Anfrage

Um den Report eines bestimmten Tages anzufordern, fügen Sie den **Tag** {period} im Format YYYY-MM-DD in den Pfad der Anfrage ein. Ein Wert in einem anderen Format führt zu einem 404-Fehler.

Als Ergebnis erhalten Sie in `data` eine Liste von Tages-Einträgen. Jeder Eintrag enthält das Datum sowie in `countries` die Länder-Einträge. Der Aufbau der Antwort entspricht der Anfrage für den aktuellen Tag. Siehe [Den Country-Packet-Report des aktuellen Tages abrufen](#).

Für Tage ohne aggregierte Daten enthält die Antwort eine leere Liste `data`.

2.3.6.4.4 Beispiel

Beispiel-Antwort:

```
{
  "data": [
    {
      "date": "2026-06-08",
      "countries": [
        {
          "country": "DE",
          "packets": 3023924
        },
        {
          "country": "US",
          "packets": 953069
        },
        {
          "country": "NL",
          "packets": 561701
        }
      ]
    }
  ]
}
```

2.3.6.4.5 Antworten

Die folgenden Antworten sind möglich:

STATUSCODE	BESCHREIBUNG
200	Die Anfrage war erfolgreich.
401	Die Anfrage war nicht erfolgreich, da der Authorization -Header fehlt oder kein Bearer-Token enthält.
403	Die Anfrage war nicht erfolgreich, da das übermittelte Token ungültig ist.
404	Die Anfrage war nicht erfolgreich, da der angegebene Tag kein gültiges Format hat.

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 `AuditLogV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
<code>event</code>	Der Typ des protokollierten Ereignisses.	<code>string</code>
<code>resource</code>	Der Typ der vom Ereignis betroffenen Ressource.	<code>string</code>
<code>resource_iden tifier</code>	Die Kennung der betroffenen Ressource.	<code>string</code>
<code>performed_by</code>		<code>string</code>

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 Nutzens 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 Nutzens 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 Nutzens anzufordern, fügen Sie dem Pfad der Anfrage keine zusätzlichen Informationen hinzu.

Als Ergebnis erhalten Sie ein Objekt `UserV0` mit den angefragten Informationen.

Das Objekt liefert die folgenden Informationen:

Attribut	Beschreibung	Werte
<code>id</code>	Die ID des Nutzens.	string
<code>name</code>	Der vollständige Name des Nutzens.	string
<code>email</code>	Die E-Mail-Adresse des Nutzens.	string
<code>activeOrganisation</code>	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 Nutzers 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 Nutzens für E-Mail-Benachrichtigungen zu Mitigationen und Anomalien.

2.3.8.2.2 Voraussetzungen

Werte der Anfrage: keine

Objekte: NotificationPreferencesV0

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 NotificationPreferencesV0 mit den folgenden Attributen:

Attribut	Beschreibung	Werte
notification sEnabled	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 Nutzens.	string
name	Der vollständige Name des Nutzens.	string
email	Die E-Mail-Adresse des Nutzens.	string
notification sEnabled	Zeigt an, ob der Nutzende für E-Mail-Benachrichtigungen zu Mitigationen und Anomalien angemeldet ist.	true , false
activeOrgani sation	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.

Die Einrichtung beschreibt [**Zwei-Faktor-Authentifizierung aktivieren**](#).

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 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 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.

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		Wiederholen Sie den Vorgang.

Meldung	Ursache	Abhilfe
Fehler aufgetreten. Bitte versuchen Sie es später noch einmal.	Der Server hat das Unternehmen nicht gelöscht.	
Beim Löschen der Unternehmen ist ein Fehler aufgetreten. Löschen Sie zuerst die YAML-Datei auf dem Server und versuchen Sie es noch einmal.	Das Unternehmen ist zusätzlich über eine YAML-Datei auf dem Server beschrieben. Solange sie besteht, legt die Anwendung das Unternehmen wieder an.	Löschen Sie die YAML-Datei des Unternehmens auf dem Server und löschen Sie das Unternehmen anschließend erneut. Siehe Konfiguration über YAML .



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 <code>ViolationV0</code> 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.
Dicktengleich	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 Konfiguration über YAML

Neben der Verwaltung der Unternehmen und Nutzenden über die grafische Oberfläche des Myra DataHub haben Sie zudem die Möglichkeit, sämtliche Konfigurationen mittels YAML-Dateien vorzunehmen.

Damit das Anlegen von Unternehmen, deren Nutzenden und deren Netzwerken funktioniert, müssen die Anweisungen als YAML im nachstehenden Format übergeben werden.

```
custname: 'Client A'
timestamp: 2025-02-27 143232
portal:
  enabled: true
  email: noc@myrasecurity.com
  lastname: Myra
  forename: Security
1.1.1.1/32:
  enabled: true
  email:
    - noc@myrasecurity.com
pps_limit: 500000
bw_limit: 4000
duration: 14400
type: ACTION_BLACKHOLE
wholenet:
  enabled: true
nettype: RIPE (PI)
extra:
  INTERNET-SERVICEKENNUNG: L2220001
  CUSTNETNAME: Network 1
  DIENST-ID: HWDDSxxx
  DEBITOR: Debitor 2
  CHANNEL: 1000
  DETAILS: Description for the network
```



Sie können mit der YAML-Datei nur Unternehmen und jeweils einen Nutzenden mit Admin-Rechten hinzufügen. Das Ändern und Löschen ist per YAML nicht möglich und muss in der grafischen Benutzeroberfläche vorgenommen werden.



Sie können mit der YAML-Datei ein oder mehrere Netzwerke einem Unternehmen hinzufügen, ändern oder löschen.



Sie können mit der YAML-Datei für Unternehmen nicht die SIEM-Integration (Security Information and Event Management) aktivieren. Die Aktivierung von SIEM für ein Unternehmen ist nur über die grafische Benutzeroberfläche des Myra DataHub möglich.

Die Werte, die im YAML-Format übergeben werden, entsprechen den Informationen in der grafischen Benutzeroberfläche des Myra DataHub und lassen sich wie folgt zuordnen:

Element

Beschreibung

Unternehmenskonten

NAME	KUNDEN-ID
Muster GmbH	10024

YAML - Unternehmenskonten

Benutzerverwaltung

E-MAIL-ADRESSE
max.mustermann@example.com

YAML - Nutzerverwaltung 1

NAME	ROLLE
Max Mustermann	Administrator

YAML - Nutzerverwaltung 2

Netzwerke

NAME	IP-ADRESSE	NETZWERKTYP
Network 1	XXX.XXX.XXX.XXX/24	RIPE (PI)
Network 2	XXX.XXX.XXX.XXX/24	RIPE (LIR)

YAML - Netzwerke

Im Folgenden finden Sie eine tabellarische Zuordnung aller Werte in der YAML-Datei und auf der grafischen Benutzeroberfläche:

Abgleich der Felder in der Myra DataHub UI mit der YAML-Datei

Myra DataHub UI	YAML	Beschreibung
Unternehmen		
Name	Custname	Name des Kunden
Kunden-ID	Name der YAML-Datei	Individuelle ID des Kunden
Nutzerverwaltung		
E-Mail-Adresse	portal:email	E-Mail-Adresse des ersten Adminkontos. Hinweis: Beim Hinzufügen eines neuen Unternehmens über die YAML-Datei wird nur ein Nutzender mit Admin-Rechten angelegt. Weitere Konten können nur über die grafische Benutzeroberfläche hinzugefügt werden.
Name	portal:lastname	Name des ersten Adminkontos.
Name	portal:forename	Vorname des ersten Adminkontos.
	portal:enabled	Nur in YAML: Definiert, ob ein Adminkonto für das neue Unternehmen angelegt wird. Die folgenden Werte sind verfügbar: true : Ein Adminkonto wird angelegt. false : Ein Adminkonto wird nicht angelegt.
Netzwerke		
Name		Der Name des Netzwerkes.

Myra DataHub UI	YAML	Beschreibung
	extra: CUSTNET NAME	
IP	CIDR	Die IP-Adresse des Netzwerkes.
Paketraten-Schwellewert (Pakete/s)	pps_limit	Der Schwellenwert für die maximale Anzahl der erlaubten Pakete pro Sekunde.
Dienst-ID	extra: DIENST-ID	Ein Versatel-spezifischer Wert.
Channel	extra: CHANNEL	Ein Versatel-spezifischer Wert.
Netzwerktyp	nettype	Der Netzwerktyp für das entsprechende Netzwerk. Die folgenden Werte sind verfügbar: RIPE : Nutzt das Regional Internet Registry for Europe (RIPE) als Netzwerktyp. RIPE (PI) : Nutzt den Provider Independent Address Space (PI-Adressraum) als Netzwerktyp. RIPE (LIR) : Nutzt das Local Internet Registry (LIR) als Netzwerktyp. RIPE (AS8881) : Nutzt das autonome System (AS) von Versatel als Netzwerktyp. SUBNET or Subnet : Nutzt einen selbstdefinierten IP-Adressbereich als Netzwerktyp.
Netzwerk Referenz	extra: INTERNET-T-	Enthält die Unique L-Number für die Internetleitung, über die die Kunden bei Versatel angebunden werden.

Myra DataHub UI	YAML	Beschreibung
	SERVICE KENNUNG	
Bandbreiten-Schwelle wert (MBit/s)	bw_limit	Der Schwellenwert für die maximale Höhe der möglichen Bandbreite.
Dauer der Mitigation (in Sek)	duration	Die Dauer der Mitigation in Sekunden, nachdem der Datenverkehr unterhalb der Schwellwerte gefallen ist.
Debitor	extra: DEBITOR	Ein Versatel-spezifischer Wert.
Details	extra: DETAILS	Ein individueller Kommentar zur Beschreibung des Netzwerkes.
Mitigationstyp	type	Definition der Art und Weise, wie die Mitigation durchgeführt wird. Die folgenden Werte sind verfügbar: ACTION_BLACKHOLE: Bei Überschreitung des Schwellenwertes wird der komplette Traffic verworfen. ACTION_MITIGATE_ONPREM: Bei Überschreitung des Schwellenwertes wird der Traffic über die internen Server bereinigt. ACTION_MITIGATE_CLOUD: Bei Überschreitung des Schwellenwertes wird der Traffic über das Myra Scrubbing Center bereinigt.
Mitigationstrategie	Wholene t: enabled	Definiert, 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.

Myra DataHub UI	YAML	Beschreibung
E-Mail-Adresse für Benachrichtigungen	email	Die E-Mail-Adresse des Nutzenden, an den Mitteilungen zur Mitigation gehen.
Automatische Aktionen	enabled	Zeigt an, ob eine automatische Mitigation für das ausgewählte Netzwerk durchgeführt wird oder nicht. Die folgenden Werte sind verfügbar: true : Die automatische Mitigation ist aktiviert. false : Die automatische Mitigation ist deaktiviert.

4.3 Glossar

Element	Beschreibung
Scrubbing	Scrubbing bezeichnet den Vorgang, Internet-Traffic, insbesondere auf OSI-Layer 3/4, 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 3/4 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 3/4 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 3/4 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 erfolgreichem 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 DataHub	Der Myra DataHub ist eine webbasierte Benutzeroberfläche (WebGUI) für Myra Partner zur Übersicht der Endkunden. Darauf sind die Endkunden mit den angeschalteten Netzen, sowie deren angelegten Konten dargestellt. Dem Endkunden werden innerhalb dieser WebGUI die Übersicht zum Traffic-Verlauf, die angeschalteten Netze, sowie die gesammelten Mitigationsreports präsentiert. Innerhalb der Darstellung des Traffic-Verlaufs ist eine Filterung zwischen Bandbreite und Paketrage, 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 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.