

Splunk & AI

Splunk MCP-Server

Kai-Ping Seidenschnur
Udo Götzen

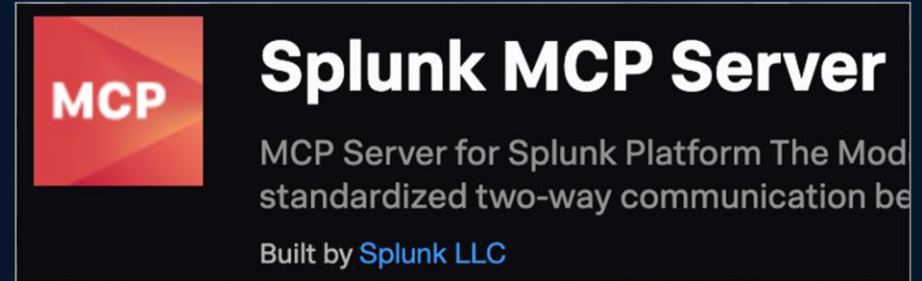
March 2026

Agenda

1. Wofür brauche ich MCP (Model Context Protocol)
2. Splunk Token für MCP erstellen
3. Node.js auf dem eigenen Laptop/Macbook installieren
4. MCP-Konfiguration in Splunk MCP-Server App generieren
5. AI-Agent (Claude) als MCP-Client konfigurieren
6. Erfolgreiche Verbindung zu Splunk überprüfen
7. Use Case Beispiel zur Arbeit mit MCP-Clients
8. Troubleshooting

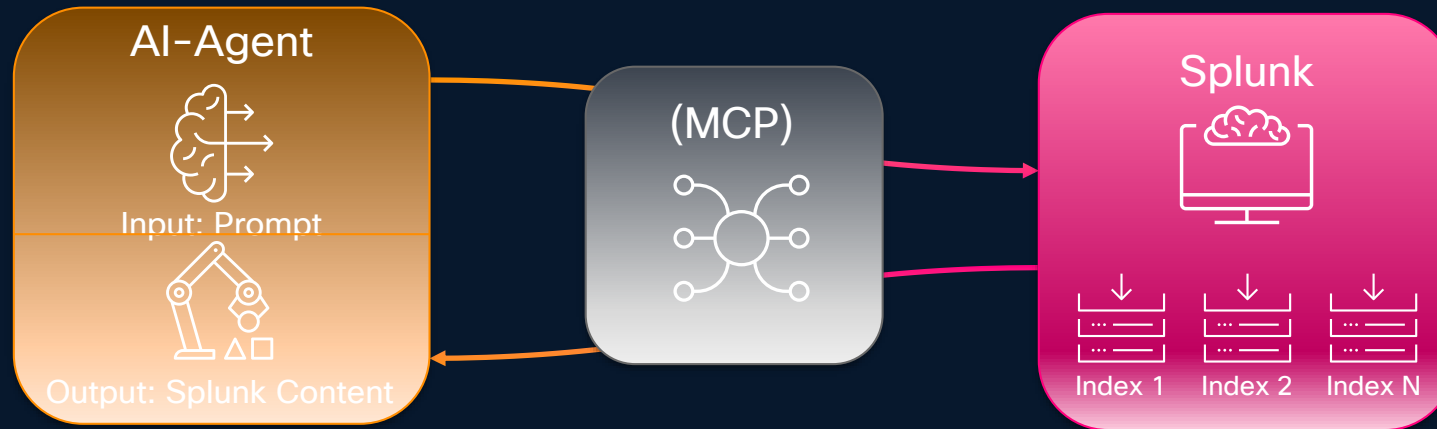
Voraussetzungen

- Was benötigt wird:
 - Eine Splunk Umgebung
 - https://www.splunk.com/en_us/download.html
 - Die Splunk MCP-Server App (Model Context Protocol)
 - <https://splunkbase.splunk.com/app/7931>
 - Einen Claude Account bzw. Lizenz
 - <https://claude.ai/login>
 - Node JS
 - <https://nodejs.org/en/download>
 - Claude Client
 - <https://www.claude.com/download>



Wofür brauche ich MCP (Model Context Protocol)?

- Mittels MCP können externe AI-Assistants auf eine Splunk Umgebung zugreifen



Welche Use Cases lassen sich daraus ableiten?

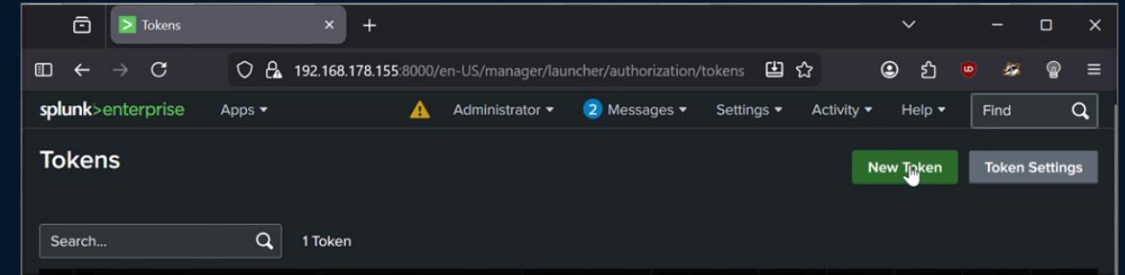
SPL
Create,
Optimize,
Explain

NLP-2-Splunk
Ask questions and
run queries in
natural language

Information
Retrieve data about
indexes, Metadata,
users and KO

Splunk Token für MCP erstellen

- Installiere die „Splunk MCP Server“ App
- <https://splunkbase.splunk.com/app/7931>
- „Settings“ -> „Tokens“ -> „New Token“
 - Audience = mcp
 - „Create“
- Token aufbewahren!



Token appears here after creation and is no longer accessible after you close this window.

- Wir brauchen den später!

New Token

i You can only create tokens for SAML users if you enable either attribute query requests or authentication extensions.

* User
User who will receive this token.

* Audience
Purpose of the token.

Expiration
Examples: +10m,+20h,+30d

Not Before
Examples: +10m,+20h,+30d

Token
Token appears here after creation and is no longer accessible after you close this window.

Cancel Create

New Token

i You can only create tokens for SAML users if you enable either attribute query requests or authentication extensions.

* User
User who will receive this token.

* Audience
Purpose of the token.

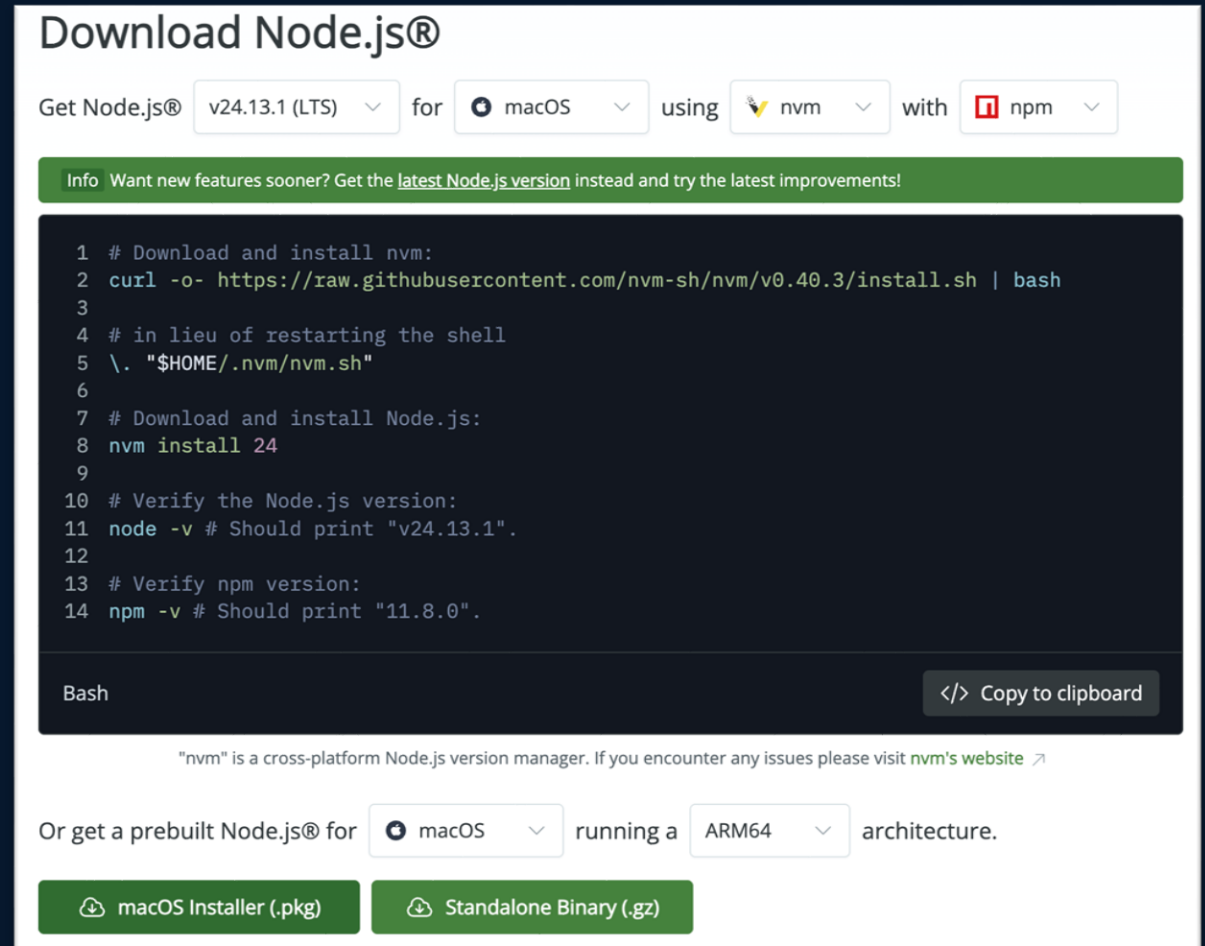
Expiration
Examples: +10m,+20h,+30d

Not Before
Examples: +10m,+20h,+30d

Token
Token appears here after creation and is no longer accessible after you close this window.

Node.js auf dem eigenen Laptop/Macbook installieren

- Node.js wird für Verbindungsaufbau von Claude zu Splunk benötigt
 - Der nxp Befehl wird von MCP verwendet
- <https://nodejs.org/en/download>
- Nach der reinen Installation gibt es keine weiteren Schritte



The screenshot shows the Node.js download page for macOS. At the top, it says "Download Node.js®". Below that, there are dropdown menus for "Get Node.js®" (set to v24.13.1 (LTS)), "for" (set to macOS), "using" (set to nvm), and "with" (set to npm). A green banner below the dropdowns says "Info Want new features sooner? Get the latest Node.js version instead and try the latest improvements!". The main content is a code block with the following instructions:

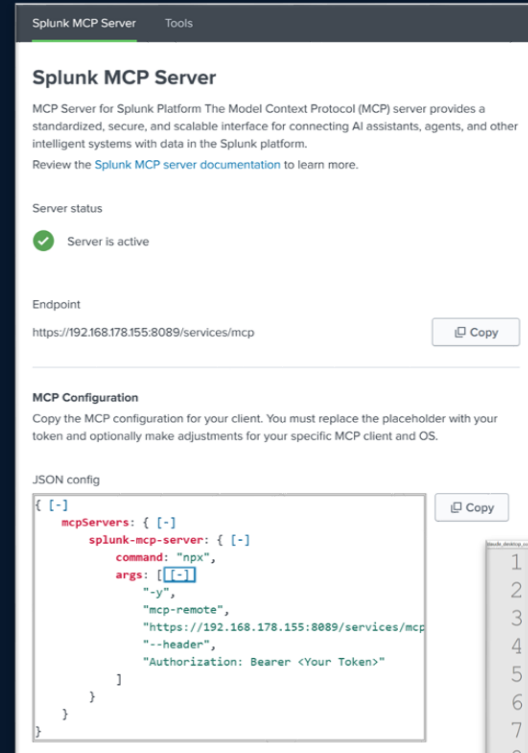
```
1 # Download and install nvm:
2 curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.40.3/install.sh | bash
3
4 # in lieu of restarting the shell
5 \. "$HOME/.nvm/nvm.sh"
6
7 # Download and install Node.js:
8 nvm install 24
9
10 # Verify the Node.js version:
11 node -v # Should print "v24.13.1".
12
13 # Verify npm version:
14 npm -v # Should print "11.8.0".
```

Below the code block, there is a "Bash" label and a "Copy to clipboard" button. At the bottom of the page, there is a note: "nvm" is a cross-platform Node.js version manager. If you encounter any issues please visit [nvm's website](#). Below this, there are two more dropdown menus: "Or get a prebuilt Node.js® for" (set to macOS) and "running a" (set to ARM64) "architecture." At the bottom, there are two buttons: "macOS Installer (.pkg)" and "Standalone Binary (.gz)".

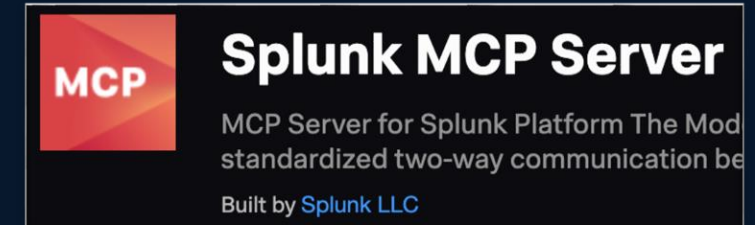
MCP-Konfiguration in Splunk MCP-Server App generieren

- Innerhalb der Splunk MCP Server App kann eine MCP-Konfiguration generiert werden
- Durch einen Editor lässt sich die Konfiguration anpassen
- Der Token muss eingefügt werden (<Your Token>)
- Folgende Zeile sollte in einer Demo hinterlegt werden (Keine Zertifikatsüberprüfung)

```
“env“: {  
  “NODE_TLS_REJECT_UNAUTHORIZED“: “0“  
}
```



The screenshot shows the 'Splunk MCP Server' web interface. It includes a 'Server status' section with a green checkmark indicating the server is active. Below that is the 'Endpoint' section with the URL 'https://192.168.178.155:8089/services/mcp' and a 'Copy' button. The 'MCP Configuration' section contains instructions to copy the configuration for the client and a 'JSON config' section with a 'Copy' button. The JSON config is partially visible in the screenshot.

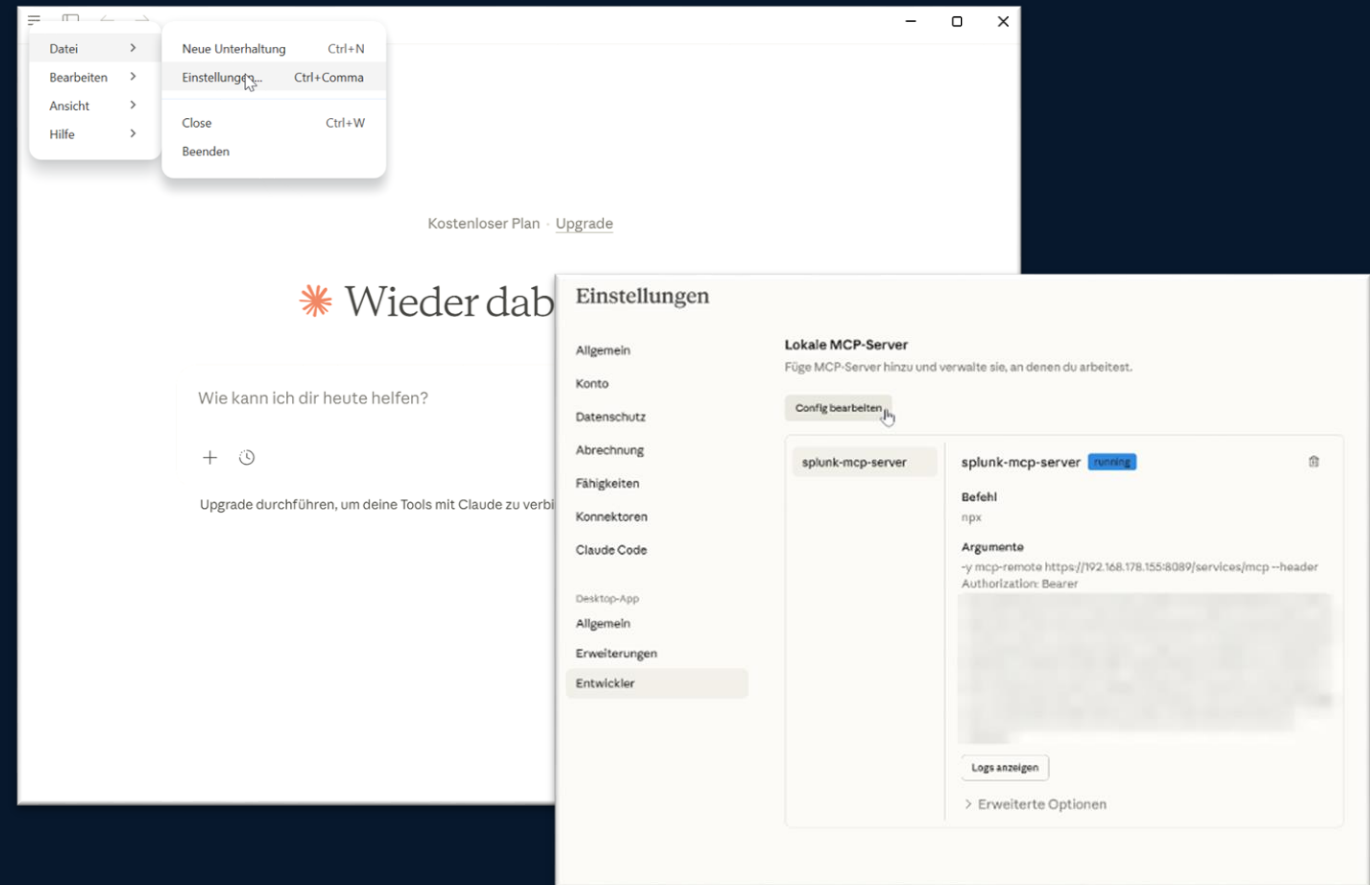


The image shows the 'Splunk MCP Server' branding. It features the 'MCP' logo in a red square, followed by the text 'Splunk MCP Server' and 'MCP Server for Splunk Platform The Mod standardized two-way communication be'. At the bottom, it says 'Built by Splunk LLC'.

```
1 {  
2   "mcpServers": {  
3     "splunk-mcp-server": {  
4       "command": "npx",  
5       "args": [  
6         "-y",  
7         "mcp-remote",  
8         "https://192.168.178.155:8089/services/mcp",  
9         "--header",  
10        "Authorization: Bearer eyJraWQiOiJzcGxlbmsuc  
11      ],  
12      "env": {  
13        "NODE_TLS_REJECT_UNAUTHORIZED": "0"  
14      }  
15    }  
16  }  
17 }
```

AI-Agent (Claude) als MCP-Client konfigurieren

- Nach der Installation von Claude Desktop kann MCP hinterlegt werden
- Dafür müssen in der UI die Einstellungen geöffnet werden (Datei -> Einstellungen)
- In den Einstellungen auf den Reiter “Entwickler“ wechseln
- Die Konfiguration für den Lokalen MCP-Server bearbeiten
- Hier kann die fertige Konfiguration eingefügt werden



Erfolgreiche Verbindung zu Splunk überprüfen

- Es ist Zeit für die ersten Prompts!
- Zuerst sollte überprüft werden, ob auf Splunk zugegriffen werden kann
- Frage: „Hast du Zugriff auf Splunk“?
- Sobald die Verbindung steht, können individuelle Prompts genutzt werden

Do you have access to splunk?

No, I do not have access to Splunk.

check again the Splunk MCP is running

You're right - let me check what tools I actually have available.

get_splunk_info

I apologize - you're absolutely correct! I **do** have access to Splunk through the Splunk MCP server.

I can see you have a Splunk instance (SplunkLab) running version 10.2.0 on Linux with multiple server roles including indexer, license master, and KV store.

I can help you with:

- Running Splunk queries (SPL)
- Getting information about indexes, users, and knowledge objects
- Retrieving metadata about hosts, sources, and sourcetypes
- Accessing KV Store collections
- And more

What would you like to do with Splunk?

Beispiel zur Arbeit mit einem MCP-Client: Datenanalyse

The screenshot shows a chat window with a sidebar on the left and a main chat area on the right. The sidebar contains navigation options like 'Neuer Chat', 'Suchen', 'Anpassen', 'Chats', 'Projekte', 'Artefakte', and 'Code'. The main chat area displays a conversation about analyzing suspicious activities in firewall logs. A system message at the top asks to analyze the 'index=firewall_fortigate' index for suspicious activities between 05.01.2025 and 08.05.2025. The assistant's response starts with 'Ich starte die Analyse...' and provides a security analysis titled 'Sicherheitsanalyse — index=firewall_fortigate' for the specified time period. The analysis identifies a critical finding: 'Befund 1: Massiver SSH-Brute-Force / Port-Scanning aus Estland (KRITISCH)'. The source is identified as IP '2a07:1182:101::104' (Estonia), which is on the firewall's blacklist. The analysis notes that this IP made over 107,500 blocked connection attempts over port 22 (SSH) directed at various internal hosts in the subnet '2a07:1182:2:f20::x'. At the bottom, there is an input field for a response, a version indicator 'Sonnet 4.6', and a disclaimer: 'Claude ist eine KI und kann Fehler machen. Bitte überprüfe die Antworten.'

Verdächtige Aktivitäten in Firewall-Logs analysieren

Analysiere den index=firewall_fortigate und finde verdächtige Aktivitäten im Zeitraum 05.01.2025 bis 08.05.2025

Ich starte die Analyse des `firewall_fortigate` Index. Lass mich zunächst einen Überblick über die Daten verschaffen.

Splunk-Integration-Integration verwendet >

Ich habe nun alle relevanten Daten gesammelt und kann eine umfassende Analyse erstellen.

Sicherheitsanalyse — `index=firewall_fortigate`

Zeitraum: 05.01.2025 – 08.05.2025

🚩 Befund 1: Massiver SSH-Brute-Force / Port-Scanning aus Estland (KRITISCH)

Quelle: `2a07:1182:101::104` (Estland) — steht auf der **Blacklist** der Firewall

Die weitaus auffälligste Aktivität im gesamten Zeitraum: Diese einzelne IP-Adresse hat **über 107.500 geblockte Verbindungsversuche** erz ⬇, ausnahmslos über **Port 22 (SSH)**, gerichtet auf zahlreiche interne Zielhosts im Subnetz `2a07:1182:2:f20::x`. Die

Antworten...

+ Sonnet 4.6 🗣

Claude ist eine KI und kann Fehler machen. Bitte überprüfe die Antworten.

Beispiel zur Arbeit mit einem MCP-Client: Dashboard

Neuer Chat

Suchen

Anpassen

Chats

Projekte

Artefakte

Code

Zuletzt verwendet

Splunk access inquiry

Beste LLM-Modelle für Ollama

Vigor DSL-Qualität in Splunk analy...

MCP-konfigurierte Splunk-Umgeb...

Verdächtige Aktivitäten in Firewal ...

Fortigate firewall malicious activit...

Awtrix-Display für Sonnenbatteri...

Homeassistant Sensoren und Wer...

Firewall malicious activity audit

Tesla BLE Projekt auf M5Stack Na...

ESP Home Tesla BLE Konfiguratio...

Feiertage und Wochenenden in de...

UG Udo Goetzen
Kostenloser Plan

Verdächtige Aktivitäten in Firewall-Logs analysieren

Ich verstehe — du meinst ein natives **Splunk XML Dashboard**, das direkt in Splunk importiert werden kann. Lass mich zuerst die vorhandenen Daten und Indizes prüfen, um die Panels optimal zu bauen.

Splunk-Integration-Integration verwendet >

Gut – ich habe alle nötigen Feldnamen. Jetzt baue ich das native Splunk XML Dashboard.

Datei erstellt, datei lesen >

Hier ist dein natives **Splunk XML Dashboard** – direkt importierbar. So gehst du vor:

Import in Splunk:

1. In Splunk → **Dashboards** → **Create New Dashboard**
2. Oben rechts auf **Edit XML** klicken
3. Den gesamten XML-Inhalt einfügen → **Save**

Was das Dashboard enthält (8 Zeilen, 22 Panels):

Antworten...

Sonnet 4.6

Claude ist eine KI und kann Fehler machen. Bitte überprüfe die Antworten.

Soc dashboard splunk · XML

```
BE34" midColor="#6DB7C6" minColor="#53A051"/>
  <scale type="minMidMax" minValue="0"/>
</format>
</table>
</panel>

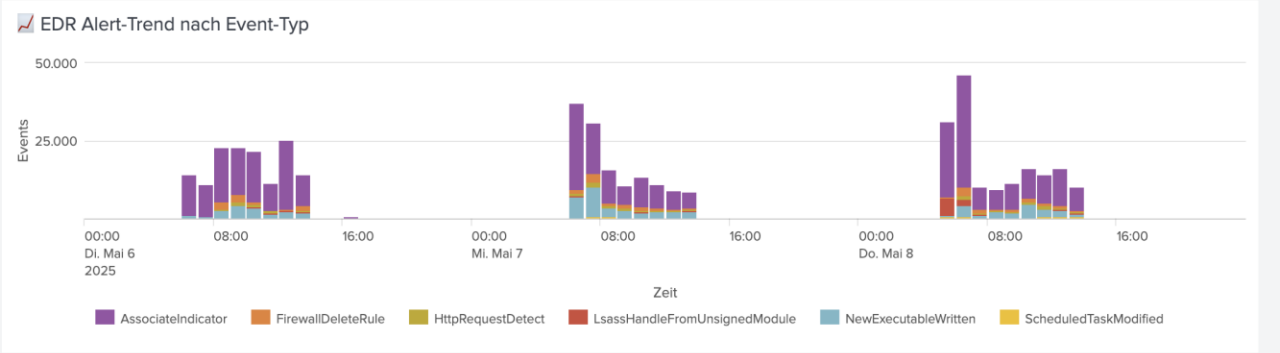
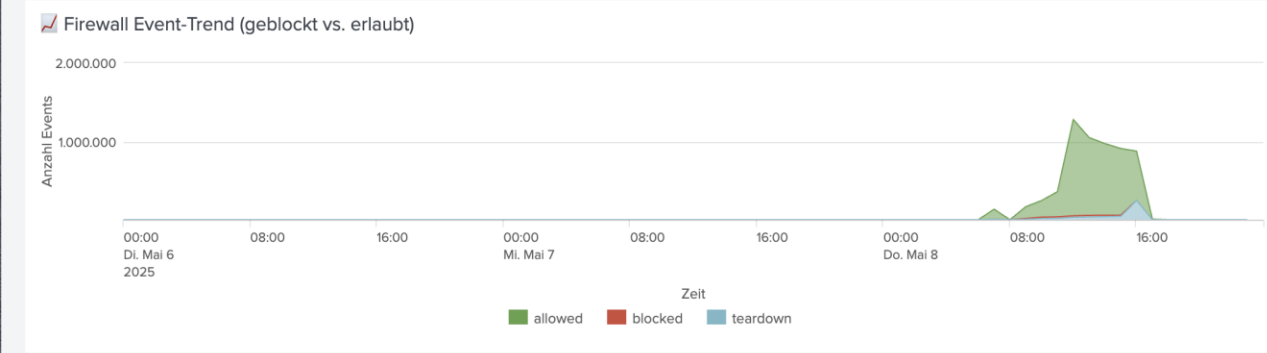
<panel>
  <title>🚒 Firewall Traffic-Volumen nach Dienst</t
itle>
  <chart>
    <search>
      <query>index=firewall_fortigate sourcetype=f
ortigate_traffic
| stats count by service
| sort - count
| head 10
| rename service as "Dienst", count as "Verbindungen"
</query>
    <earliest>$time_range.earliest$</earliest>
    <latest>$time_range.latest$</latest>
    </search>
    <option name="charting.chart">pie</option>
    <option name="charting.legend.placement">right
</option>
    <option name="charting.drilldown">all</option>
    <option name="height">250</option>
  </chart>
</panel>
</row>
</form>
```

SOC Operations Dashboard

Security Operations Center – Tägliche Übersicht | FortiGate Firewall + CrowdStrike EDR

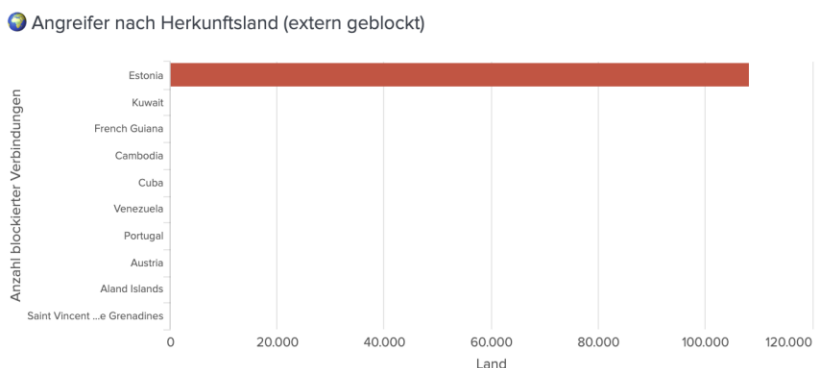
Zeitraum: Mai 6 – 8, 2025 Senden Filter ausblenden

115.980 Gebrockte Verbindungen (FW)	104 IPS Anomalien (UTM)	11.219 LSASS Credential Dump Versuche	26.350 Firewall-Regeln gelöscht (EDR)	143 Betroffene Endpoints (EDR)	10 Externe Angreifer-IPs (Blacklist)
---	-----------------------------------	---	---	--	--



Top Blocked Sources (Firewall)

Quell-IP	Ziel-IP	Port	Dienst	Land	Anzahl
2a07:1182:101::104	2a07:1182:2:f20::17	22	SSH	Estonia	10752
2a07:1182:101::104	2a07:1182:2:f20::13	22	SSH	Estonia	10750
2a07:1182:101::104	2a07:1182:2:f20::11	22	SSH	Estonia	10744
2a07:1182:101::104	2a07:1182:2:f20::14	22	SSH	Estonia	10744
2a07:1182:101::104	2a07:1182:2:f20::15	22	SSH	Estonia	10742
2a07:1182:101::104	2a07:1182:2:f20::19	22	SSH	Estonia	10740
2a07:1182:101::104	2a07:1182:2:f20::16	22	SSH	Estonia	10738
2a07:1182:101::104	2a07:1182:2:f20::5	22	SSH	Estonia	10732
2a07:1182:101::104	2a07:1182:2:f20::12	22	SSH	Estonia	10726
2a07:1182:101::104	2a07:1182:2:f20::18	22	SSH	Estonia	10716
10.2.20.17	196.216.245.213	443	HTTPS	Reserved	1898
100.98.2.33	100.95.95.4	53	DNS	Reserved	440
10.2.13.10	20.91.147.72	443	HTTPS	Reserved	378



IPS / UTM Anomalien Detail

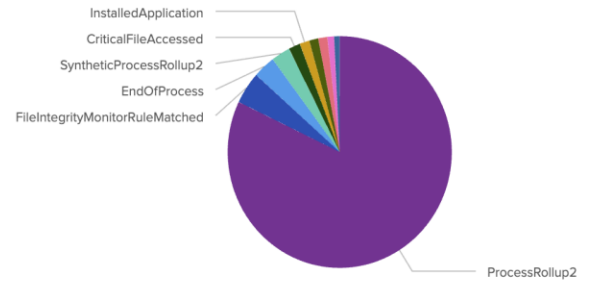
Quell-IP	Ziel-IP	Anomalie-Typ	Ereignisse
100.95.95.2	100.98.2.3	anomaly: udp_src_session, 5001 > threshold 5000, repeats 354 times	4
100.95.95.2	100.98.2.2	anomaly: udp_src_session, 5001 > threshold 5000, repeats 338 times	4
100.100.202.202	100.98.2.8	anomaly: tcp_port_scan, 1001 > threshold 1000, repeats 79 times	2
100.100.202.202	100.98.2.8	anomaly: tcp_port_scan, 1114 > threshold 1000	2
100.100.202.79	100.98.2.13	anomaly: tcp_dst_session, 5001 > threshold 5000, repeats 1219 times	2
100.100.202.79	100.98.2.13	anomaly: tcp_dst_session, 5001 > threshold 5000, repeats 2114 times	2
100.100.202.79	100.98.2.13	anomaly: tcp_dst_session, 5001 > threshold 5000, repeats 2398 times	2
100.100.202.79	100.98.2.13	anomaly: tcp_dst_session, 5001 > threshold 5000, repeats 2929 times	2

Task-Name	Ausführung
RunAsTrustedInstaller_BT_Peng_Hwee	powershell.exe
Microsoft\Windows\Offline Files\Background Synchronization	
MicrosoftEdgeUpdateTaskMachineCore	C:\Program Files (x86)\Microsoft\EdgeUpdate\Mi
MicrosoftEdgeUpdateTaskMachineUA	C:\Program Files (x86)\Microsoft\EdgeUpdate\Mi
Microsoft\Windows\ConsentUX\UnifiedConsent\UnifiedConsentSyncTask	
Microsoft\Windows\Data Integrity Scan\Data Integrity Check And Scan	
Microsoft\Windows\EnterpriseMgmtNonCritical\D2397D24-958F-462A-9E04-41D3484D6CCA\Queued Schedule created for queued alerts	%windir%\system32\deviceenrol
Microsoft\Windows\EnterpriseMgmtNonCritical\7FC05219-AE7A-405A-AD6E-FB44925A63F5\Queued Schedule created for queued alerts	%windir%\system32\deviceenrol
Microsoft\Windows\EnterpriseMgmtNonCritical\D9444A3F-8A36-426B-808F-B5FA290D19A3\Queued Schedule created for queued alerts	%windir%\system32\deviceenrol
Microsoft\Windows\EnterpriseMgmtNonCritical\794EF25E-8D61-489F-AA09-878C832153CB\Queued Schedule created for queued alerts	%windir%\system32\deviceenrol

« Zurück 1 2 3 4 5 6 7 8 Weiter »

Q ⏴ ⓘ ⌂ vor 2 Minuten

Quell-IP	Gelöschte Regeln	Hosts	Benutzer
185.139.252.20	23855	114	ADCS\$ Administrator BEG-ENG-WS\$ BEG-PGS-OPERAT0\$ BEG-POWER-WS\$ DC1\$ DC2\$ FILES\$ LOCAL SERVICE LSAdmin MAIL\$ SP\$ SQL\$ SYSTEM WS1-BAF01\$ WS1-BAF02\$ WS1-BAF03\$ WS1-BAF05\$ WS1-BEG01\$ WS1-BEG02\$ WS1-BEG03\$ WS1-BEG04\$ WS1-BEG05\$ WS1-FHQ01\$ WS1-FHQ02\$ WS1-FHQ03\$ WS1-M36501\$ WS1-M36502\$ WS1-M36503\$ WS2-BAF01\$ WS2-BAF02\$ WS2-BAF03\$ WS2-BAF05\$ WS2-BEG01\$ WS2-BEG02\$ WS2-BEG03\$ WS2-BEG05\$ WS2-M36501\$ WS2-M36502\$ WS2-M36503\$ WS3-M36501\$ WS3-M36502\$ WS3-M36503\$ WS4-M36501\$ t2adm01 t2adm02 t2adm05 t2adm07
185.139.255.2	2431	9	ADFS\$ MAIL\$ WAP\$
2a07:1182:2:22::60	50	1	
185.7.107.104	10	0	DFS\TOP_02\K6000



Troubleshooting

- Im Konfigurationsbereich lässt sich der Verbindungsstatus überprüfen
- Ein Fehler-Log kann zum Troubleshooting verwendet werden
- Zunächst sollte ein Token/Zertifikatsfehler ausgeschlossen werden -> Token expired?
- Andernfalls sollte die Verbindung zur Splunk Instanz überprüft werden
- Der Endpoint des MCP Servers lautet i.d.R. <Splunk URI>/services/mcp

Lokale MCP-Server
Füge MCP-Server hinzu und verwalte sie, an denen du arbeitest.

Config bearbeiten

splunk-mcp-server failed

Befehl
npx

Argumente
-y mcp-remote https://192.168.178.155:8089/services/mcp --header Authorization: Bearer

Fehler
Server disconnected

Logs anzeigen

> Erweiterte Optionen