

NETSCOUT Cyber Threat Horizon

Real-Time DDoS Attack Map

September 9, 2026

13:55:36 (UTC -1hr)

Showing 159 DDoS events



<https://horizon.netscout.com/>

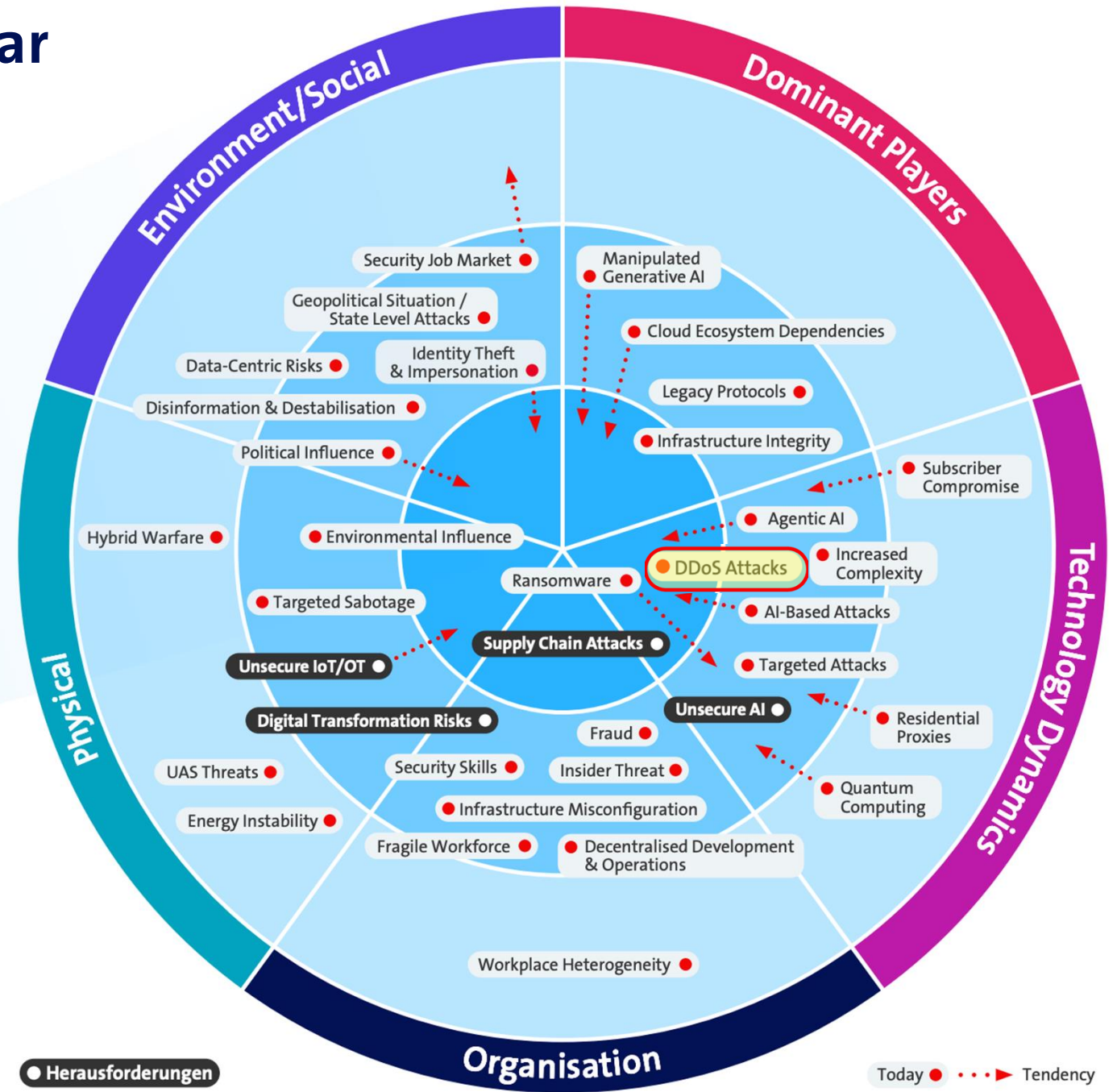
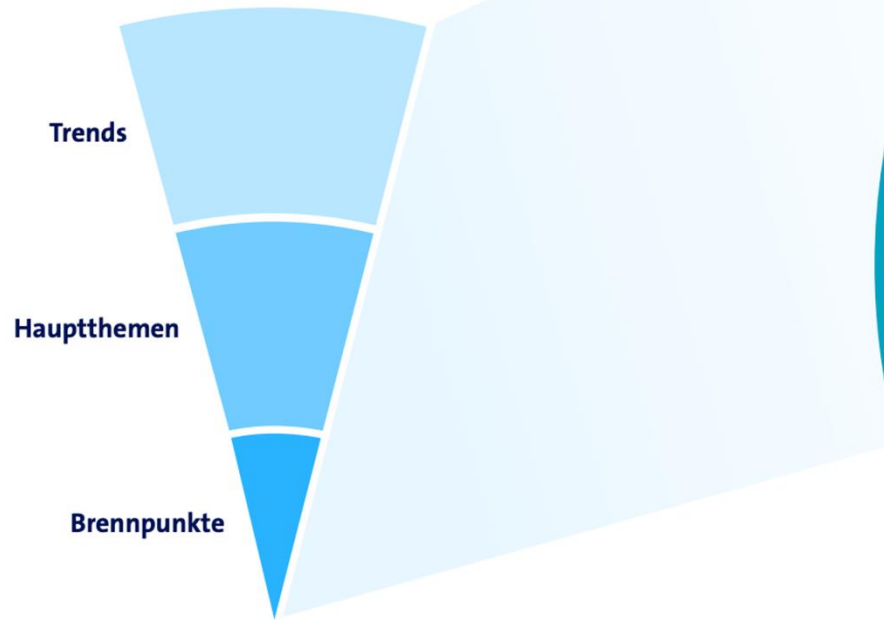
DDoS Schutz - Im Spannungsfeld zwischen Regulierung und Resilienz

September 2026

Patrick Haas, Beat Hunziker, Reto Friedl



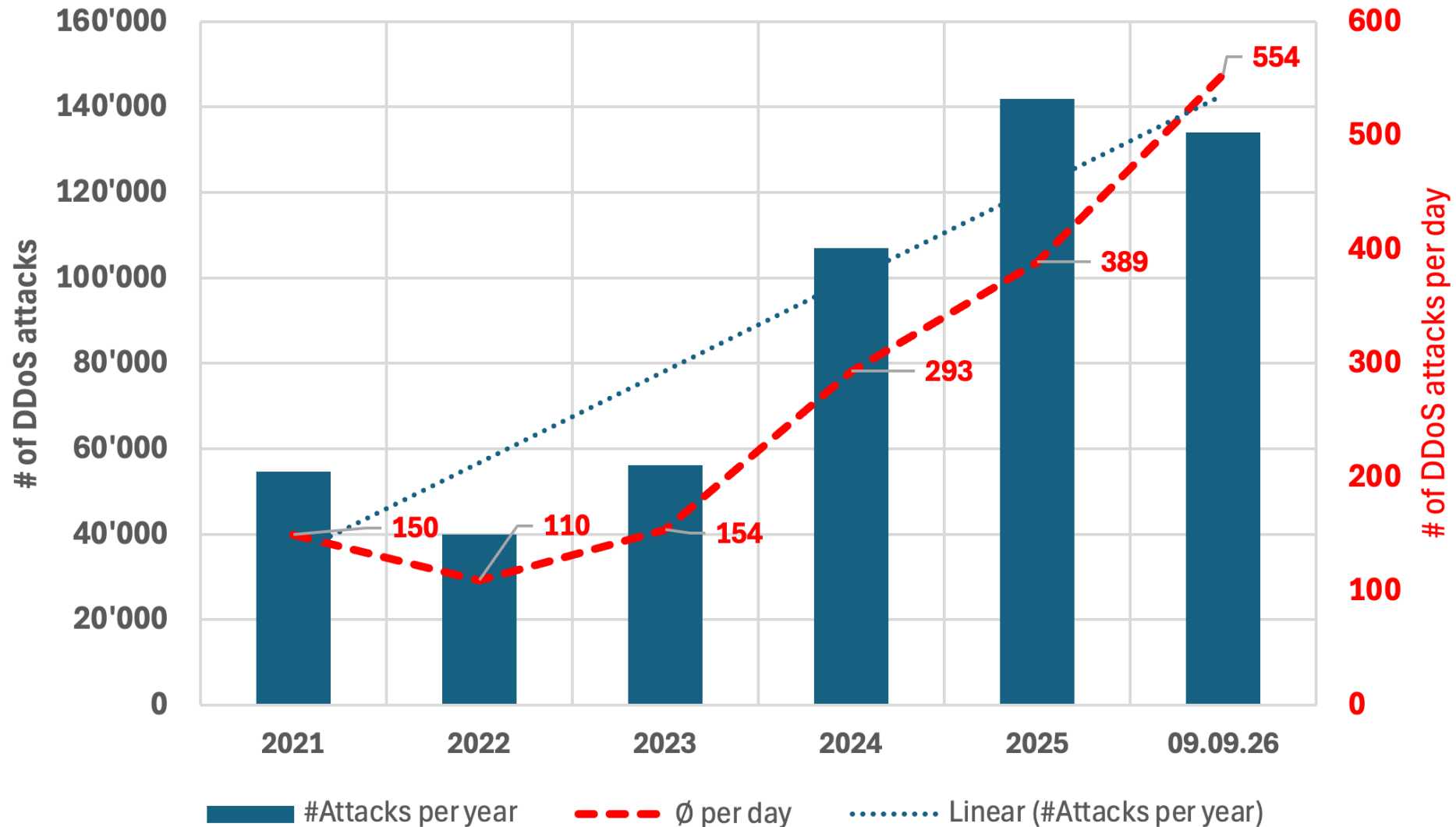
Lagebild - Bedrohungsradar





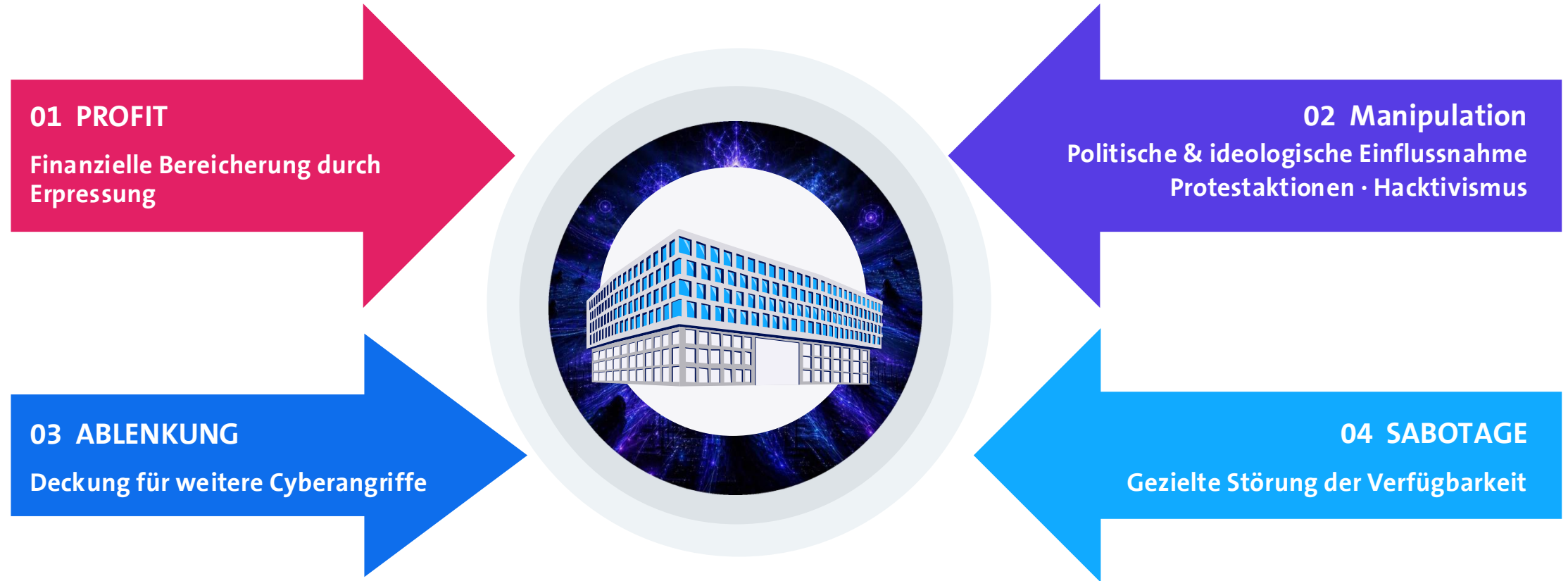
DDoS Attack Trend Schweiz

DDoS Attack Trend Switzerland





Motivation für DDoS-Angriffe





DDoS trifft Wirtschaft, Staat und Gesellschaft

BETROFFENE GRUPPE	TYPISCHE ZIELE	MÖGLICHE FOLGEN
01 Unternehmen	Online-Shops, Banken & Finanzdienstleister Cloud-Anbieter, Gamingplattformen, Streaming-Dienste	• Umsatzausfälle, Imageverlust • Kundenverlust, hohe Wiederherstellungskosten
02 Behörden & öffentliche Einrichtungen	Bund, Kantone, Stadtverwaltungen, Gemeinden, Schulen & Universitäten Gesundheitsdienstleister	• Eingeschränkte öffentliche Dienste • Verzögerte Verwaltungsvorgänge • Gefährdung kritischer Infrastruktur
03 Kritische Infrastruktur	Energieversorger, Telekommunikations- anbieter, Verkehrssysteme, Wasserversorgung	• Störungen wichtiger Dienstleistungen • Gefahr für Sicherheit & Versorgung • Grosse wirtschaftliche Schäden
04 Medien & Soziale Netzwerke	Nachrichtenportale, Social-Media-Plattformen Video-Streaming-Plattformen	• Verbreitung von Desinformation • Kommunikationsausfälle • Verlust von Werbeeinnahmen
05 Privatpersonen	Streamer & Influencer, kleine Webseitenbetreiber, Gamer	• Verlust der Internetverbindung • Sperrung von Diensten • Persönliche & finanzielle Schäden



DDoS-Resilienz verbindet Governance, Schutz und Bereitschaft

01 GOVERNANCE & ANFORDERUNGEN

Regulatorien

- NIS 2 / DORA
- ISO/IEC 27001
- DSGVO / nDSG
- FINMA / BACS

Organisationen

- Bund, Kanton, Gemeinden
- Geschäfts- & Privatkunden
- Partner und Lieferanten
- Kritische Infrastruktur

02 SCHUTZ & MITIGATION

Dienstleister

- Risk - / Business Continuity Management

Managed Security Provider

- Managed Security Services & SOC – 24/7
- Skalierbare Mitigations-Kapazität
- Internet-Backbonekapazität
- Expert DDoS Engineering / SOC Team

03 WIRKUNG & BEREITSCHAFT

Schaden begrenzen

- Service- / Produktionsausfälle
- Finanzielle Verluste
- Reputationsschäden

Betriebsbereitschaft

- Business Continuity Management
- Incident Workflow
- Manager on Duty
- Stresstest

Resilienz • Meldepflicht • Bussen

Reagieren • Lernen • Verbessern



DDoS-Angriffsmuster wirken auf unterschiedlichen Ebenen

Auszug der aktuell häufigsten Attack - Muster

01 BANDBREITE & INFRASTRUKTUR



UDP Flood

UDP-Pakete überlasten Bandbreite und Infrastruktur.



DNS Amplification

Offene DNS-Server verstärken den Antwortverkehr.

02 PROTOKOLL & RESSOURCEN



SYN Flood

TCP-Handshakes erschöpfen Serverressourcen.

03 ANWENDUNG & API



HTTP/HTTPS Flood

Legitime Webanfragen überlasten Anwendungen und APIs.

EBENENÜBERGREIFENDE

TAKTIKEN



Multi-Vektor-Angriff

Kombiniert mehrere Techniken, um Schutzmassnahmen zu umgehen.



Carpet Bombing

Greift einen IP-Bereich oder ein gesamtes Netzwerk parallel an.

Techniken werden kombiniert oder auf ein breites Zielgebiet verteilt.

-> Schutz muss Angriffsebene und Zielbreite gleichzeitig abdecken.

Cyberkrieg im Alltag

DDoS Angriff – Auswirkungen ...

DDoS-Attacke auf Deutsche Bahn: Verwundbarkeit auf offener Strecke

19. Februar, 2026 10:03

Störungen bei App und Webseite

DDoS-Angriff schränkt Buchungssystem der Deutschen Bahn massiv ein

19.02.2026 · Quelle: dpa · 3 min Lesedauer ·

Störungen bei Navigator und bahn.de

Bahn macht Cyberangriff für IT-Probleme verantwortlich

Seit Dienstag kommt es zu Störungen mit Auskunfts- und Buchungssystemen der Deutschen Bahn. Jetzt meldet der Konzern, dass dahinter ein Cyberangriff steckt.

18.02.2026, 15.01 Uhr

NACH DDOS-ATTACKE

Hacker haben nicht nur die Deutsche Bahn im Visier

Von Stephan Finsterbusch, Maximilian Sachse 19.02.2026, 14:56 Lesezeit: 4 Min.

DDOS-ANGRIFF AUF DEUTSCHE BAHN

War das wirklich Russland?

Eine DDoS-Attacke trifft die Deutsche Bahn – und sofort wird Russland verdächtigt. Doch damit machen wir uns die Sache zu einfach.



DDoS for Hire - Automatisierung & Künstliche Intelligenz “KI”

DDoS Automatisierung

Set Source IP by ISP

Select the ISP for source IPs to be set.
If you need another ISP not listed below, click on the "New Method" button.

✓ Rand
Valve
China-Telecom
Microsoft
Sony
Google
Akamai
Hetzner
Comcast
Cloudflare
Voxility
OVH
NFO
Reserved

Schedule Layer 4 Attack

Enter your attack settings in the attack hub, and then come back to this window by clicking on the "Schedule" button.
Once scheduled, attacks will immediately start executing using the settings below.
If auto-renew is enabled then it will not stop until you **delete** the scheduled attack or the attack is manually stopped.

Attack Settings Review

Attack Type: [Layer 4](#)
Destination IPs/Subnets: None : 0
Method: TCP-REFLECT (TCP AMP) ★
Attack Duration: 120 Seconds
PPS (Packets per Second): 100%
Simultaneous Attacks: 1
Source IPs/Subnets: Default : Default
Origin Country Codes (AMP Only): ALL
TCP Flags: syn
TCP Options: None : 4 Attack (Automatic Attacks)
Payload: Default

Schedule Settings

Initial Execution Delay (seconds):
0
The initial attack will start after the specified delay has been reached (useful for testing).
☒ Re-Execute
Re-Execution Delay (seconds):
3600
If enabled the attack will be re-executed after the specified delay has been reached (useful for testing).

Up to /24

Host: 127.0.0.1
Port: 80
Time: 45
Method: DNS [DNS Amplification]
Concurrents: 1
Schedule Attack

Send Attack



DDoS heute: KI und Large Language Modelle “LLMs”

The screenshot shows a web-based control panel for DDoS attacks. The top navigation bar includes links for Dashboard, Attack Panel (highlighted), Graph, Deposit, Store, Invoices, Referral, API Documentation, and Terms of services. The main interface is divided into two sections. On the left, there are configuration options: Layer 7 (selected), Host (https://example.com/), Time (a slider from 0 to 60), Subnet (Ex: 24), and Method (a dropdown menu). The Method dropdown is open, showing a list of attack types under the heading 'Hypertext Transfer Protocol (HTTP/S)': HTTP2-FLOODER - Unavailable, HTTP1-FLOODER - Unavailable, AI-BYPASS - Unavailable, HTTP-CLOUDFLARE - Unavailable, HTTP-KOREA - Unavailable, HTTP-CHINA - Unavailable, and HTTP-BOSSITA - Unavailable. On the right, there are buttons for 'Recent Attacks' and 'Schedule Attacks'. Below these buttons, a message states 'No data available.' with an information icon. At the bottom right of the panel, there is a 'Customer Support' chat window with a message: 'Hi! How can we h...'

The screenshot shows a Telegram chat interface. At the top, the chat header reads '[redacted].net | StressTesting'. The message history includes a greeting 'Hello everyone!' and a longer announcement: 'We are happy to announce that the development of our AI assistant called QueryAI-1.0 is fully completed. You can already ask a couple of questions in our bot @ [redacted] SupportBot using the command «/helpme Hello», where Hello is your question. The assistant will be happy to answer any questions regarding [redacted] and our services. Our AI assistant can also answer other questions, but in a limited way so as not to create a heavy workload. Try it out now!'. A 'Customer Support' chat bubble is visible at the bottom of the chat history.

219% Zunahme Angebote böstiger KI-Tools

\$60-\$200 Dark-web LLMs Angebote / pro Monat



KI-gestützte und Chatbot-gesteuerte Koordination

Von automatisierten zu intelligenten DDoS-for-hire-Operationen

Echtzeit-Schwachstellenanalyse

KI analysiert kontinuierlich den Netzwerkverkehr, um Schwachstellen in den Abwehrmechanismen zu identifizieren und Angriffe gezielt auf diese kritischen Punkte auszurichten.

Intelligente Angriffskoordination

KI ist in der Lage, groß angelegte Angriffe über mehrere Vektoren hinweg zu orchestrieren und gleichzeitig sowohl das Netzwerk- als auch Anwendungen zu überlasten.

Täuschend realistische Datenverkehrsgenerierung

Durch Nachahmung legitimer Verkehrsmuster und dynamischer Anpassung von Angriffsmethoden kann KI Sicherheitsbarrieren umgehen und die Erkennung durch traditionelle, statische Abwehrsysteme effektiv verhindern.

Autonome Botnet-Steuerung

Moderne Botnets nutzen KI, um kompromittierte Geräte automatisiert zu identifizieren, zu rekrutieren und für Angriffe zu koordinieren – ohne menschliches Eingreifen

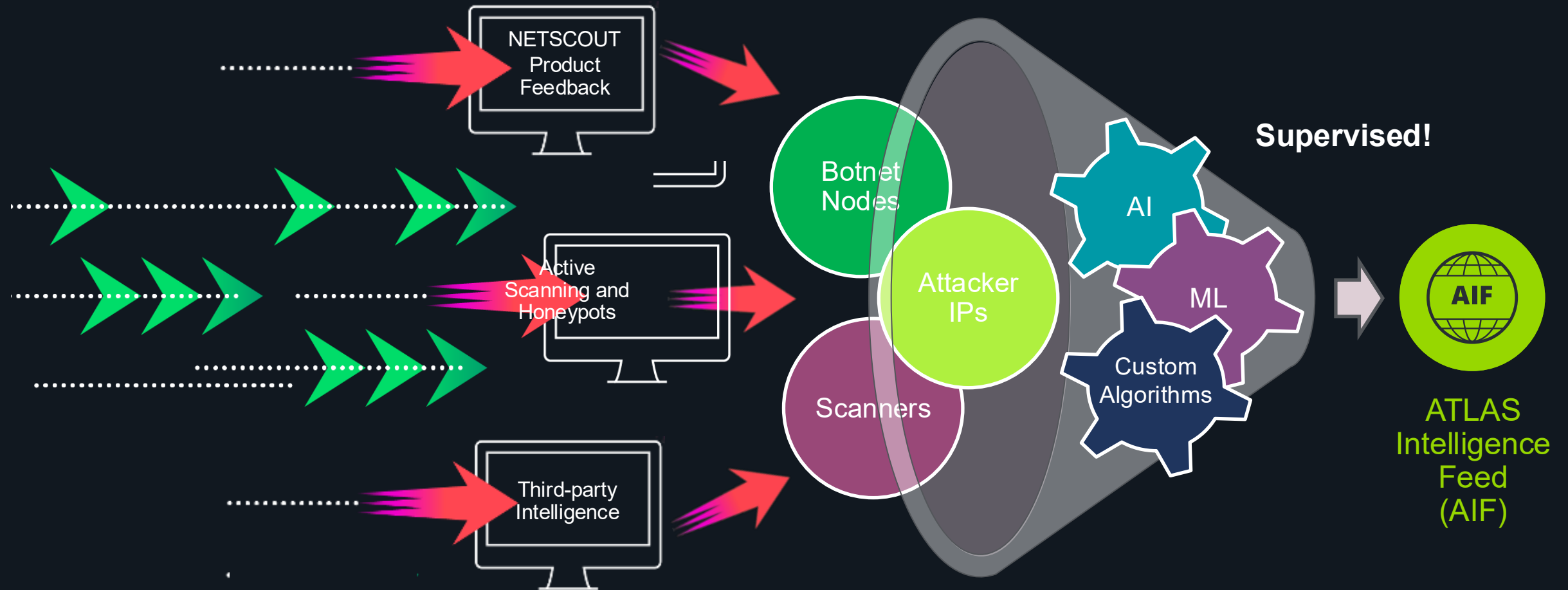
Smarter Targeting and Timing

KI-Systeme analysieren Muster der Netzwerkaktivität, um den besten Zeitpunkt für einen Angriff zu ermitteln – beispielsweise während der Hauptgeschäftzeiten oder Systemwartungsfenstern.



ATLAS Collection and Processing

AI / ML Enables Accuracy And Automated Updates on Massive Data Collection



DDoS Schutz für jedes Unternehmen

Vom Managed Service bis zum eigenständigen Betrieb



Managed Service

Vollumfänglich betreut durch Swisscom



Hybrider Schutz

OnPrem in Kundenverantwortung,
Swisscom im Hintergrund



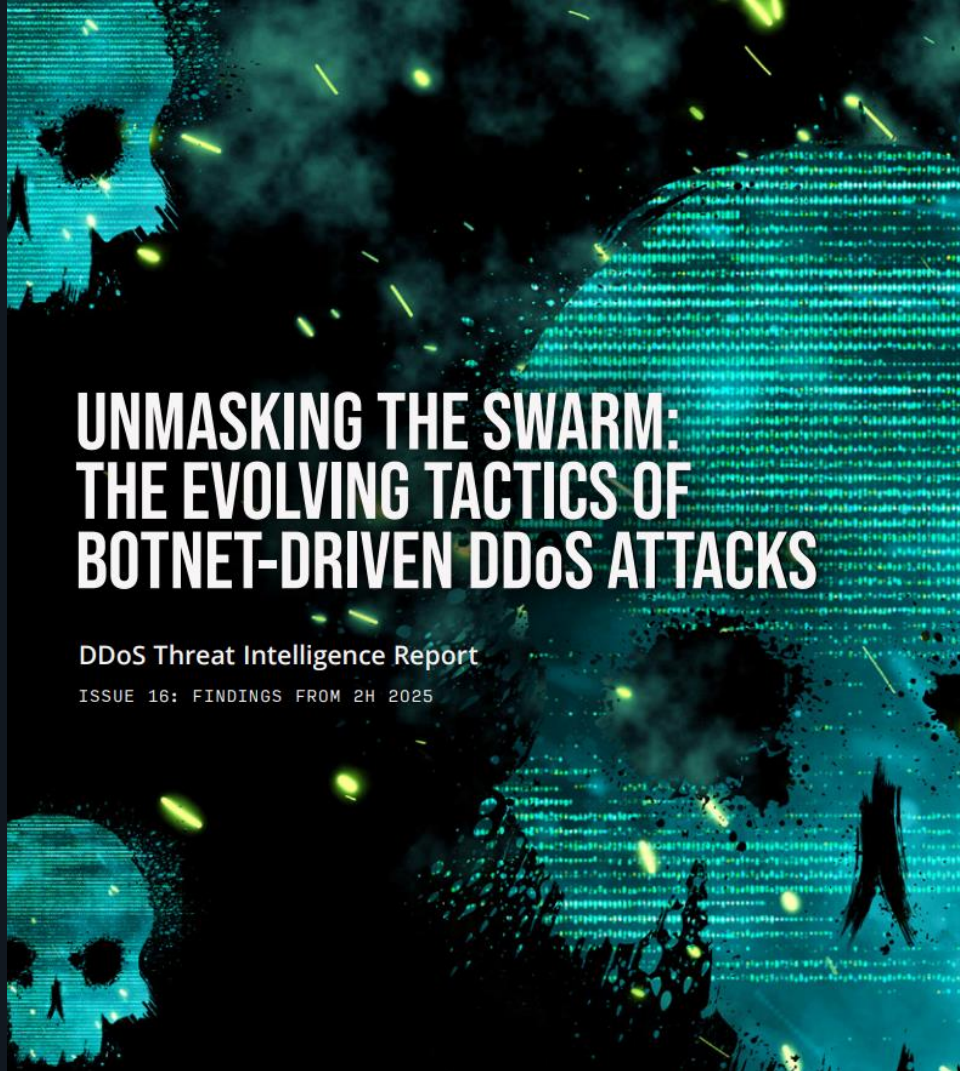
Autarker Betrieb

Provider unabhängig

Überwacht und geschützt durch die Profis von Swisscom und NETSCOUT.



Resources 1/2



NETSCOUT DDoS Threat Intelligence Report:

<https://www.netscout.com/threatreport/>

NETSCOUT Real-Time-Monitor – global DDoS Attacks:

<https://horizon.netscout.com/>

NETSCOUT “Threat Hunting” Blog:

<https://www.netscout.com/asert>

next layer DDoS Protection:

<https://www.nextlayer.at/de/produkte/netzwerk/ddos-schutz>





Ressources 2/2

DDoS-Angriffe als IT-Sicherheitsrisiko

<https://www.swisscom.ch/de/business/enterprise/downloads/security/181120-sy-whitepaper-ddos.html#>

Mit DDoS Protection die Verfügbarkeit sicherstellen

<https://www.swisscom.ch/de/business/enterprise/angebot/security/network-and-cloud-security/ddos-protection.html>

Bundesamt für Cybersecurity – Lagebericht

<https://www.bacs.admin.ch/de/hjb-26-de1>





Kontakt Informationen



Patrick Haas

Regional Director DACH, NETSCOUT

Mobile: +49 171 232 11 21

[netscout.com](https://www.netscout.com)



Beat Hunziker

Senior Product Manager, Swisscom

Mobile: +41 79 634 40 41

[swisscom.ch/DDoS](https://www.swisscom.ch/DDoS)