BOTNET RELOADED

AGENDA

LINK11

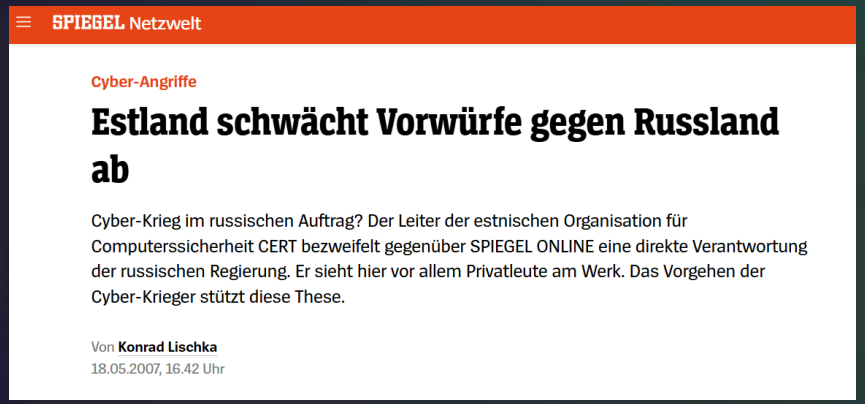
1 **Evolution** der DDoS-Bedrohung
2 **Womit** wir es heute zu tun haben
3 **Was** moderne Erkennung leisten muss

Evolution der DDoS-Angriffe

Was als digitale Randnotiz begann, bedroht heute Unternehmen, KRITIS und Staaten

LINK11

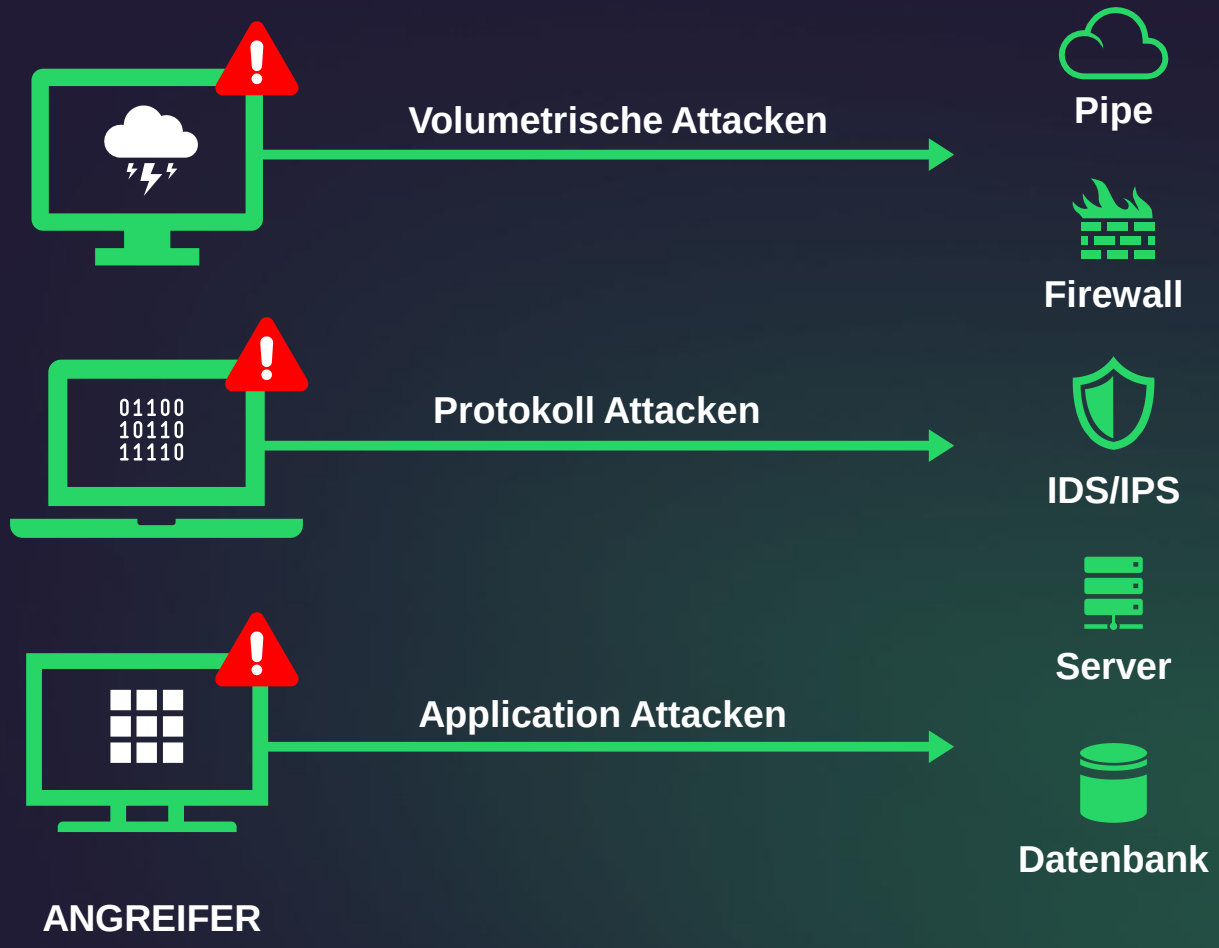
1996 — 2000 — 2007 — 2016 — 2025



Verschiedene DDoS-Angriffstypen

Vom Schraubenschlüssel zum Vorschlaghammer

LINK11



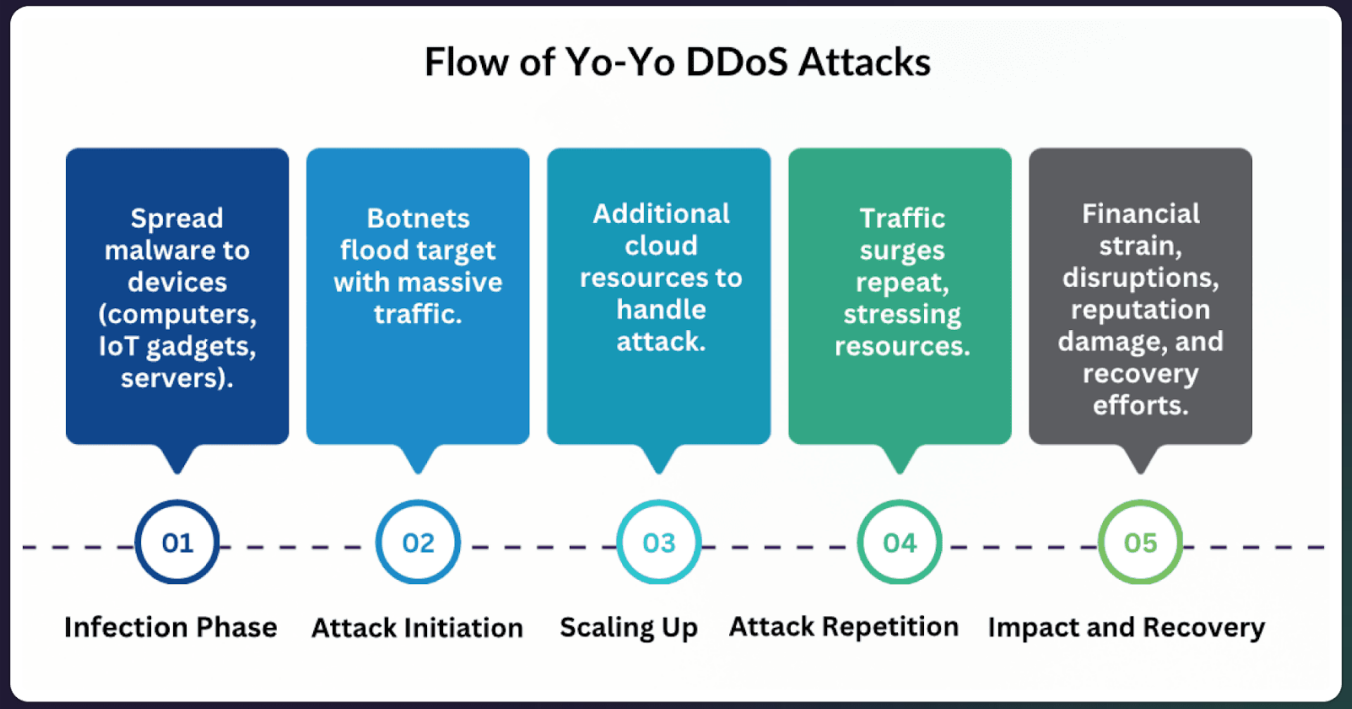
Evolution der DDoS-Angriffe

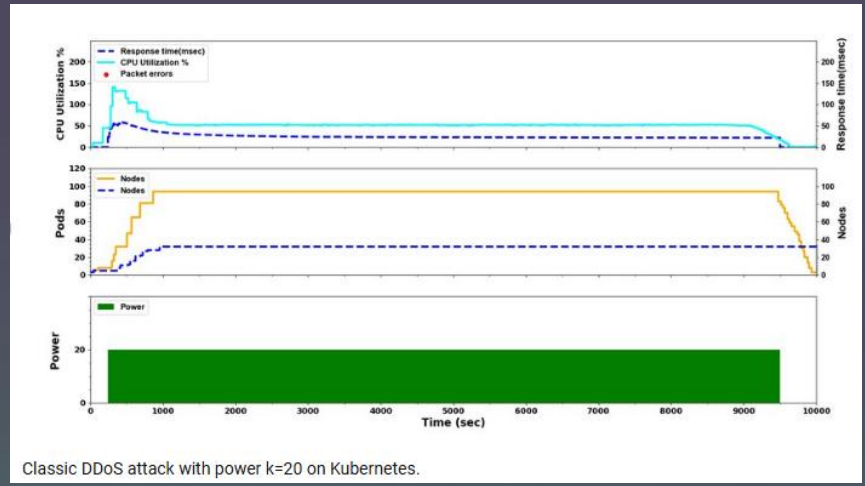
Mehr als nur Hochvolumenattacken

	„Website-Killer“	„ISP-Killer“	Nuisance Attack	Carpet-Bombing	Jo-Jo-Angriff
Primäres Ziel	Einzelne Website oder einzelner Server	Uplink-Kapazität eines gesamten ISPs oder Rechenzentrums	Performance-Störung ohne vollständigen Ausfall	Breite Störung ganzer Subnetze oder IP-Bereiche	Cloud-Infrastruktur mit Auto-Scaling-Funktion
Technische Schwelle	85 % Auslastung, d. h. ca. 850 Mbit/s (bei 1 Gbit/s Anbindung)	85 % Auslastung, d. h. ca. 85 Gbit/s (bei 100 Gbit/s Backbone)	Ab 50 Mbit/s bis 1 Gbit/s, unter Abwehrschwellen	Abhängig vom Zielnetz, oft mittlere bis hohe Gesamtvolumina	Bereits mittlere Lastspitzen reichen, wenn Auto-Scaling ausgelöst wird
Angriffsvolumen	Mittel	Sehr hoch	Niedrig	Mittel bis hoch (verteilt)	Variabel, oft in Wellen mit wechselnder Intensität
Typische Wirkung	Zielseite nicht erreichbar	Großflächiger Ausfall vieler Dienste/Kunden	Spürbare Latenz, Paketverlust, Zusatzkosten	Überlastung von Firewalls, Routern und Upstream-Links	Instabilität durch permanentes Hoch- und Runterskalieren, Kostenexplosion
Merkmale	Gezielter Angriff, relativ geringer Datenstrom	Hochvolumige, verteilte Kampagnen	Häufige Mini-Angriffe, oft automatisiert	Verteilter Traffic auf viele Ziele, schwerer zu filtern	Wechsel zwischen Traffic-Bursts und Ruhephasen, nutzt Cloud-Auto-Scaling aus

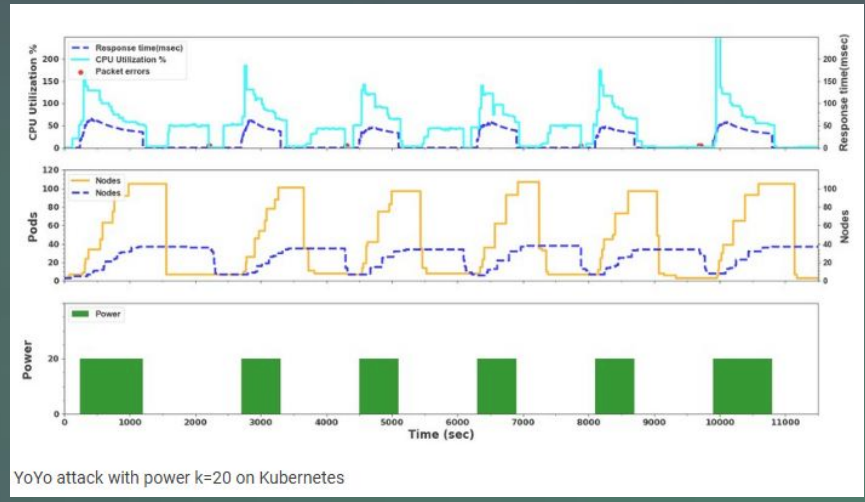
Evolution der DDoS-Angriffe

Wenn Cloud-Skalierung zum Ziel wird





Classic DDoS attack with power k=20 on Kubernetes.



YoYo attack with power k=20 on Kubernetes

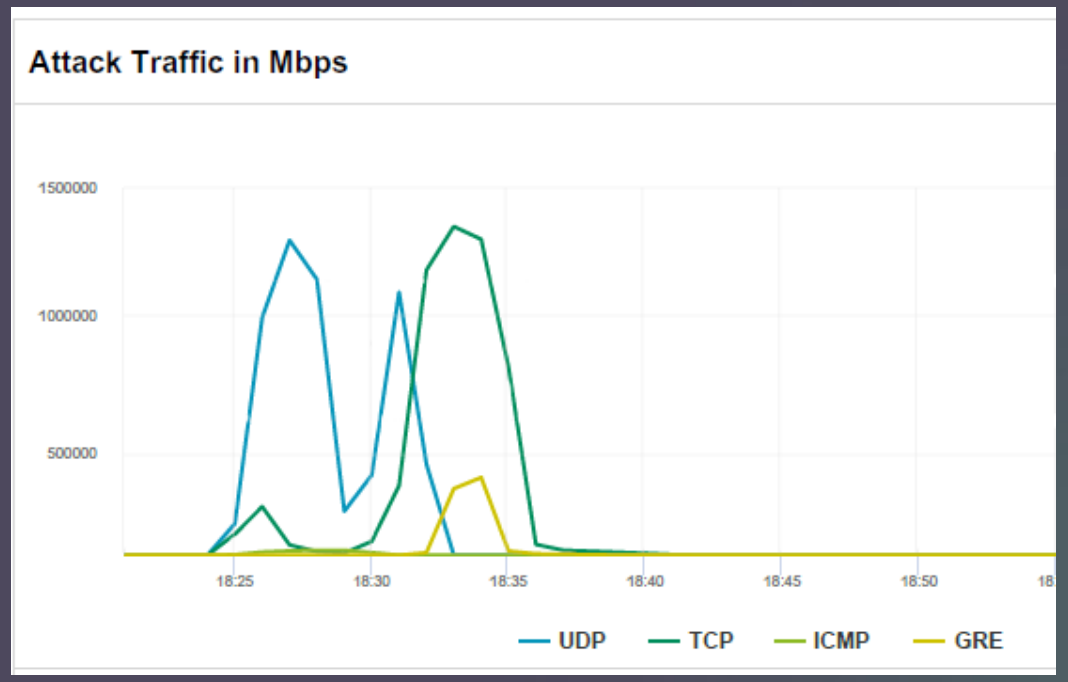
Quelle: Kubernetes Autoscaling: YoYo Attack Vulnerability and Mitigation, Emerging Threat: Yo-Yo DDoS Attacks Targeting Cloud Environments | Blogs - Cyberware Hub

AGENDA

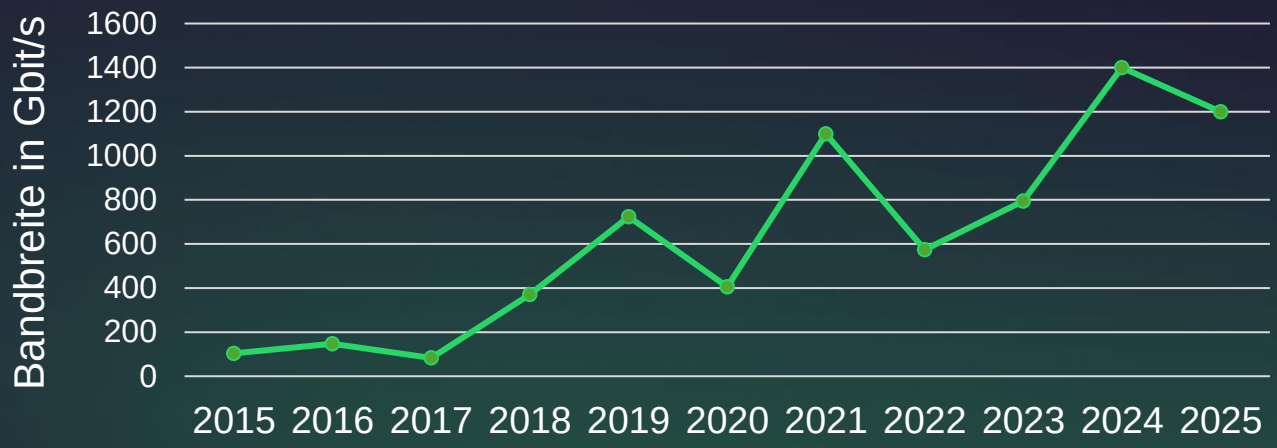
1 Evolution der DDoS-Bedrohung
2 **Womit wir es heute zu tun haben**
3 Was moderne Erkennung leisten muss

Womit wir es heute zu tun haben

Massiver DDoS-Angriff mit 1,4 Tbit/s – simple, aber effektive Angriffsmethode

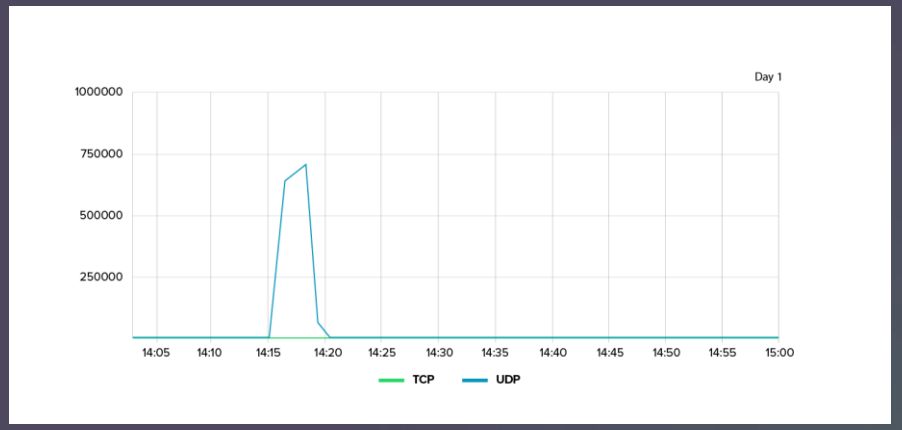


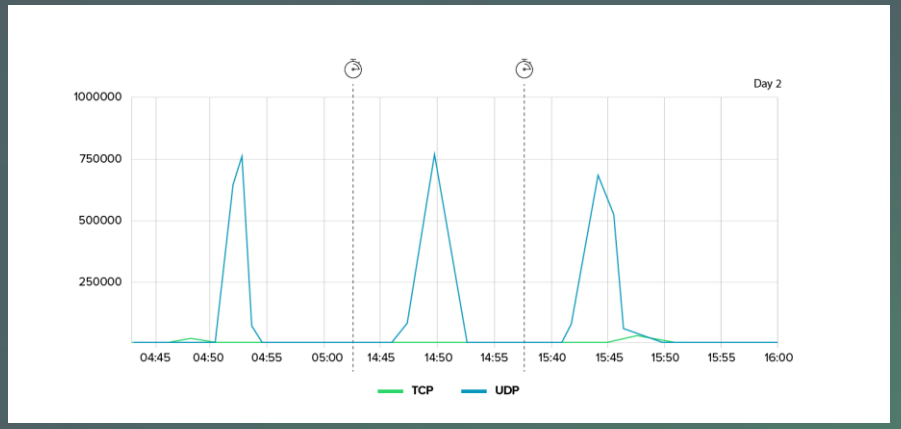
Entwicklung der Bandbreite



Womit wir es heute zu tun haben

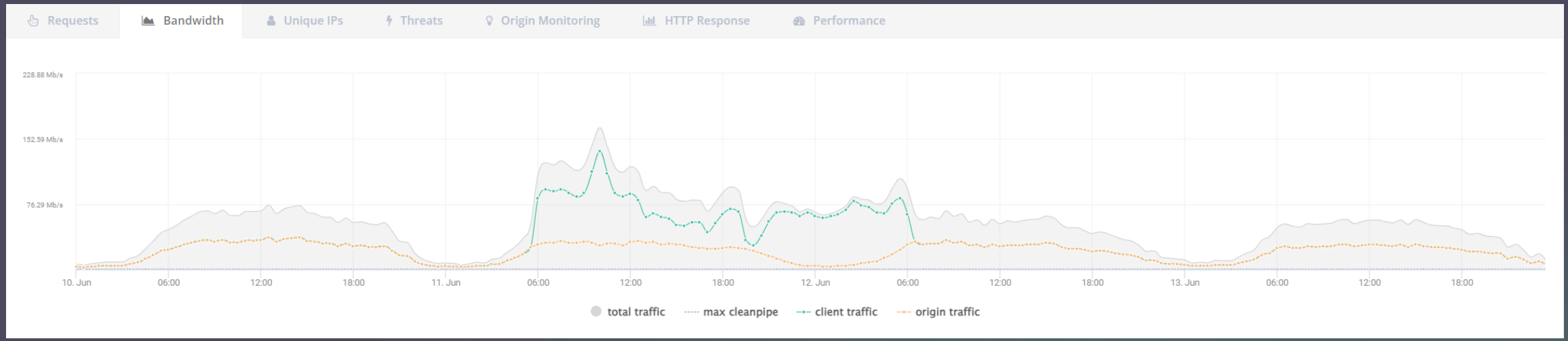
Gezielt gestaffelt statt dauerhaft überlastet.





Womit wir es heute zu tun haben

Cybercrime-as-a-Service: DDoS-Angriffe auf Bestellung



HTTP Protocol Challenge	
Missing	8.065.013
Invalid	106.036
Vallid	6.121.422

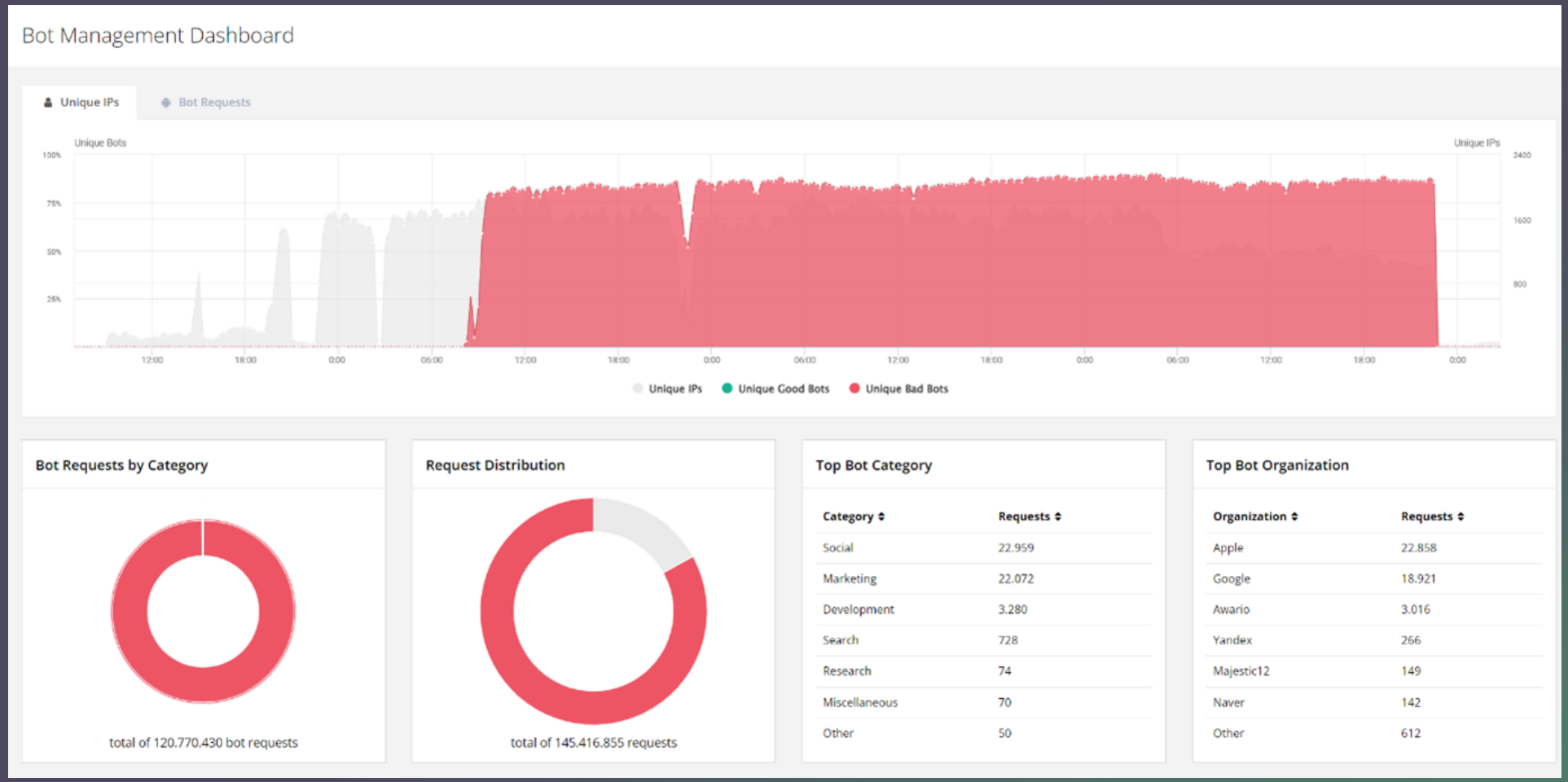
Captcha Challenge (Mitigation rate: 96.01%)	
Started	115.259
Unanswered	110.655
Failed	140
Valid	4.604

Womit wir es heute zu tun haben

Gezielte Überlastung von Netzwerk und Anwendungen – Hybrider Layer-3/4- und Layer-7-Angriff

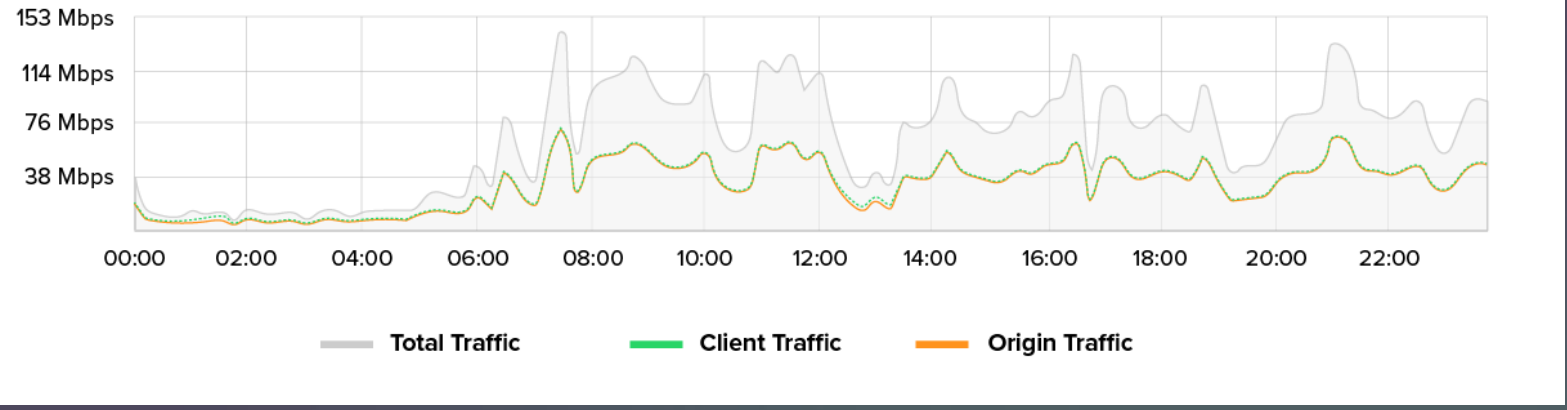
Womit wir es heute zu tun haben

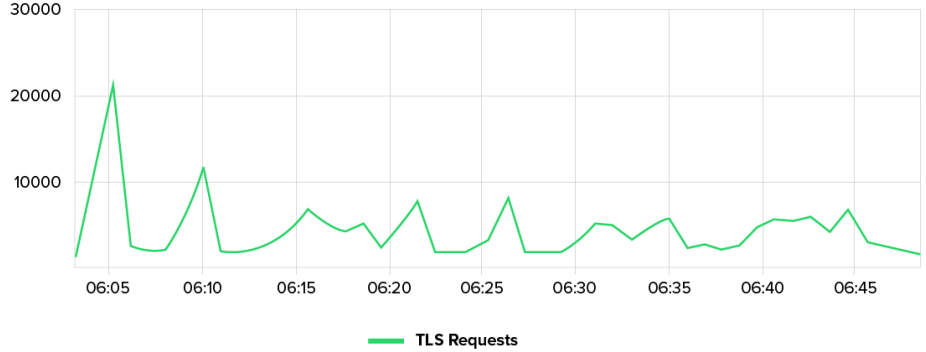
Botnetze schlafen nicht – und sie lernen schnell



Womit wir es heute zu tun haben

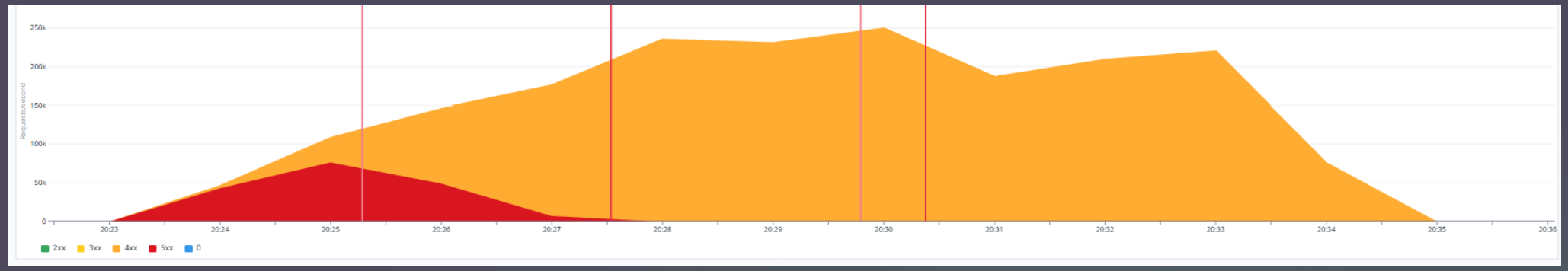
Layer-7-DDoS mit Fokus auf Tarnung

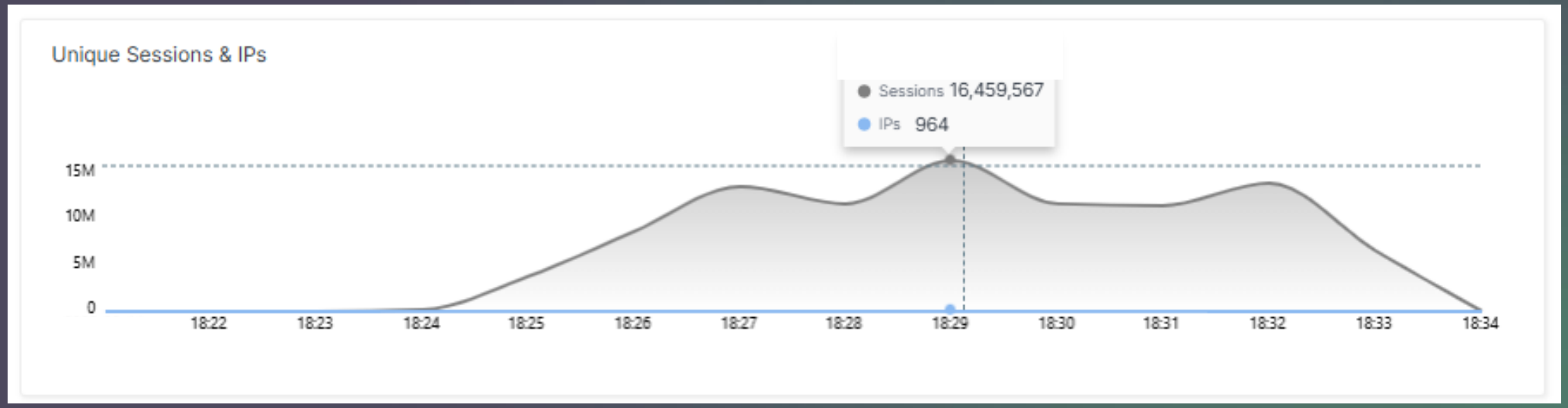




Womit wir es heute zu tun haben

Millionen scheinbar legitimer Anfragen – täuschend echt und ressourcenintensiv



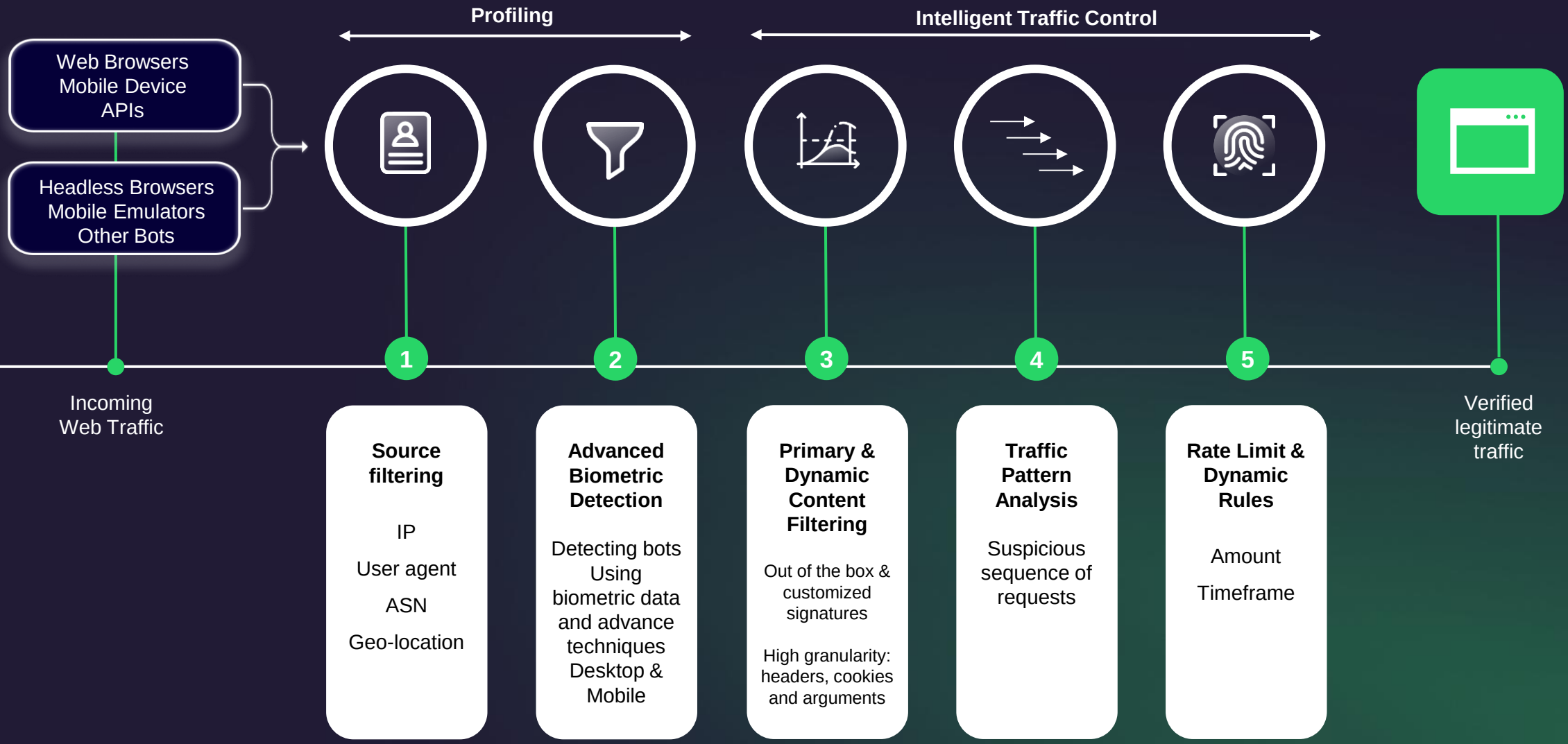


AGENDA

1 Evolution der DDoS-Bedrohung
2 Womit wir es heute zu tun haben
3 Was moderne Erkennung leisten muss

Was moderne Erkennung leisten muss

Systeme, die lernen, können Angriffe erkennen, bevor sie eskalieren



Fazit – Erkennen. Lernen. Handeln.

Blackholing war gestern. Heute entscheiden Präzision und Geschwindigkeit

Klassische Systeme reichen nicht mehr aus

KI erkennt, was wir nicht mehr sehen

NIS-2 macht Reaktionsfähigkeit zur strategischen Pflicht

VIELEN DANK!

Lisa Fröhlich

Unternehmenssprecherin
l.froehlich@link11.com

LINK 11

FOLLOW
THE WHITE
RABBIT

The IT-Security Podcast

Spotify