Officium

Információbiztonság mint stratégiai kockázat és/vagy versenyelőny

NMHH, EIVOK-77 tudományos szakmai konferencia

Hogyan váljunk védhetővé a DDoS-támadások ellen?

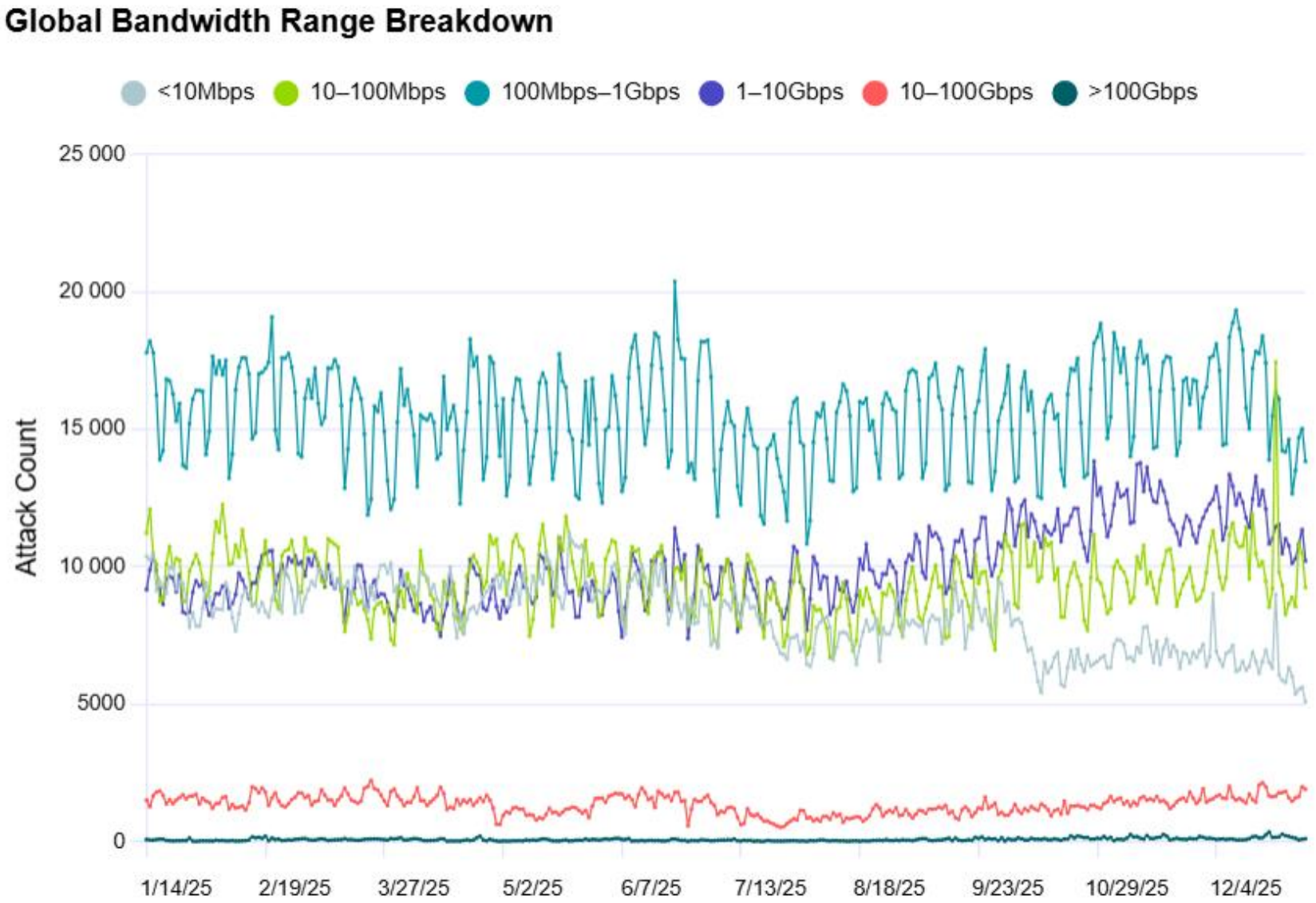
Hankó Péter

ICT Architect

hanko.peter@officium.hu

Statisztika – sávszélesség

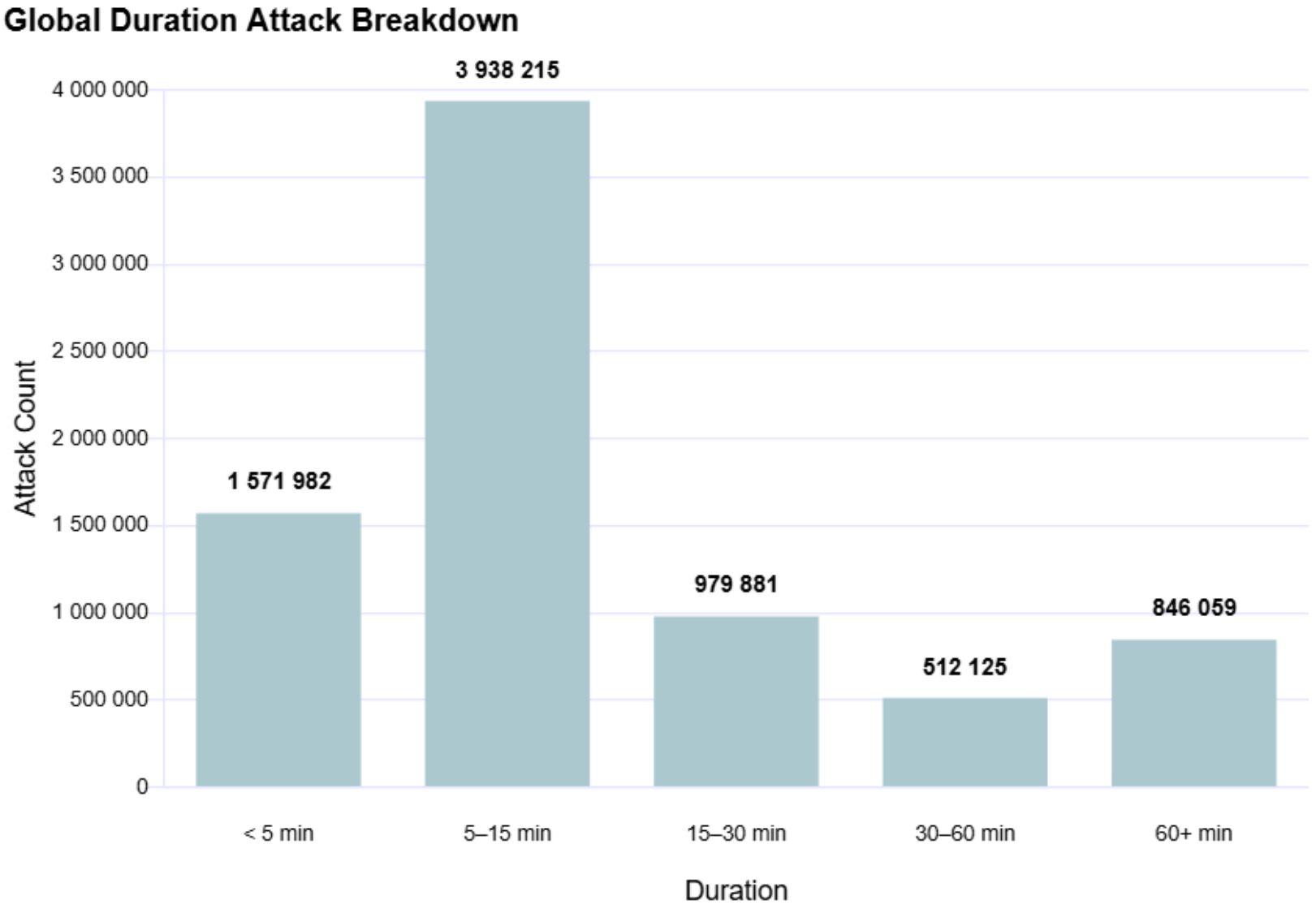
TurboMirai
Aisuru
30 Tbps / 4 Gpps



BANDWIDTH BY PERCENTAGE	
<10Mbps	16.5%
10–100Mbps	21.04%
100Mbps–1Gbps	35.04%
1–10Gbps	24.44%
10–100Gbps	2.79%
>100Gbps	0.19%

Source: Netscout DDoS Threat Intelligence Report, Issue 16: 2H 2025

Statisztika – időtartam

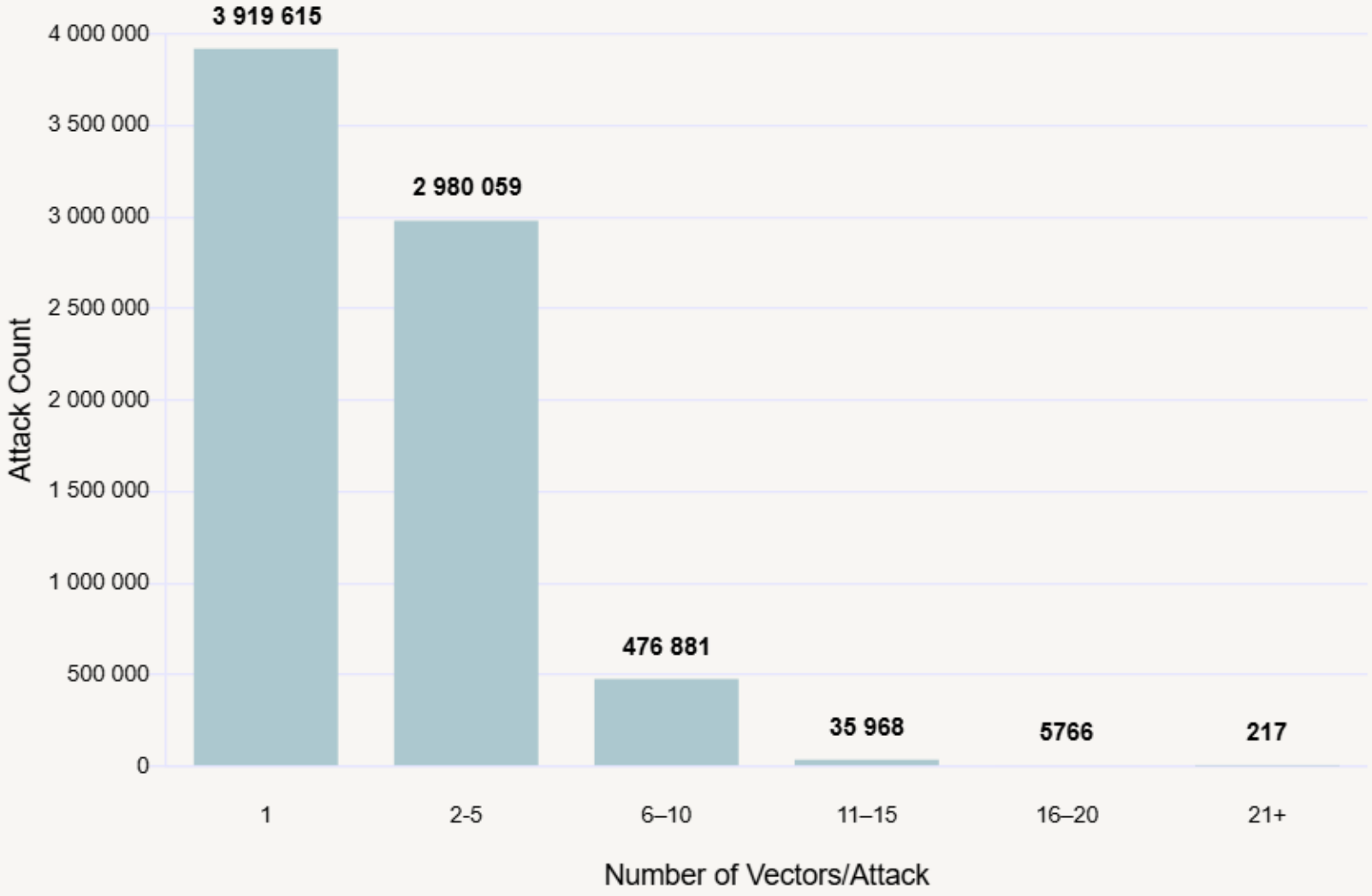


Sok kisebb támadási ciklusból álló kampányok

DURATION BY PERCENTAGE	
< 5 min	19.88%
5-15 min	49.79%
15-30 min	12.39%
30-60 min	6.48%
60+ min	10.7%

Source: Netscout DDoS Threat Intelligence Report, Issue 16: 2H 2025

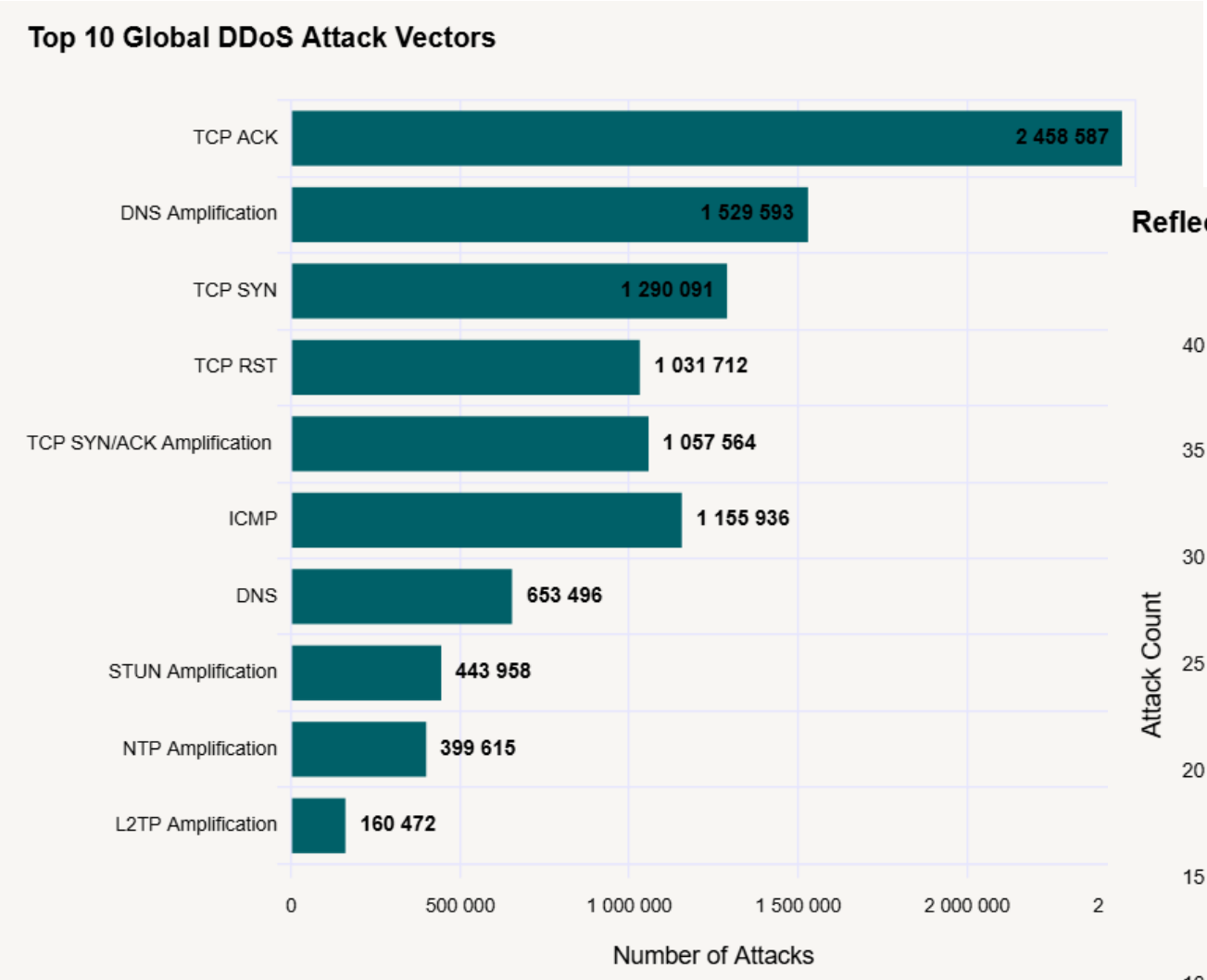
Statisztika – multivektoros támadások

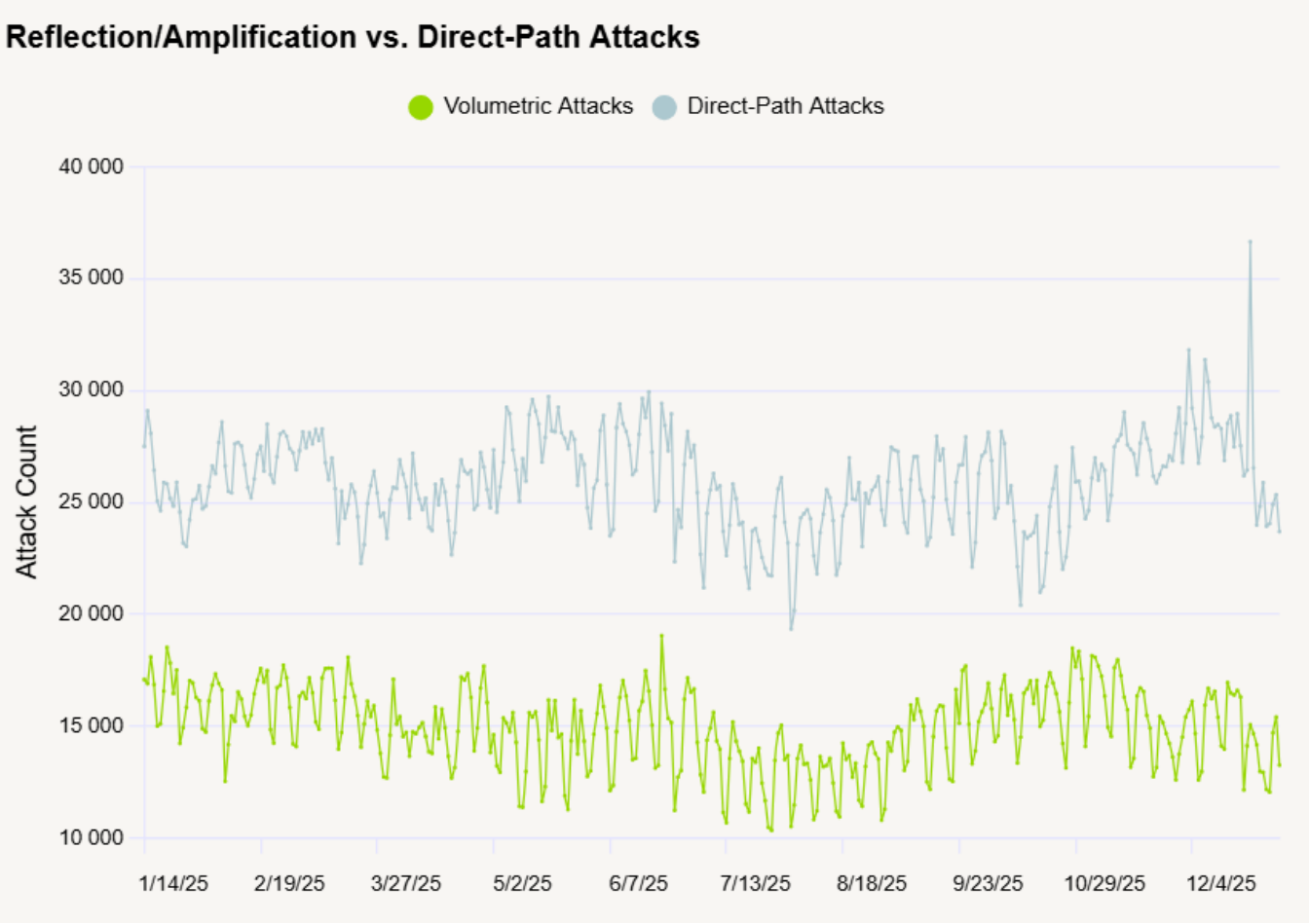


VECTORS BY PERCENTAGE	
1 Vector	48.76%
2–5 Vectors	42.06%
6–10 Vectors	8.08%
11–15 Vectors	0.8%
16–20 Vectors	0.28%
21+ Vectors	0.04%

Source: Netscout DDoS Threat Intelligence Report, Issue 16: 2H 2025

Statisztika – Top 10 támadástípus





Source: Netscout DDoS Threat Intelligence Report, Issue 16: 2H 2025

Néhány újabb fejlemény

Kifinomult támadások

- AI integráció: LLM és chatbotok révén szöveges utasításokkal indíthatók komplex támadások – a szükséges technikai tudás drasztikusan csökkent
- hatékony erőforrásgazdálkodás – csak a szükséges mértékű támadói kapacitás
- üzletileg kritikus időszakokra időzített támadások
- célzott alkalmazásszintű támadások
- DDoS detektálási és mitigációs mechanizmusok kijátszása

Ugrásszerű botnet kapacitásbővülés

- A TurboMirai variánsok akár több tíz Tbps kapacitású támadásokra képesek, ami a szolgáltatói hálózatokra is kockázatot jelent

Infrastruktúrára irányuló támadások

- telekommunikációs szolgáltatók veszélyeztetése
- alapszolgáltatások (DNS, NTP) elleni támadások
- carpet bombing

Mit értünk DDoS-védelem alatt?

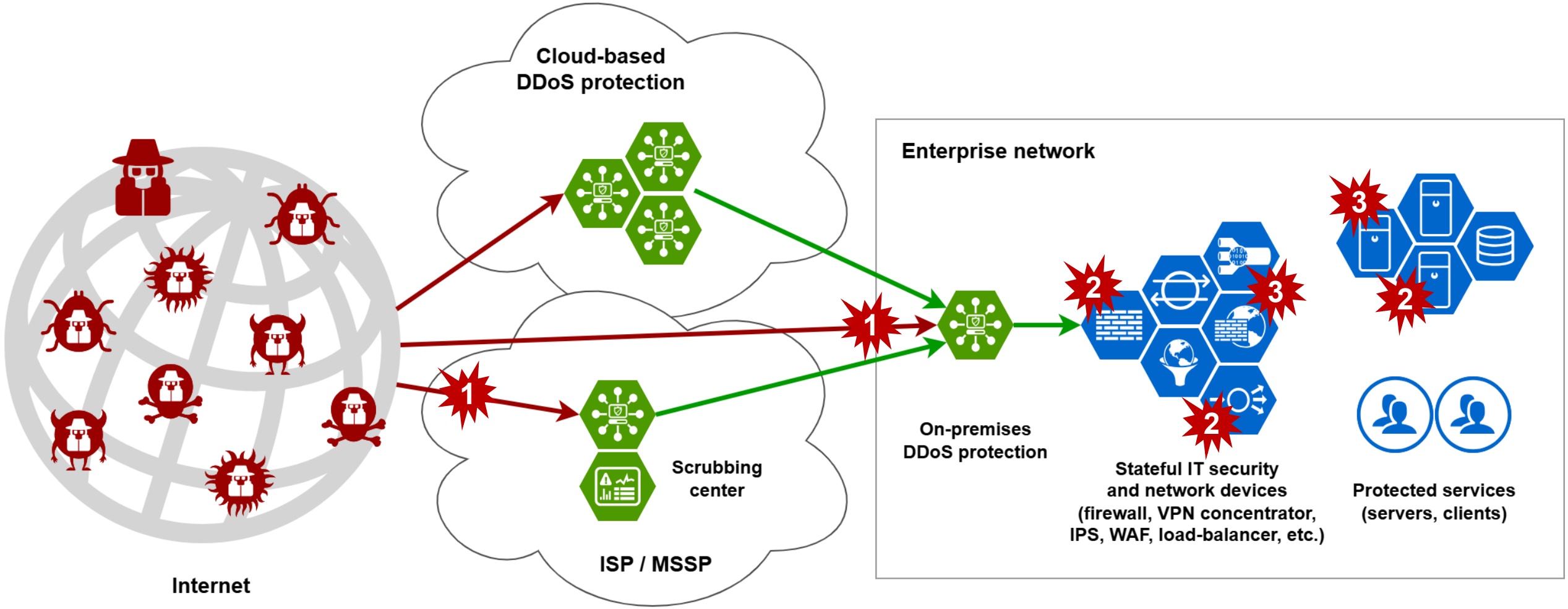
A DDoS-védelem általános célja

nem csupán a forgalom mennyiségének meghatározott szintre csökkentése,

hanem a legitim és a támadó jellegű forgalom intelligens elkülönítése,

a támadás blokkolása a legitim forgalom lehető legnagyobb arányú célba juttatása mellett.

Többrétegű DDoS-védelem



1 – Volumetric attack

2 – State exhaustion attack

3 – Application layer attack

A DDoS-kitettség csökkentése

Hálózati architektúra

- a védendő szolgáltatások szegmentált hálózati környezetben, eltérő subnetekben, eltérő lokáción történő elhelyezése
- több redundáns internet uplink használata, lehetőleg több ISP-től
- Global Server Load-Balancing (GSLB): magas rendelkezésre állás biztosítása, terheléselosztás

Public cloud és hibrid szolgáltatások

- a védelem kiterjesztése a publikus felhőkben (IaaS, PaaS, SaaS) lévő alkalmazásokra
- public cloud és on-prem alkalmazások közötti függőségek figyelembe vétele

DDoS-védelmi szolgáltatások / eszközök

- védendő erőforrások leképezése: eltérő funkcionalitású és forgalmi profilú szolgáltatások különválasztása (pl. kliens proxy, alkalmazásszerverek stb.)
- megfelelő mitigációs eszköztár

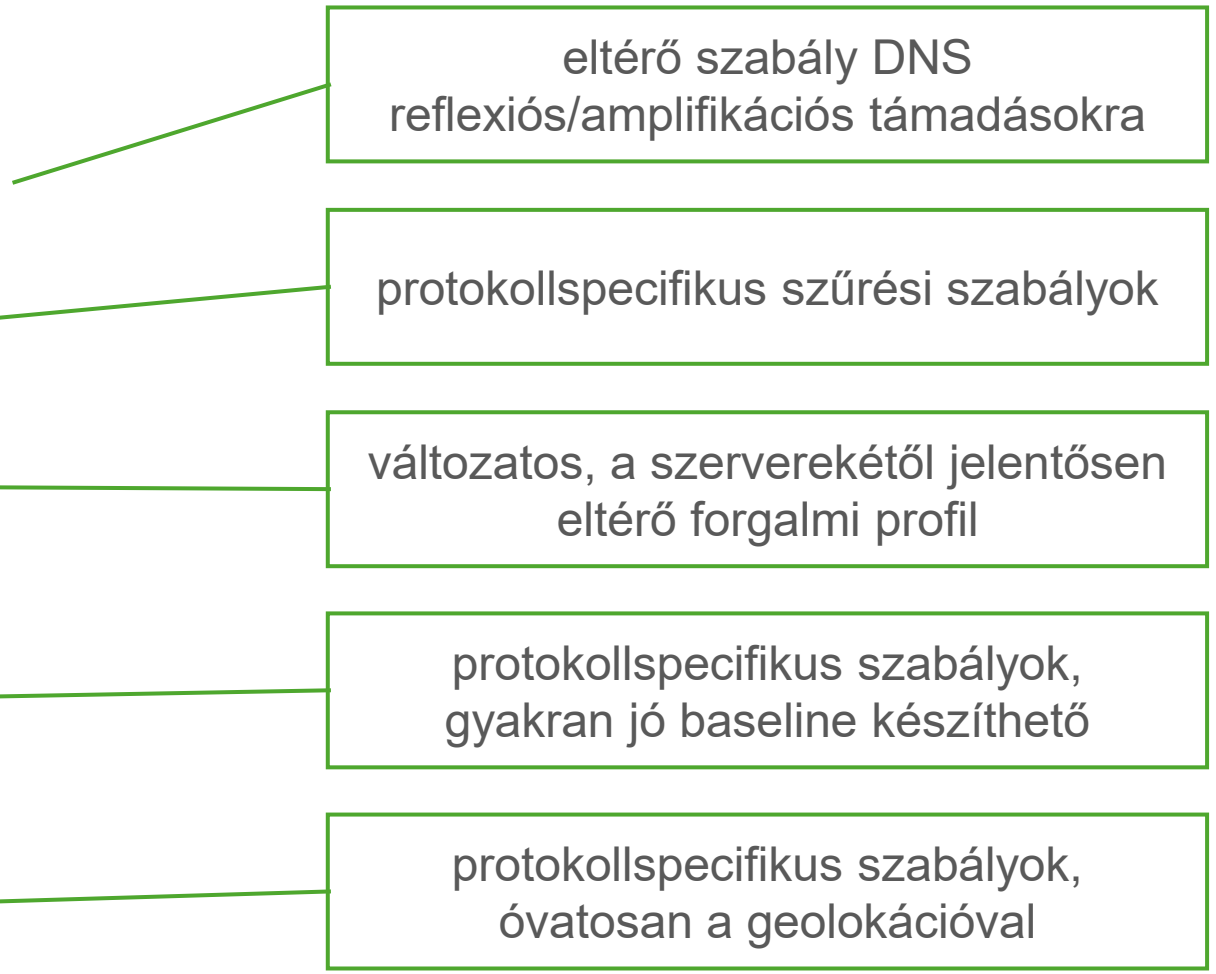
A DDoS-mitigációs eszköztár (példa)

- Whitelist / Blacklist
- Intelligence Feed provided by the vendor
- STIX Feeds
- Botnet Prevention
- Filter List
- CDN and Proxy Support
- Private Address Blocking
- Rate-based Blocking
- Flexible Rate-based Blocking
- Fragment Detection
- Multicast Blocking
- ICMP Flood Detection
- UDP Flood Detection
- Spoofed SYN Flood Prevention (TCP/HTTP authentication)
- TCP SYN Flood Detection (undistruted, high-rate attack)
- TCP Connection Limiting
- TCP Connection Reset
- Payload Regular Expression
- Block Malformed DNS Traffic
- DNS Authentication
- DNS Rate Limiting
- DNS NXDomain Rate Limiting
- DNS Regular Expression
- TLS Attack Prevention
- Malformed HTTP Filtering
- HTTP Rate Limiting
- HTTP Header Regular Expressions
- HTTP Reporting
- Block Malformed SIP Traffic
- SIP Request Limiting
- Application Misbehavior
- IP Location Policing (per country)
- Traffic Shaping

Jól tagolt DDoS-védelmi profilok (példa)

198.51.100.0/24

- .13, .130 rekurzív DNS szerverek
- .30 VPN koncentrátor
- .40 kliens gateway (proxy)
- .64/28 web szerverek 1.
- .192/28 web szerverek 2.
- .225 public cloud gateway



Hatékony detektálás és mitigáció

False positive-ok megelőzése

Együttműködés az ISP-vel / MSSP-vel

- Mennyi információt tud/akar átadni az ügyfél a védendő szervizek leképezéséhez és a védelem paraméterezéséhez? Megfelelően tájékoztatja az MSSP-t a változásokról?
- Az MSSP szolgáltatás jogi és szerződéses keretei: milyen típusú támadások elhárítását vállalja a szolgáltató, mekkora kapacitást és emberi erőforrás keretet biztosít?
- Mennyire kötődnek a szerződéses feltételek az MSSP által alkalmazott technológiához?
- Jól definiáltak a változás- és incidenskezelési folyamatok?
- Működnek a kommunikációs csatornák?
- Megfelelő visszacsatolást adnak egymásnak a felek incidens során?
- Biztosított a DDoS-védelem működőképességének és hatékonyságának rendszeres tesztelése? (vö. NIS2 megfelelőség)
- Megtörténik a tesztek és éles támadások során szerzett tapasztalatok visszaforgatása a DDoS-védelem műszaki eszköztárába és folyamataiba?

Officium

Hankó Péter
hanko.peter@officium.hu