ISACA MÁSODIK SZERDAI ELŐADÁS

BALOGH ZSOLT

Layer7-es DDoS támadások: technikai működés és gyakorlati védekezési stratégiák

2026. március 11.

ISACA®
Budapest Chapter

FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

ISACA®
Budapest Chapter

Bemutatkozás

Balogh Zsolt

ISACA elnökségi tag, Kincstárnok

VP of TechOps @ Liferay

Év információbiztonsági vezetője, 2025

ISACA®
Budapest Chapter

- Digitális Ügyfélélmény Platform
- Pénzügyi intézetek, gyártócégek, kormányzati portálok
- Önkiszolgáló rendszerek, dinamikus weboldalak, portálrendszerek
- 2004 óta, 2010 óta itthon is

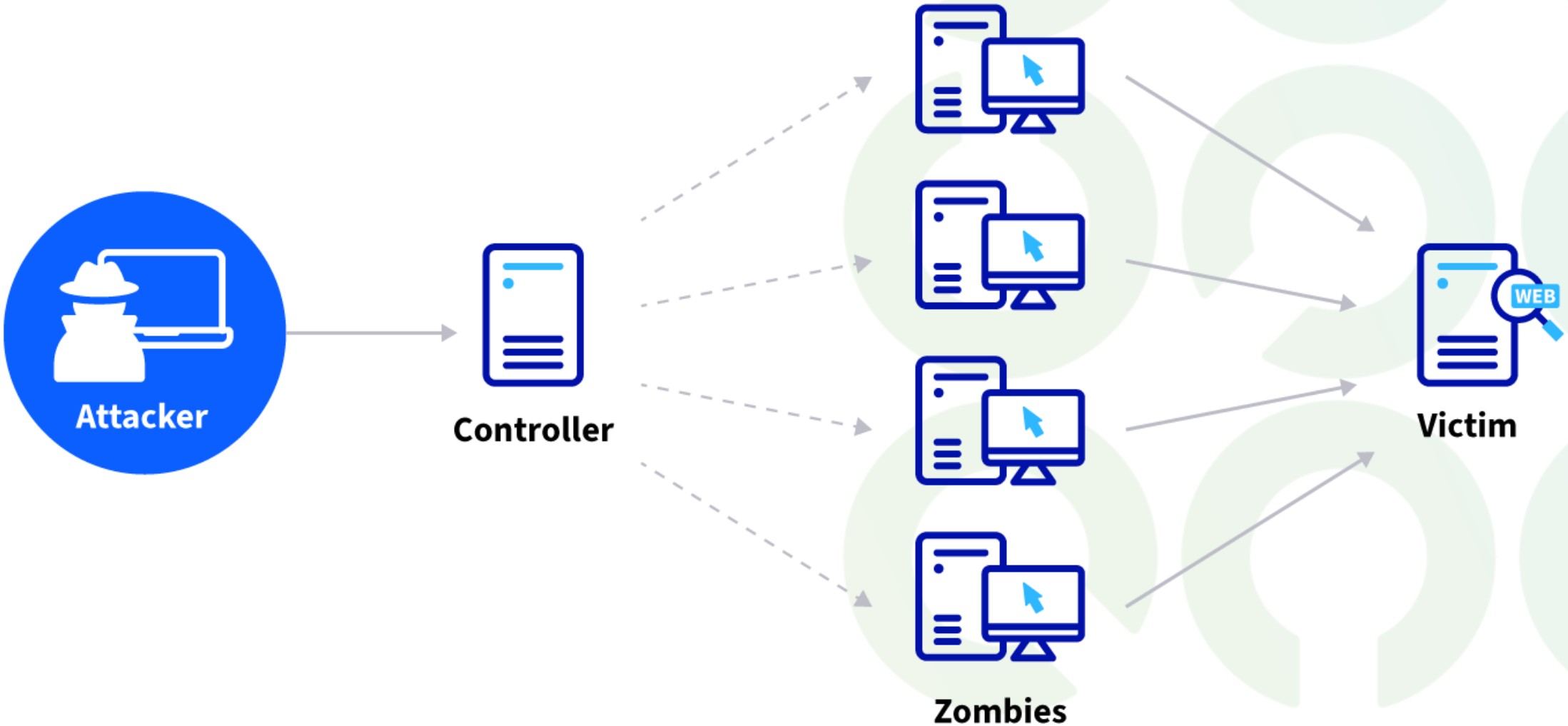
ISACA® Budapest Chapter

DDoS kihívások a mai világban

- Alapvető geopolitikai reakció egy DDoS támadás
- Hatalmas, változatos botnetek elérhetőek
- Elmozdulás a szigetszerű működés felé
- Nem biztos, hogy mindenki igénybe tudja venni a "nagyokat"
- Layer3-4 támadásokat automatikusan kivédi a felhő
- Layer7-es támadásokat egyre nehezebb kivédeni

Hogyan reagáljunk egy komplex támadásra?

ISACA®
Budapest Chapter



ISACA®
Budapest Chapter

Layer 3-4

- SYN flood
- UDP flood
- ACK flood
- volumetrikus támadások

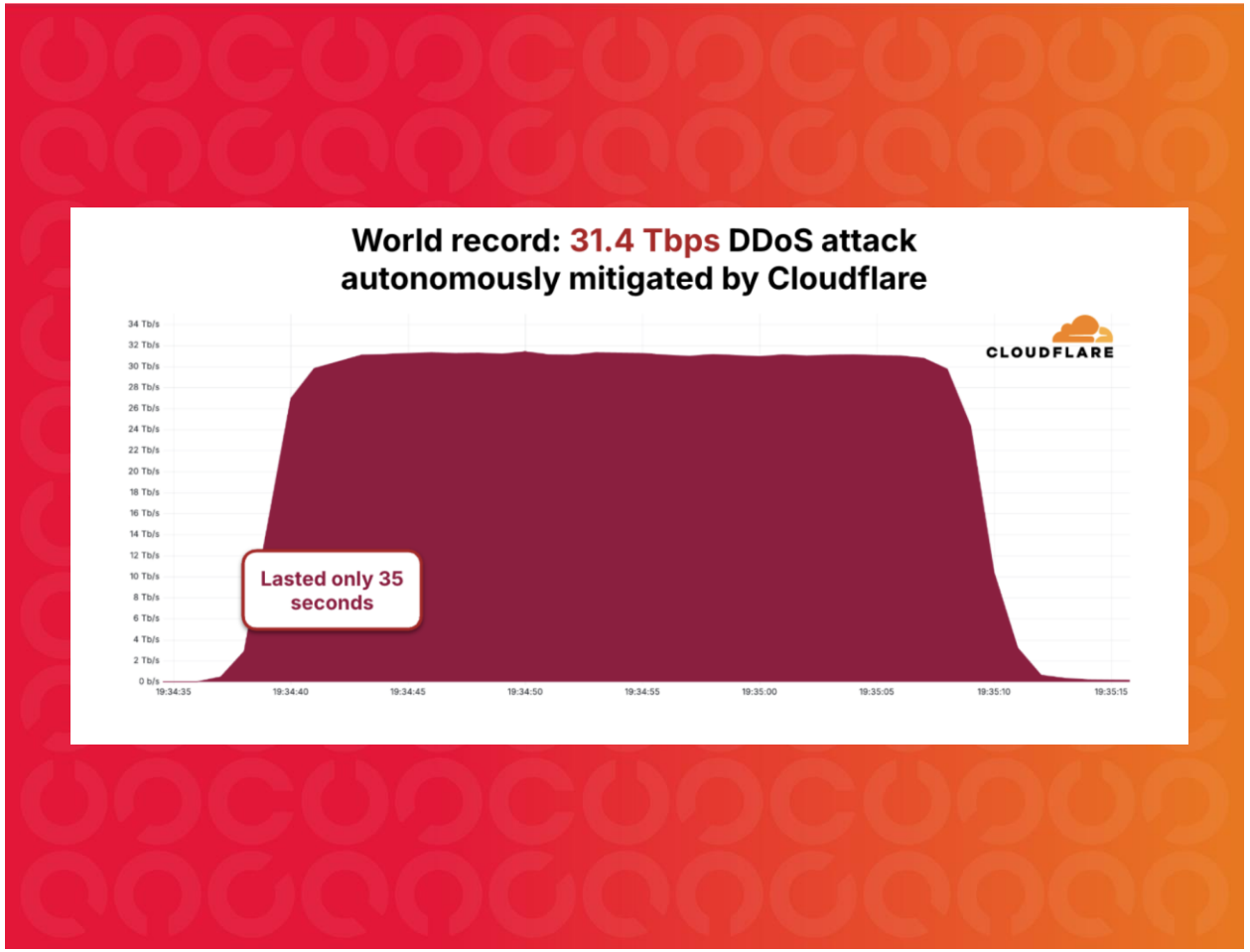
Layer 7

- HTTP flood
- login flood
- Drága lekérések futtatása
- API terhelés
- scraping-szerű terhelés

1. Elegendő sávszélesség

Ha a támodók el tudják addig a pontig, ahol ki tudjuk őket szűrni, akkor a valós kérések már nem férnek be a "csőbe".

Szerencsére a felhőszolgáltatók el tudják ezt a forgalmat nyelni az edge-en.



ISACA Budapest Chapter

2. "Drága" szolgáltatások védelme

- CDN / front-end proxy cache
- Oldal tesztelés
- Hogyan tudják a támadók a cache-t megkerülni?
- Erősen limitálja a funkcionalitás
- Automatikus skálázás - elég gyors-e

3. Rate Limiting

A régi fegyver

- IP-nként, régiónként limitálni a percenkénti kérésszámot
- Fűrész fog alakú terhelést eredményez, talán rosszabb is, mintha nem lenne
- Rate banning hosszabb időre ki is tilt utána
- Bonyolult helyzet proxy-k, VPN szolgáltatók esetén

4. JA3 / JA4 Fingerprinting

- TLS Hello csomag alapján
- Direkt kliens-szerver szükséges (CDN, front-end proxy?)
- Könnyű hamisítani
- Gyakran sikerül 100%-ban leválasztani a támadó forgalmat

5. Mesterséges Intelligencia

- Fingerprintinghez emberek szükséges - lassú reakció
- Anomáliadetektálás gyorsan segíthet
- Ez is sajnos felügyeletet igényel sokszor
- Google Cloud Armor kb. 2 perc alatt talál szabályt

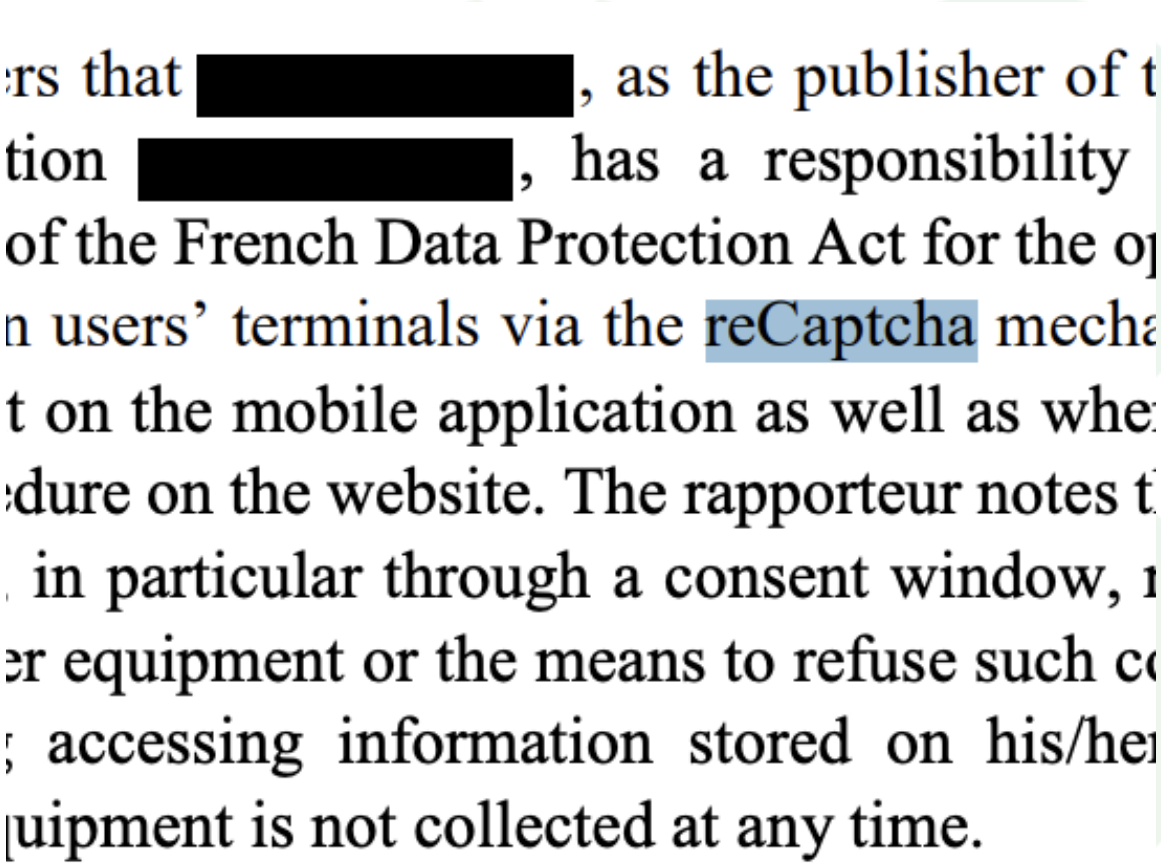
Attribute name	Value	Match type	Attack likelihood	Proportion in attack	Proportion in baseline
UserAgent	"foo"	Exact match	0.7	0.85	0.12
UserAgent	"bar"	Exact match	0.6	0.7	0.4
Source IP	"a.b.c.d"	Exact match	0.95	0.1	0.01
Source IP	a.b.c.e	Exact match	0.95	0.1	0.01
Source IP	a.b.c.f	Exact match	0.05	0.1	0.1
RegionCode	UK	Exact match	0.64	0.3	0.1
RegionCode	IN	Exact match	0.25	0.2	0.3
RequestUri	/urlpart	Substring	0.7	0.85	0.12

Energiaszolgáltató cég elleni támadás

- 23000 bot, 11 különböző fingerprint
- 1 millió jól formázott http kérés másodpercenként
- Mesterséges intelligencia kevesebb mint 2 perc alatt azonosította a fingerprinteket
- 650GB ingress log

6. Recaptcha, Turnstile és barátai

- Kiszűrik a botokat
- DE kiszűrik a botokat
- Jogi kihívások az EU-ban
- Költséges (nagyon) is lehet a védekezés
- Project Omnibus – security cookie problémák lehet meg lesznek oldva

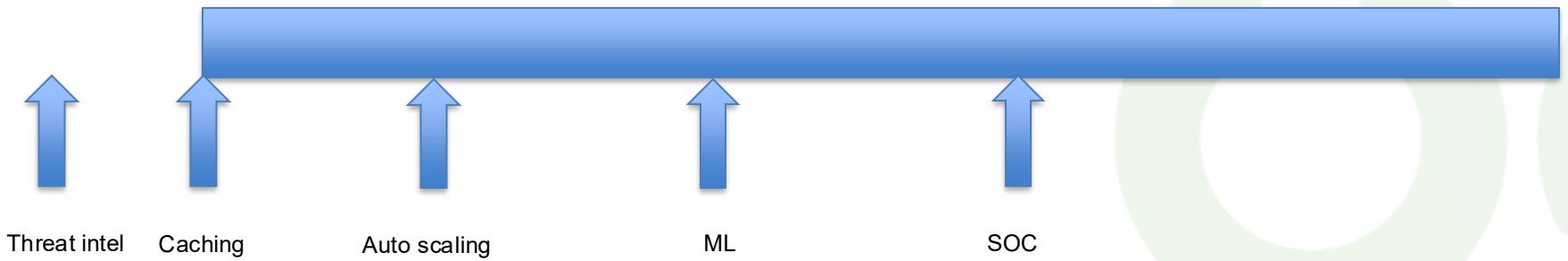


ISACA Budapest Chapter

7. Threat Intel

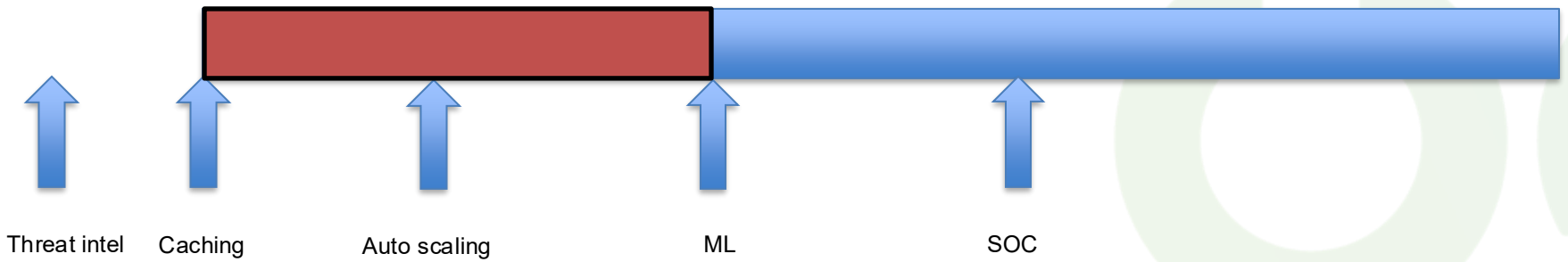
- Alapvetően kizárni a "rossz" szándékú IP-ket
- Több forrásból vásárolni ezeket
- Gyakran frissíteni
- 10-20%-os blokkolási eredményt lehet elérni
- Nagy szolgáltatóknak ez az erőssége

Az igazi kihívás



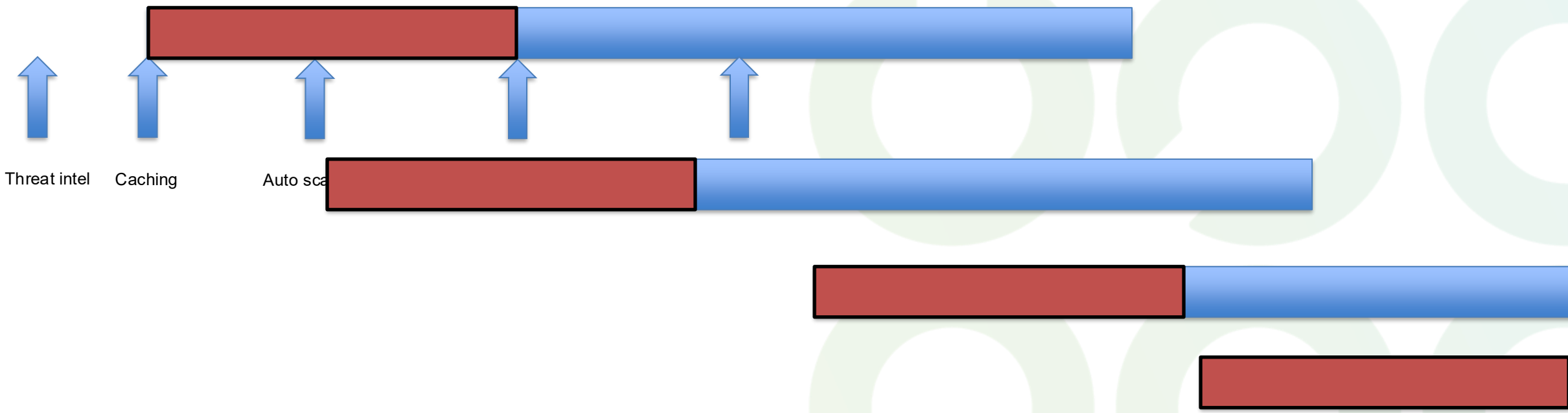
ISACA®
Budapest Chapter

Az igazi kihívás



ISACA®
Budapest Chapter

Az igazi kihívás



ISACA®
Budapest Chapter

Összefoglaló

Nagy szolgáltatók előnyben vannak, de megoldható a védelem

1. Sávszélesség
2. Megfelelő gyorsítótárak
3. Rate limiting
4. Fingerprinting
5. Mesterséges intelligencia
6. Botok leválasztása
7. Threat Intel (goto 0)

KÖSZÖNÖM A FIGYELMET!