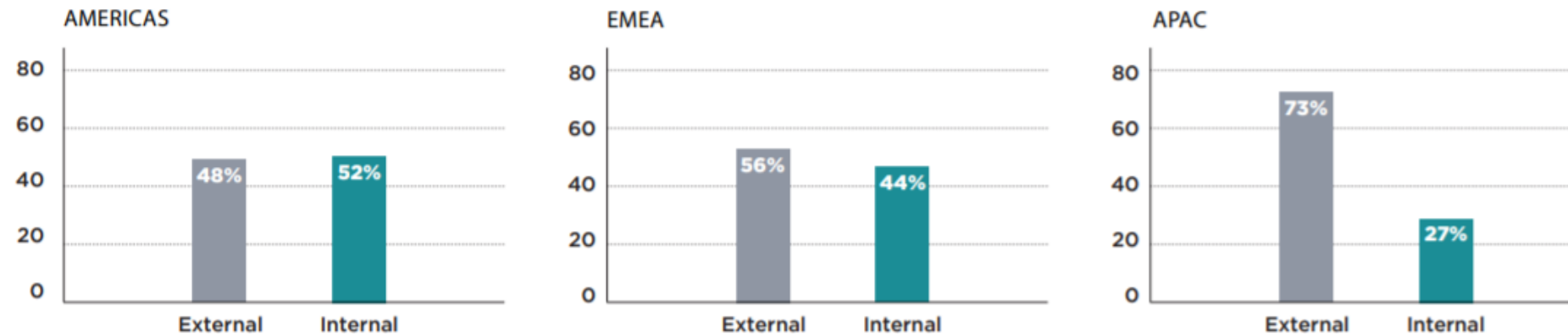


# Fire Eye MTrends 2020 report

## DETECTION BY SOURCE

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
External	94%	63%	67%	69%	53%	47%	38%	41%	53%
Internal	6%	37%	33%	31%	47%	53%	62%	59%	47%

## REGIONAL DETECTION BY SOURCE



filter:max

## Felkészülés és prevenció

*Ahogy szeretnénk, hogy működjön*



## Detekció és reakció

*Ahogy valójában működik*

**A biztonsági  
folyamat  
(Gartner:  
CARTA)**

## Felkészülés & Prevenció

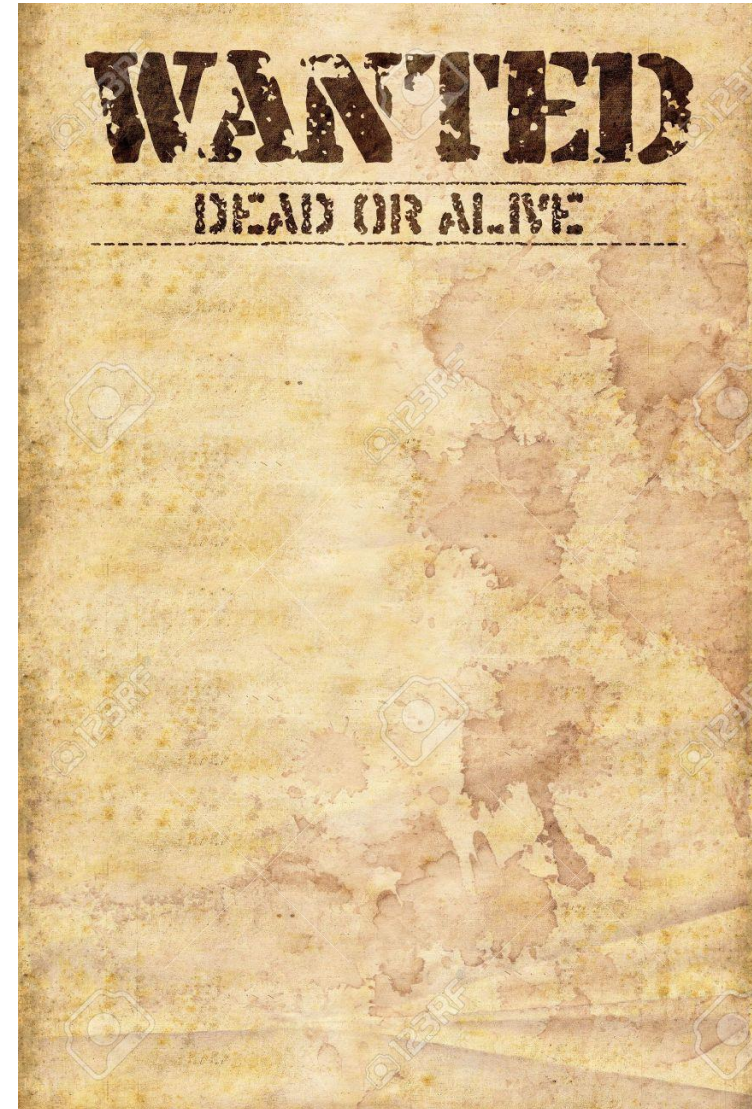
- ▶ **Várfalak, vizes árkok** (Tűzfal, Proxy, IPS, Dos, WAF stb)
- ▶ **Kapuőrök** (Jogosultság szabályozás, IDM, PAM, NAC)
- ▶ **Besúgók, őrszemek, házmesterek** (DLP, Endpoint Security, EDR)
- ▶ **Futárok** (Threat Intel, szignatúrák, domain, IP, Hash, ATO, sérülékenységek)
- ▶ **Vezérkar** (SOC, SIEM = többi eszköz tudása + rengeteg emberi ráfordítás)
- ▶ **Királylány a toronyban mégis szerelmes?**



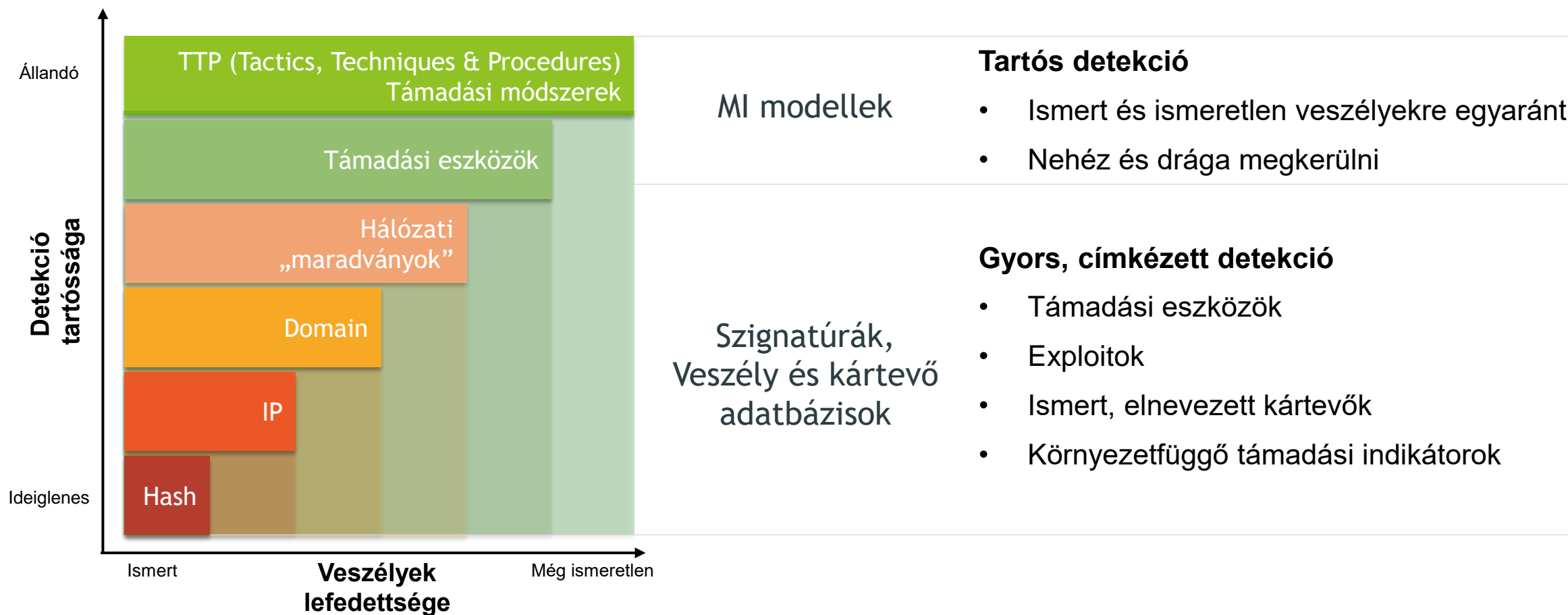


# A detekció és reakció nehéz

- ▶ Mi alapján adunk ki körözést ha nincs személyleírás? (IOC)
- ▶ Honnan tudjuk, egyedül van-e (Kill Chain)?
- ▶ Hogyan döntjük el hogy mi téves riasztás?
- ▶ Hogyan tudjuk letartóztatni, feltartóztatni?
- ▶ Mindezt nagyon gyorsan



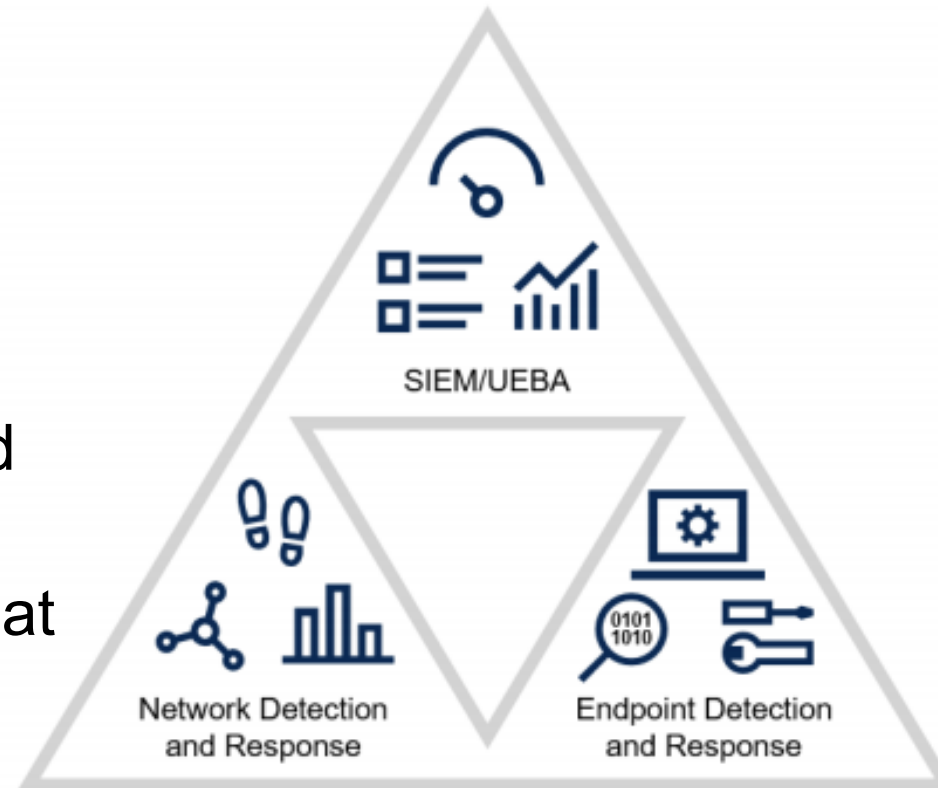
# Zero Trust = Vadászat a káros viselkedésre



# Hol vadásszunk?

## Network Detection:

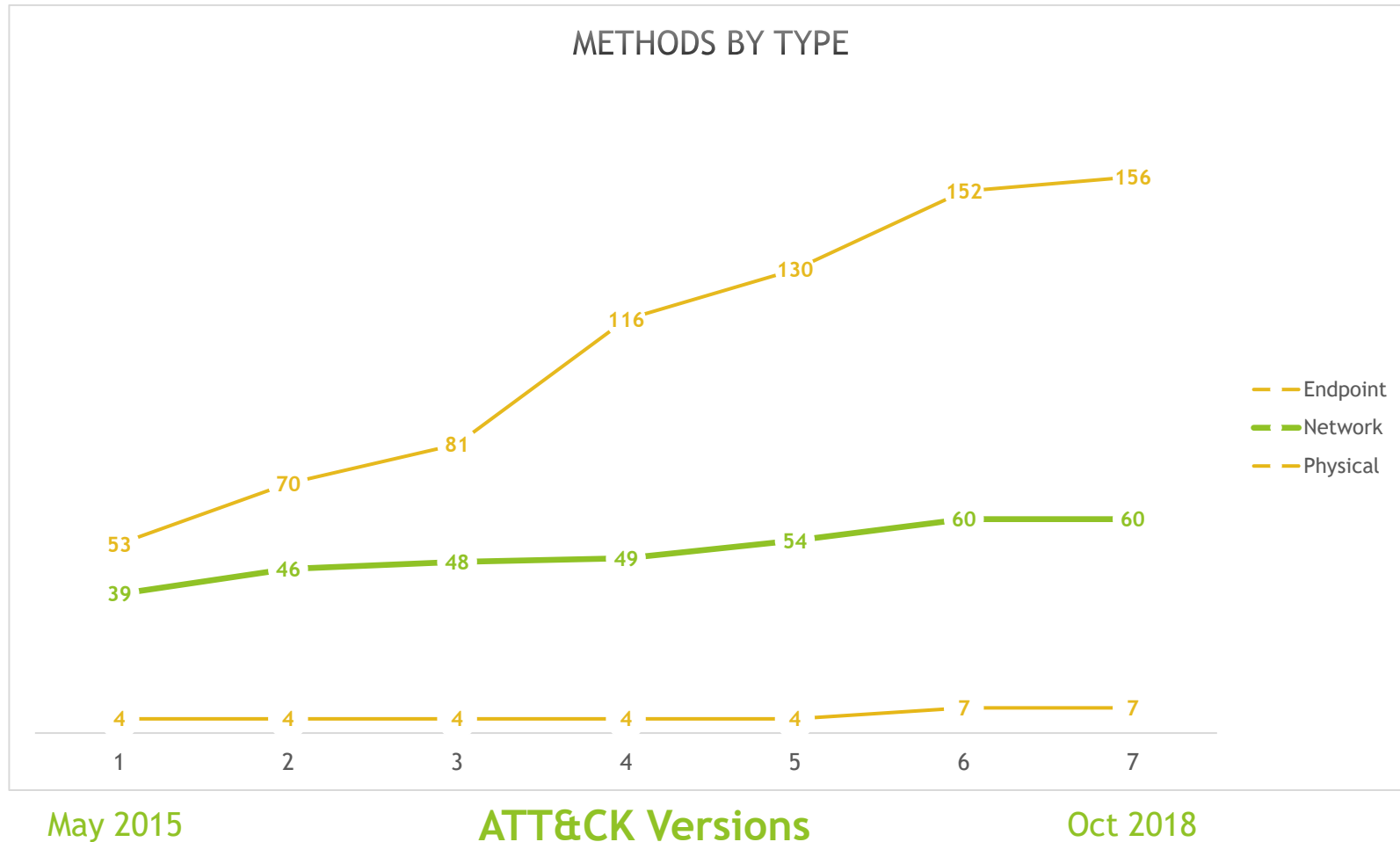
- 1 óra alatt telepíthető
- Teljes lefedettséget ad
- Elméletileg minden hálózati támadást láthat
- Nincs új szaktudás



## SIEM/UEBA és EDR:

- Több hetes/hónapos bevezetés
- Biztosan nem adhat 100% lefedettséget
- Elméletileg sem láthat minden támadási lépést
- Jelentős tréning, szaktudás igény

# A módszerek lassan fejlődnek, főleg a hálózaton



# Támadási viselkedés modellek

## Kiberbiztonsági kutatás

Alapvető támadási viselkedések azonosítása

## Adattudomány

MI modellek fejlesztése a felismeréshez



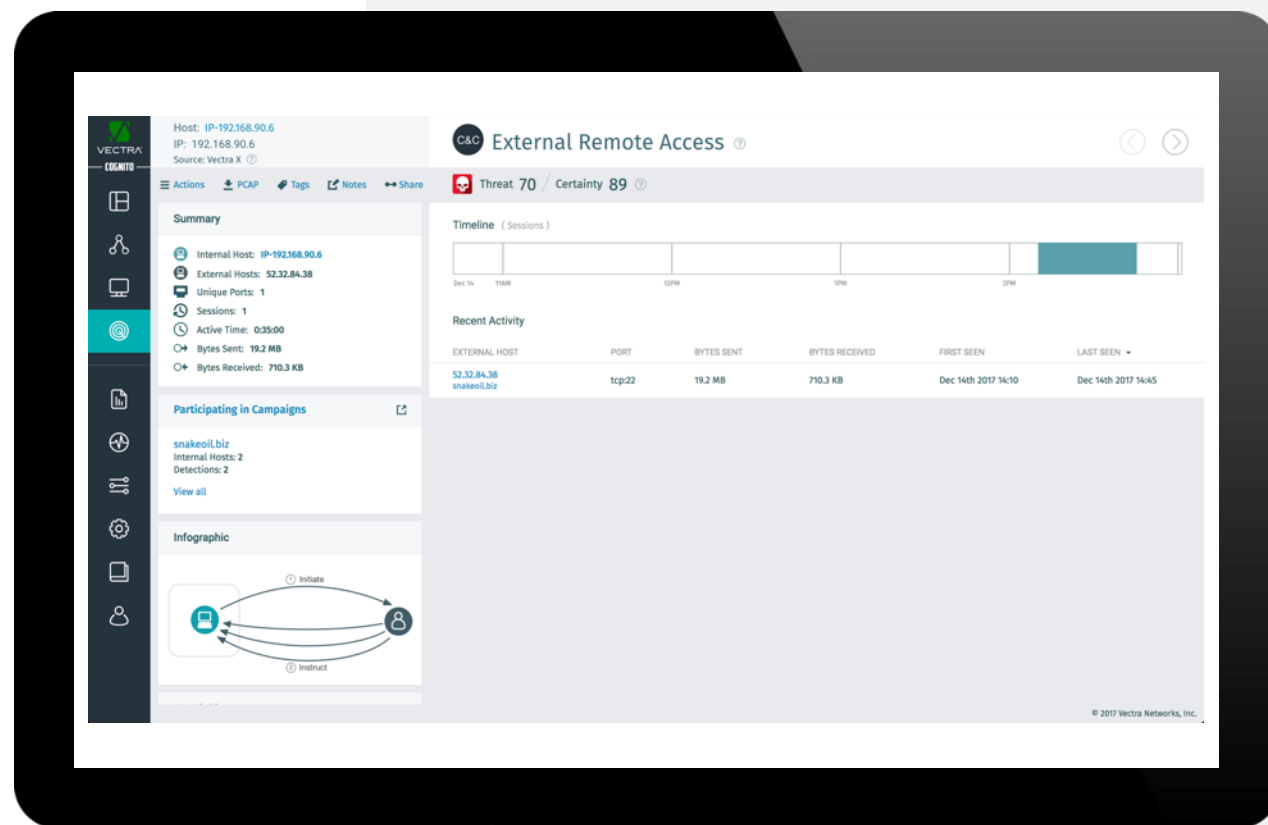
Támadási viselkedés modellek

**Rendkívül pontos, szignatúra, szabály és adatbázis mentes,  
offline, NEM anomáliákat keres**

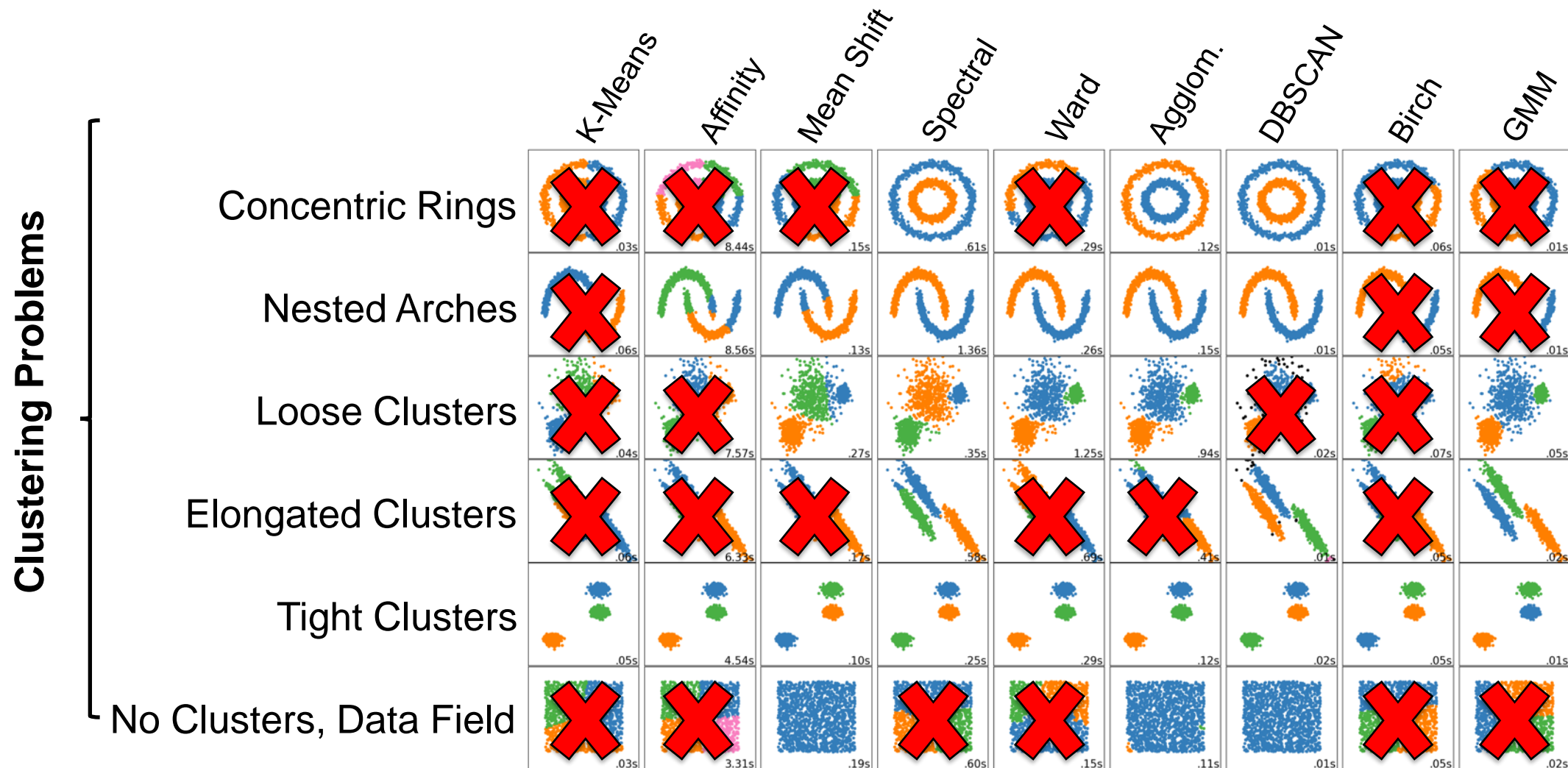


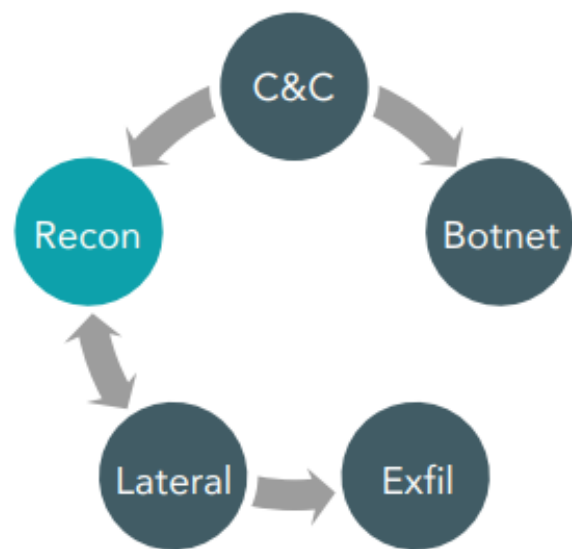
- ▶ **Probléma:** Egyedi távirányítási módszerek detektálása
- ▶ **Adat:** Különböző **Remote Access Tool** forgalmak és normál hálózati mintaforgalom, **csak metaadatok**
- ▶ **Jellemzők és elválaszthatóság:** Forgalmi statisztikát tartalmazó idősorok, milyen irányban, milyen gyakorisággal, ritmussal, mennyi adat
- ▶ **Modell:** Protokoll, desztináció, payload, semleges, nincs szükség IOC-re, szignatúrára, adatbázisokra

## Előre tanított modell: Távoli vezérlés



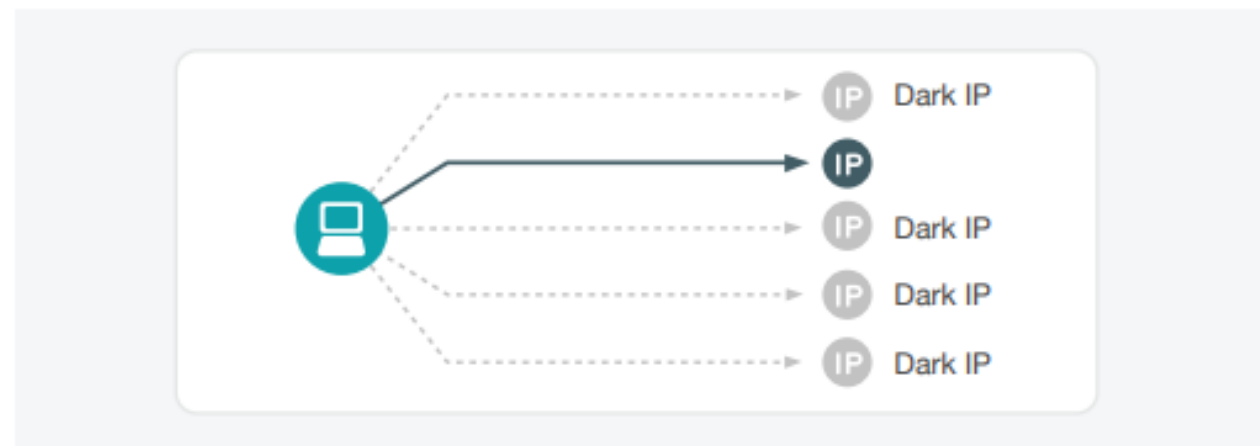
# Nem egy modell mindenek felett..





# Internal Darknet Scan

## Reconnaissance



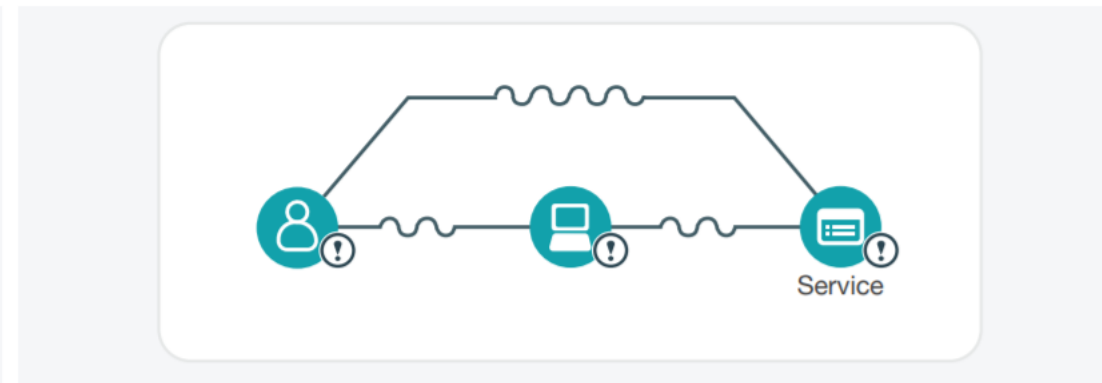
## Triggers

- An internal host has contacted a number of internal IPs that have not been active in the recent past
- Darknet detections cover longer periods than port scans and ignore contact to systems which do not respond to this host, but which are otherwise active
- The threat score places large weight on the spread of IPs, medium for spread of ports and low for the total number of dark IPs contacted
- The certainty score places equal weight on the spread of IPs, spread of ports and number of dark IPs contacted

# Helyben tanuló modell: Szokatlan Adminisztrátori tevékenység

## Privilege Anomaly: Unusual Trio

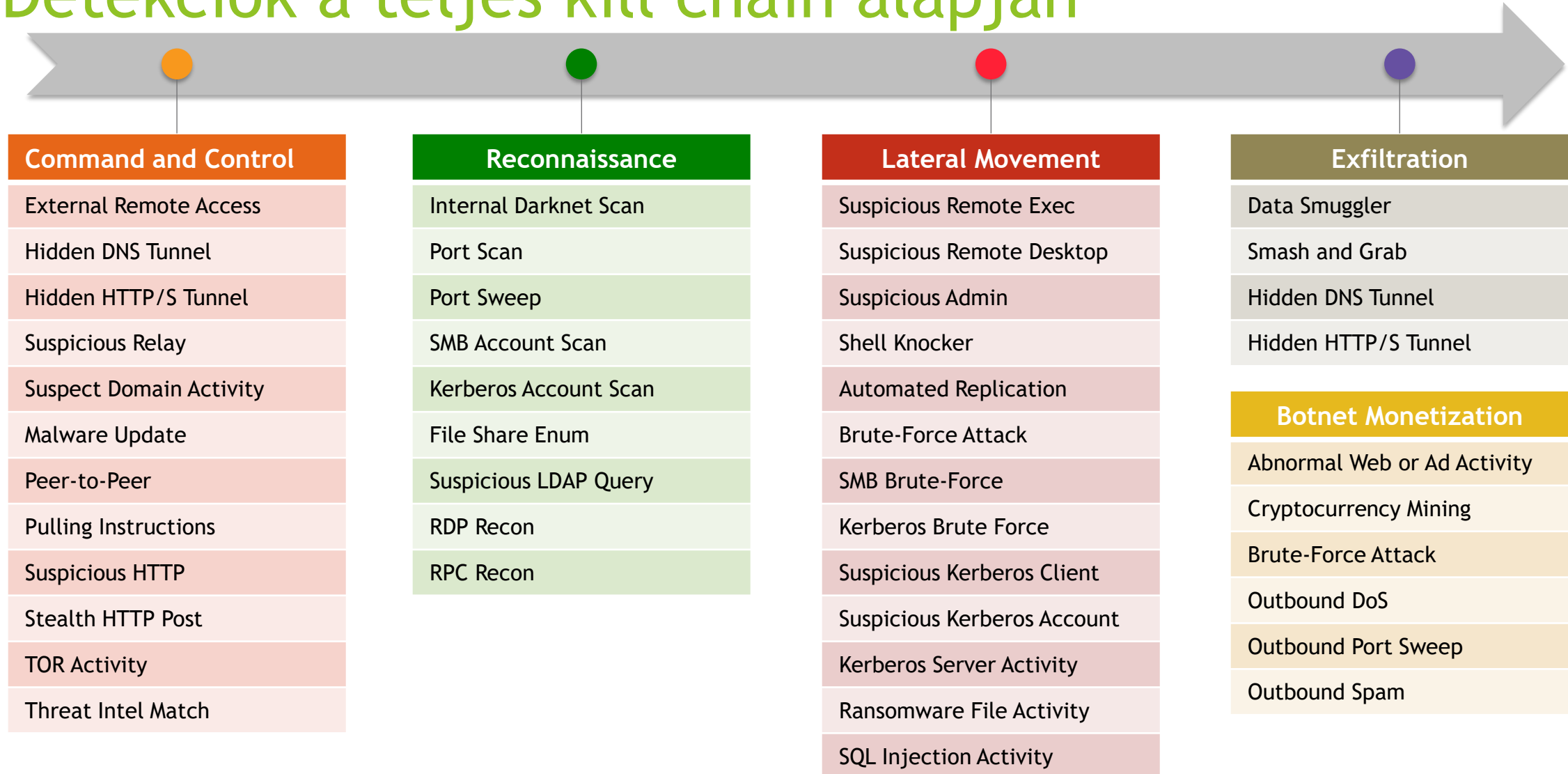
### Lateral Movement



### Triggers

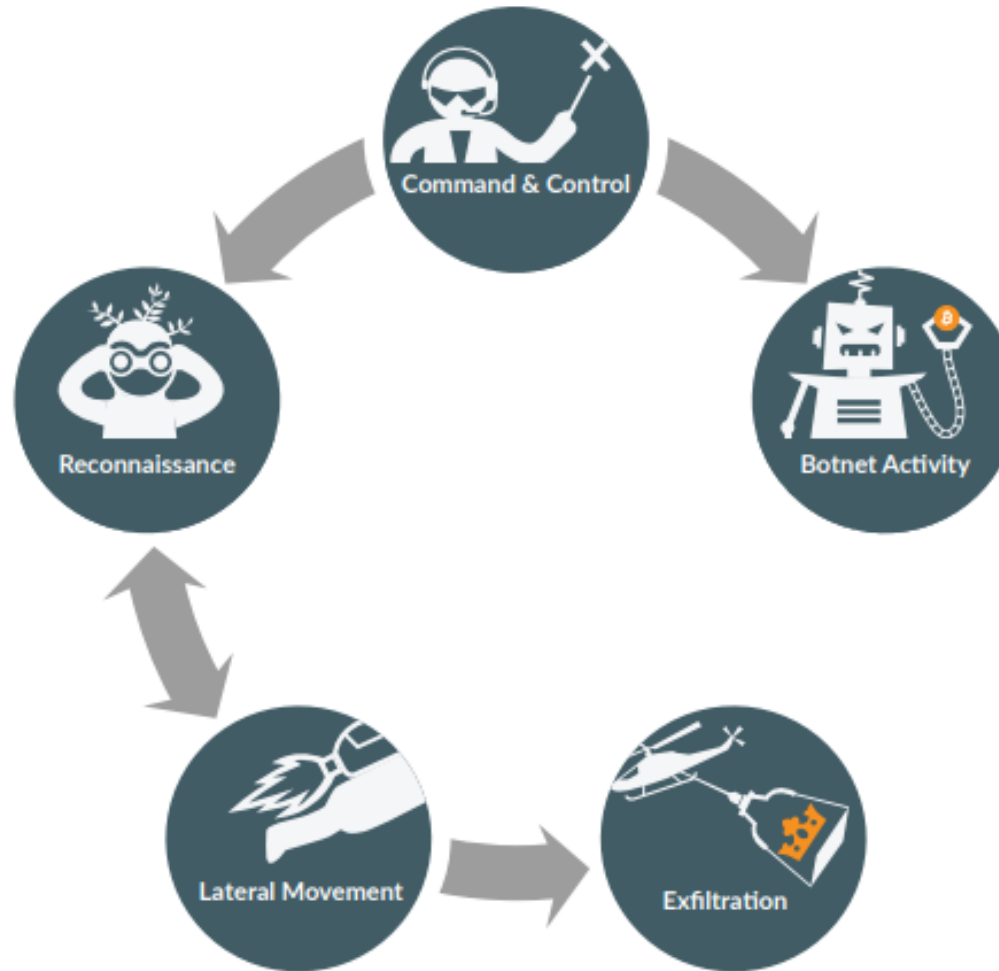
- An account is used from a host to request access to a service where none of the pairings (account-host, account-service and host-service) are consistent with prior observed behavior and at least the service is considered privileged
- The threat score is driven by the privilege scores of the three entities (account, host and service)
- The certainty score is driven by the observed stability of the account, host and service clusters and the number of entities in each relationship (e.g. the number of services the account has been observed to access) and the extent of the abnormality of the transaction with regards to each of the three entities involved

# Detekciók a teljes kill chain alapján

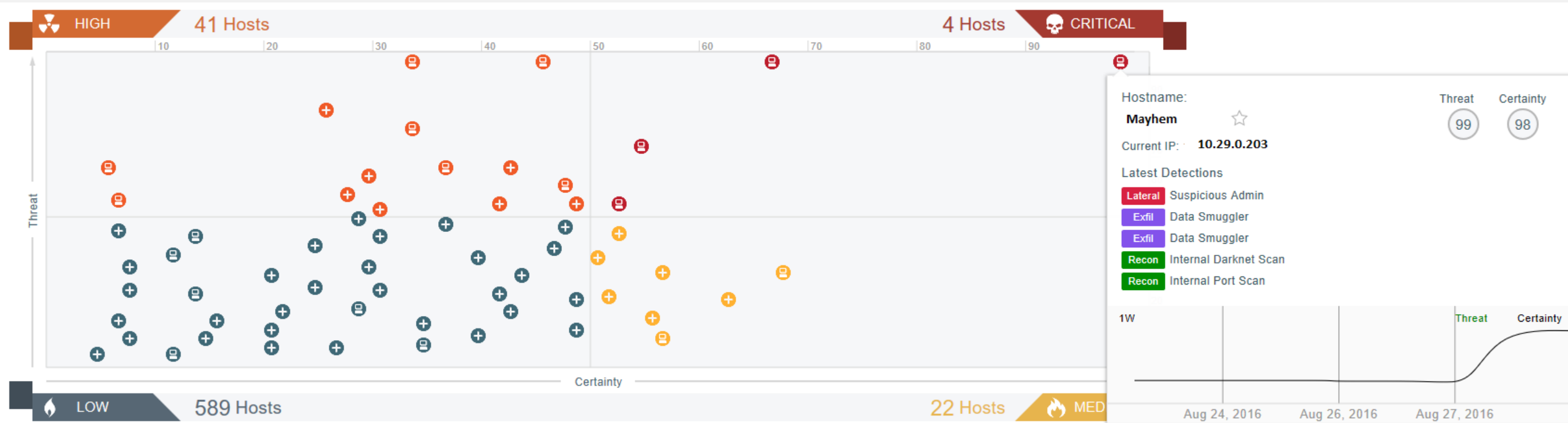


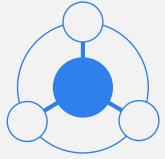


# A Vectra „Kill Chain” (elméletben) mindent láthat



# Cognito fontossági sorrendbe teszi a hosztokat(és accountokat)





# Ökoszisztéma és automatizálható reakció

## Nem csak egy API

Részletes API, minden lényeges SOAR és SIEM rendszer támogatásával. Aktív biztonsági közösség, rendezvények, esettanulmányok és széles körű integrációs megoldások.

