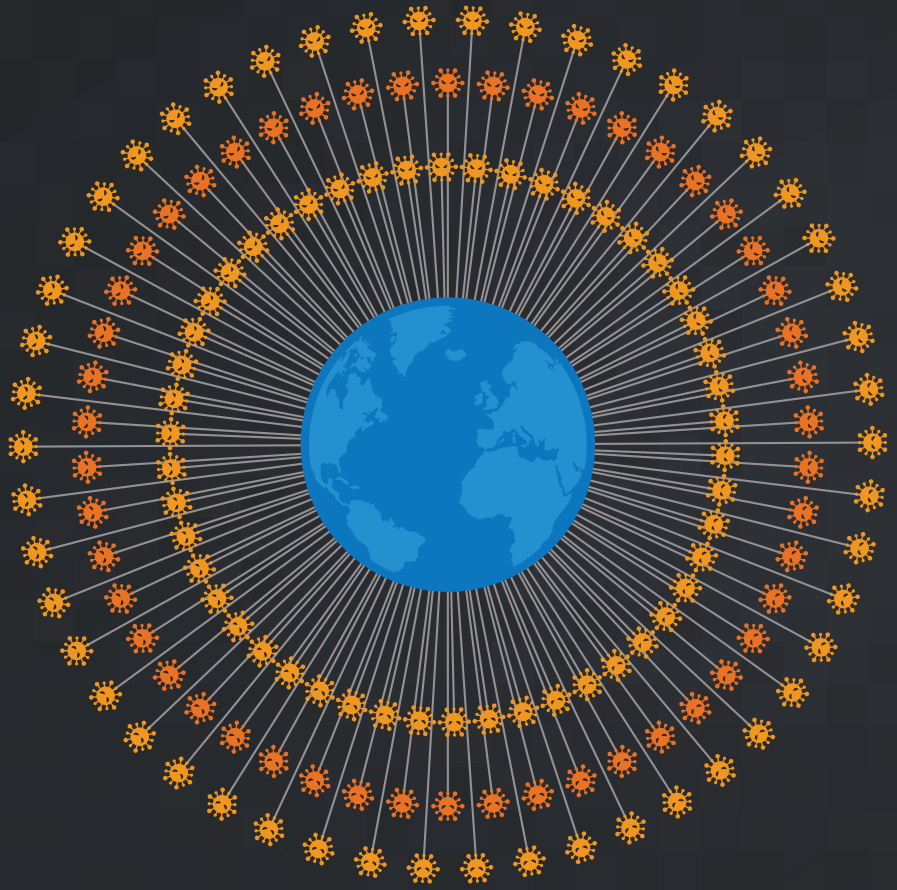
Mesterséges intelligencia alapú védelemi technológiák

Ács György, CISSP
IT biztonsági konzulens
2018. november 8.

A biztonsági helyzetkép



= 10,000

Napi 1.5 millió egyedi malware

TALOS

“Information Security is Becoming a Big Data Problem”

by Neil MacDonald, VP & Gartner Fellow

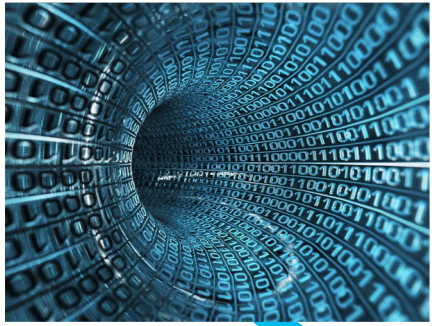
Témák

- Néhány szó az elméletről
- MI a rossz oldalon
- MI technológiák a jó oldalon
  - File vizsgálat és osztályozás
  - Ezt a domaint mire fogják használni?
  - Ismerjük fel a malware-t, visszatitkosítás nélkül

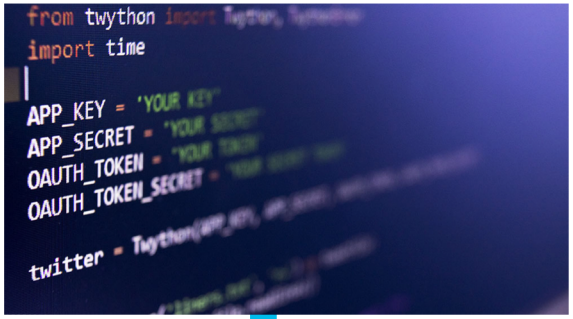
Néhány szó az elméletről

Miből áll a mesterséges intelligencia?

- Adat



Algoritmus/Software



Nagy számítási kapacitás (tanítás)

Prediction, classification, pattern discovery

scikit learn

“Feature” – ”lényegkiemelt paraméterek”, Az adat kritikus : ”DATA IS KING”
Rossz adat -> rossz végeredmény, “sok” adat kell jó végeredményhez, adattisztitás szükséges

MI a rossz oldalon

Malware gyártás MI-val

Security

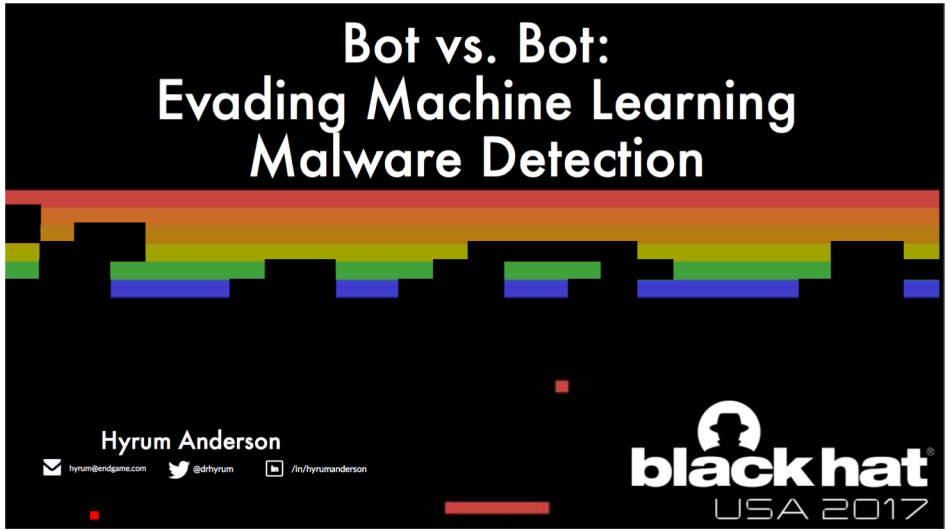
AI quickly cooks malware that AV software can't spot

Experiment used Elon Musk's OpenAI framework - no wonder he's so down on AI

By Iain Thomson in San Francisco 31 Jul 2017 at 07:02 38 SHARE ▼

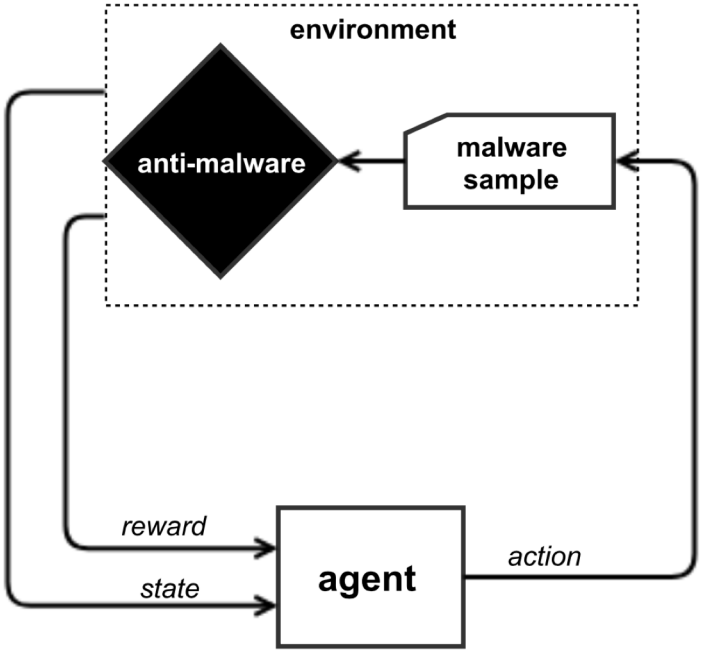
DEF CON Machine-learning tools can create custom malware that defeats antivirus software.

In a keynote demonstration at the DEF CON hacking convention Hyrum Anderson, technical director of data science at security shop Endgame, showed off research that his company had done in adapting Elon Musk's OpenAI framework to the task of creating malware that security engines can't spot.



https://www.theregister.co.uk/2017/07/31/ai_defeats_antivirus_software/

Atari játékok helyett malware



Környezet:

- Malware minta, Windows PE header
- Mutáció: új belépési pont, új section, véletlen importok, byte-ok, stb.

“Agent”:

- Bemenet : malware byte-ok
- Kimenet: akció (sztochasztikus)

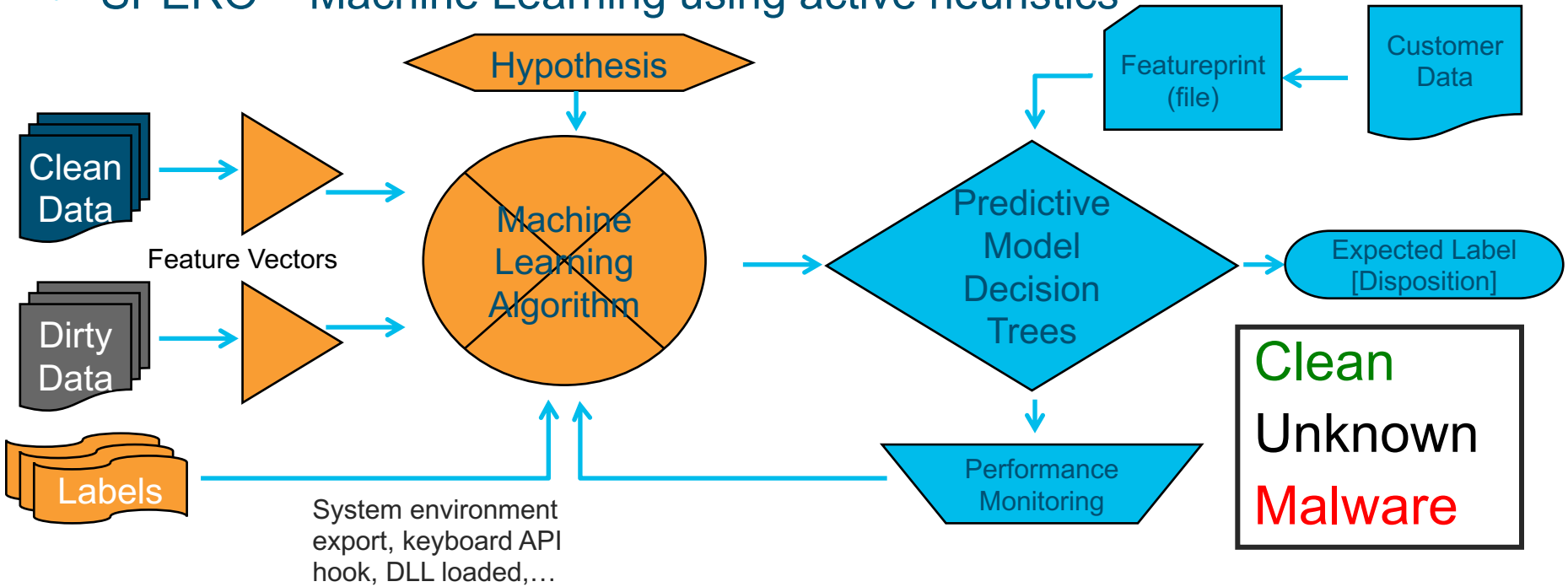
Jutalom: az AV riport szerint tiszta a file

https://www.blackhat.com/docs/us-17/thursday/us-17-Anderson-Bot-Vs-Bot-Evading-Machine-Learning-Malware-Detection.pdf

File vizsgálat és osztályozás

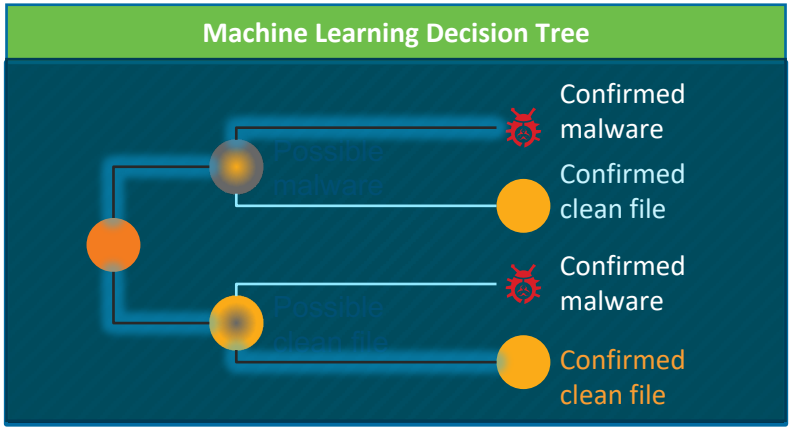
AMP, Advanced Malware Protection
Védelmi rendszer : Spero motor

- SPERO = Machine Learning using active heuristics

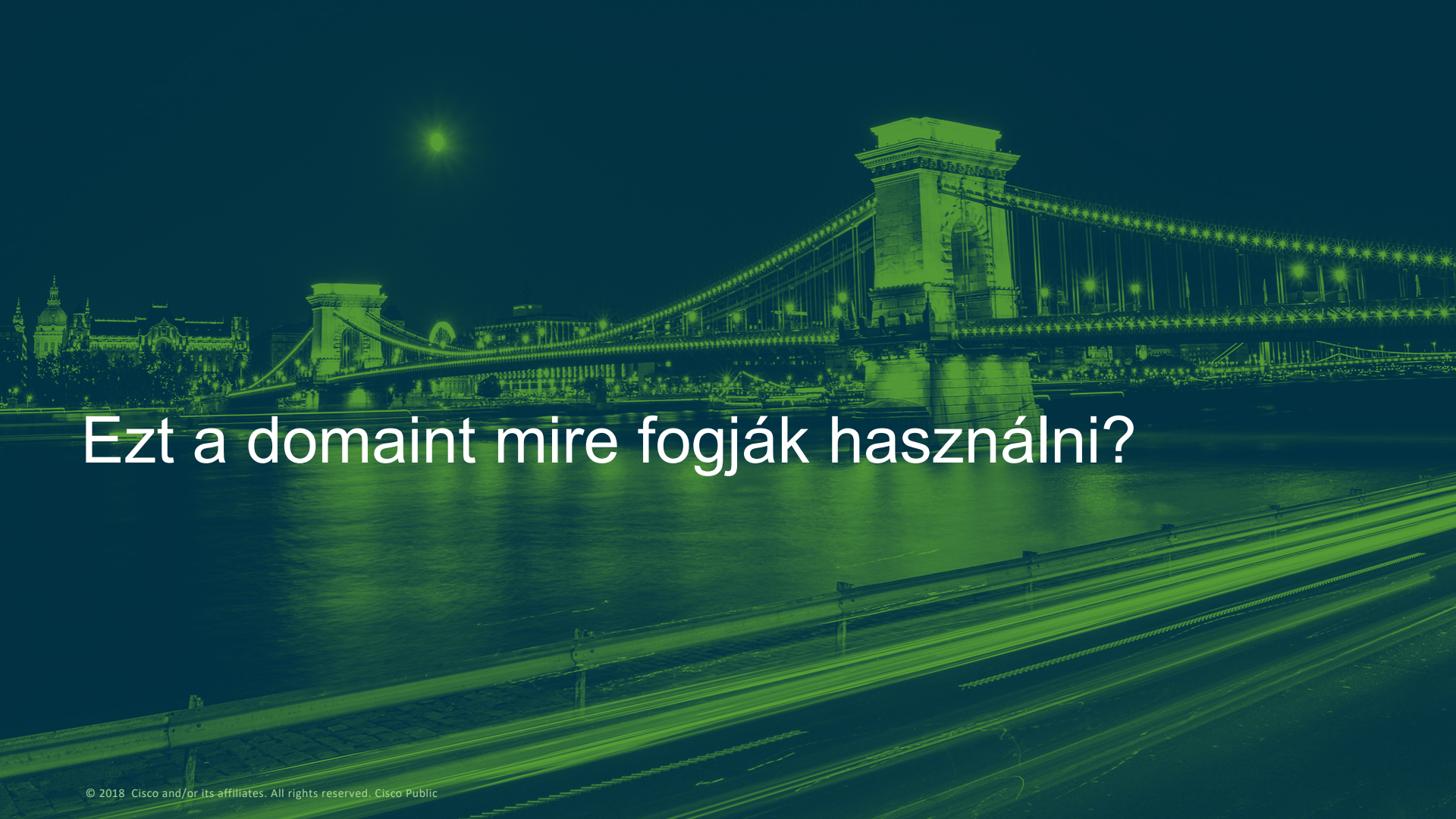


Védelmi rendszer : Spero vizsgálati motor

- AMP címkék = a végrehajtás során kapott jellemzők
  - Hálózati kapcsolatok?
  - Nem szabványos protokoll –alkalmazás
  - Hooking? Milyen API-kat használ?
  - Filerendszer változtatás?
    - Másolja magát
    - File-ok mozgatása
  - Más processzek indítása?

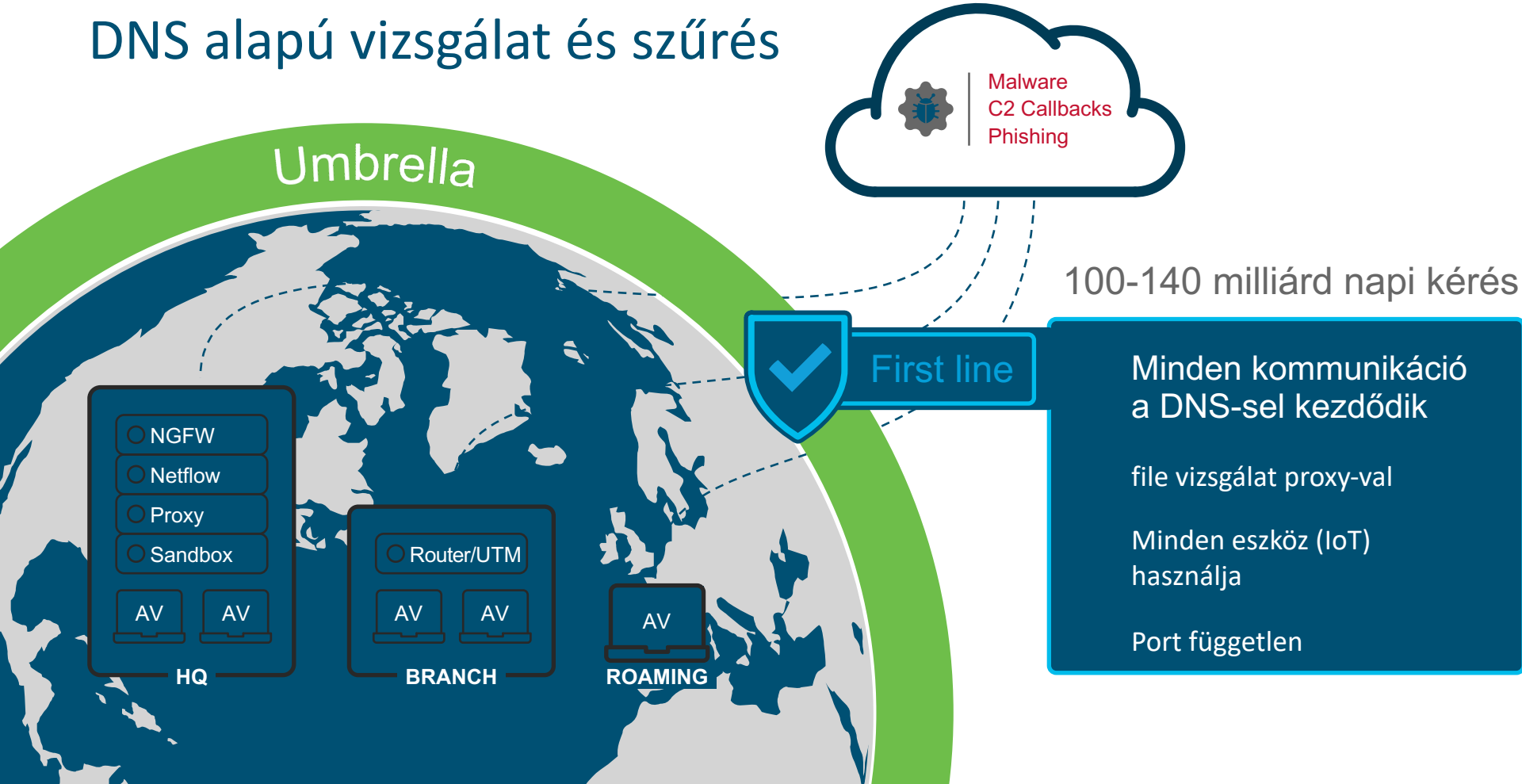


- Több, mint 400 jellemzőt elemez - azonosítja a malware-t



Ezt a domaint mire fogják használni?

DNS alapú vizsgálat és szűrés



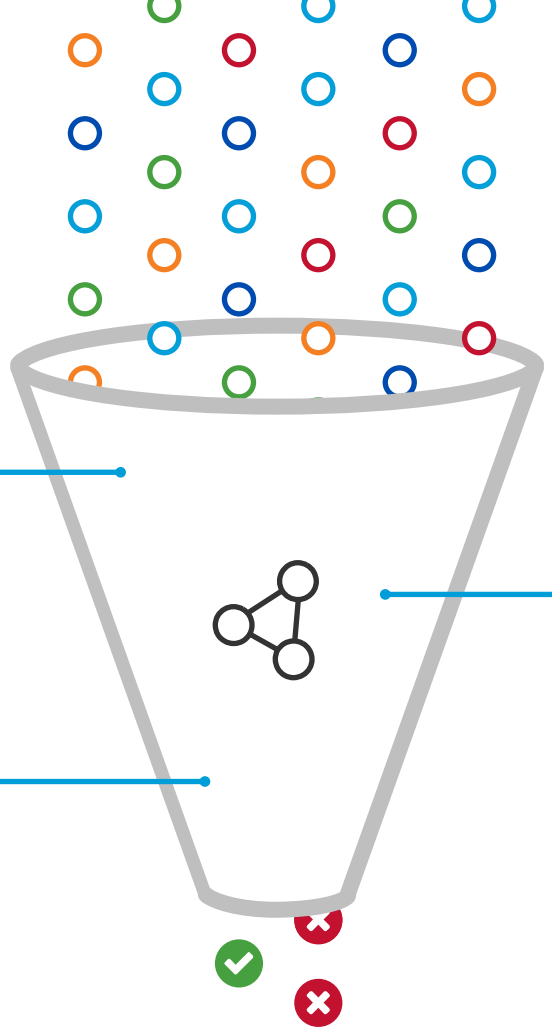
Statisztikai modellek

2M+ live events per second

11B+ historical events

100-140B queries per day

3 million new domains every day



Környezet miatt bűnös

- *Co-occurrence model*
- *IP Geo-Location model*
- Secure rank model
- *Sender rank model*

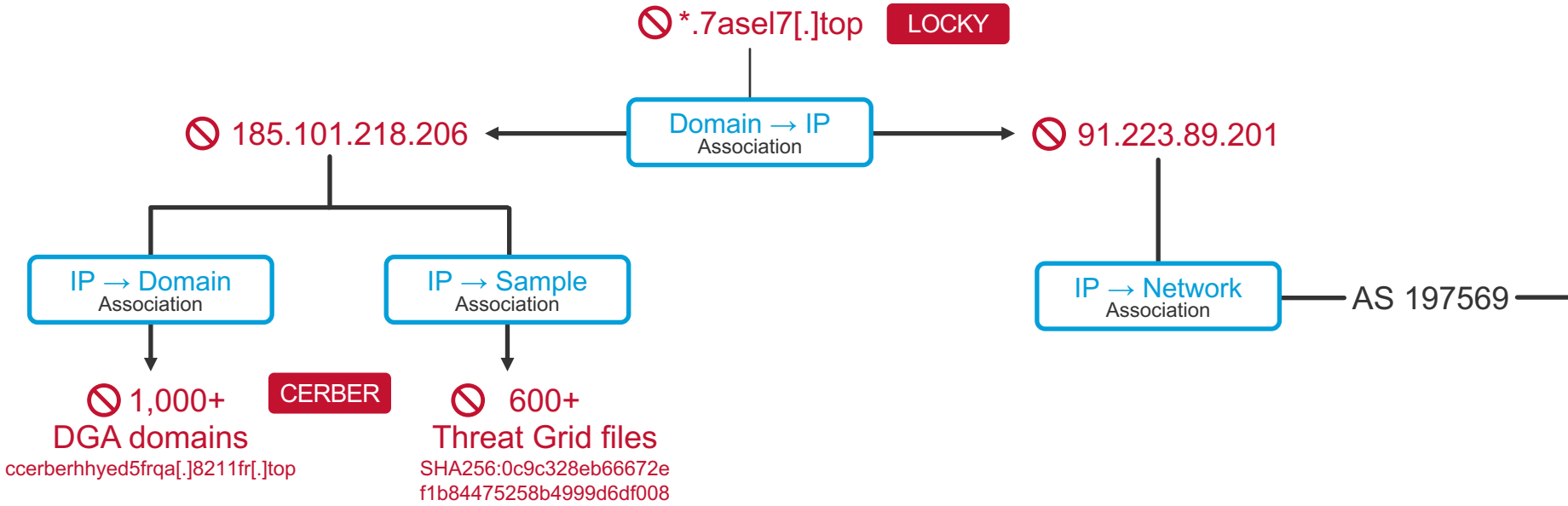
Kapcsolatok miatt bűnös

- Predictive IP Space Modeling

A bűnös mintákat mutat

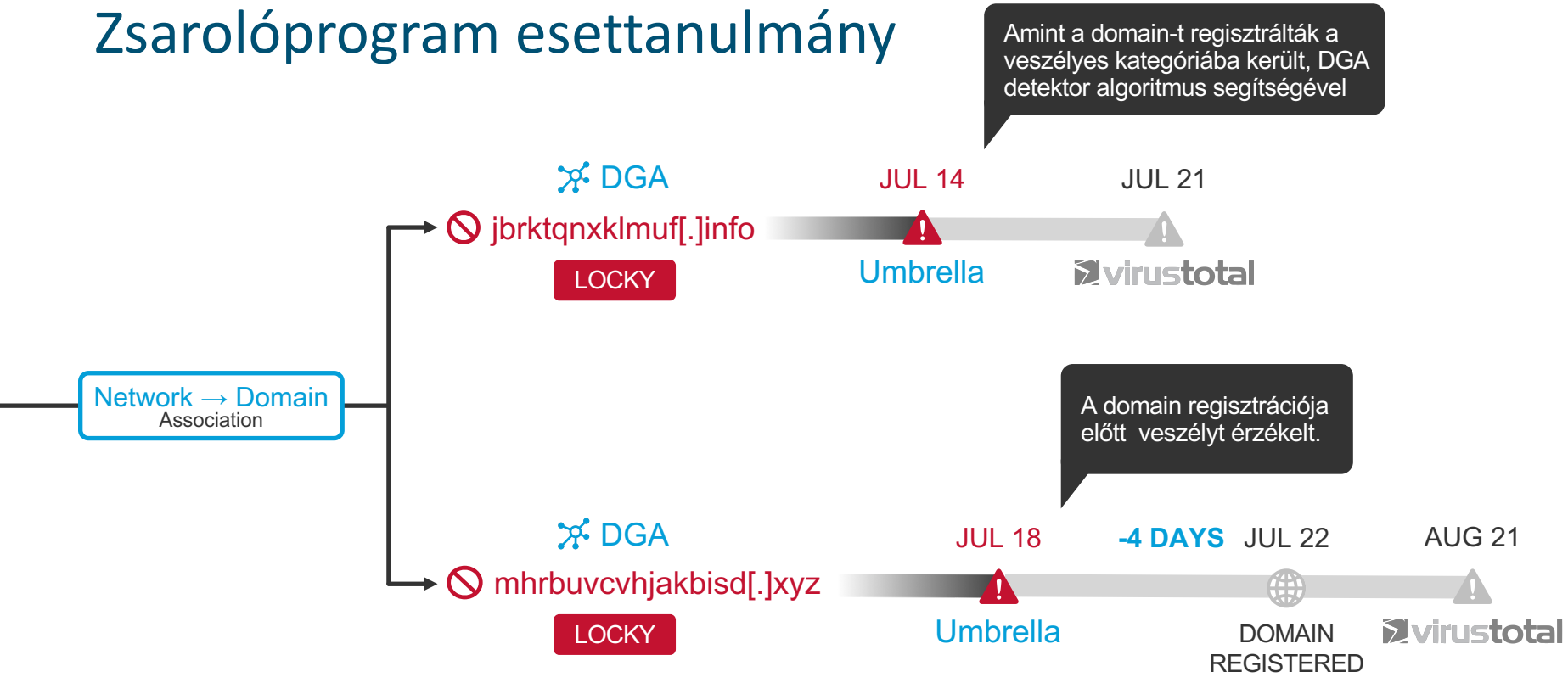
- *Spike rank model*
- *Natural Language Processing rank model*
- Live DGA Prediction

Zsarolóprogram esettanulmány



A Locky és Cerber ugyanazt az infrastruktúrát használja

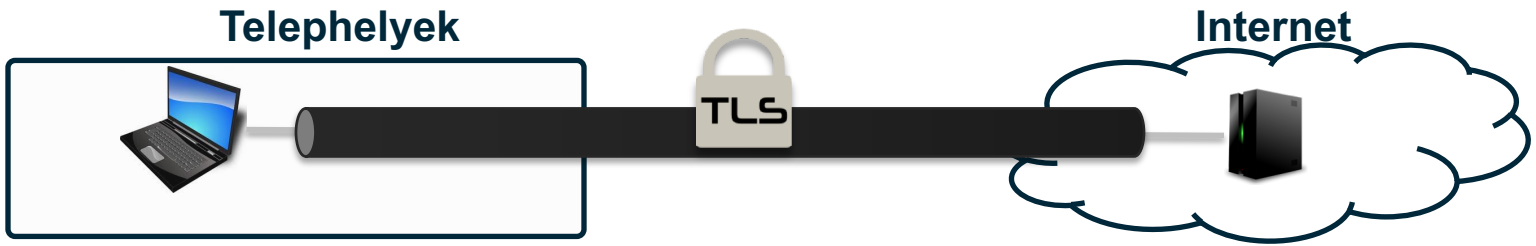
Zsarolóprogram esettanulmány



A statisztikus modellek azonosítottak és blokkoltak a DGA algoritmus által generált 2 domaint, jó néhány nappal azelőtt, hogy regisztrálták.

Ismerjük fel a malware-t, visszatitkosítás nélkül

A probléma: titkosított malware forgalom

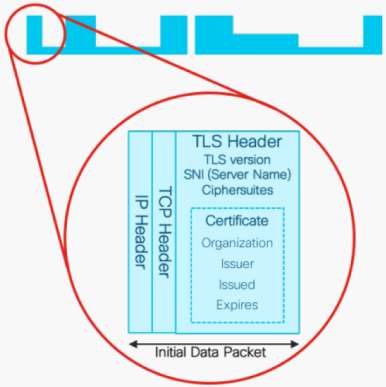


- A TLS használata többségben van már (nem baj!)
- A mintaillesztéses eljárások NEM hatékonyak
- MITM problémák
  - ”Privacy”, jogi, megvalósítási, „drága”, nem együttműködő kliensek, cert pinning, ...

A “jellemzők” : Enhanced NetFlow és intelligencia

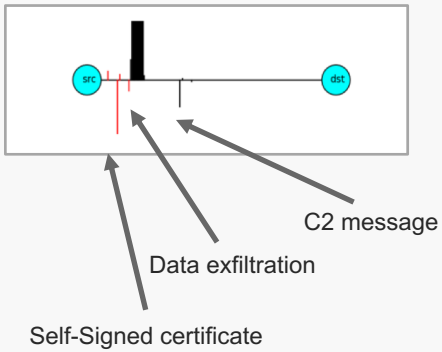
Initial Data Packet

Make the most of the unencrypted fields



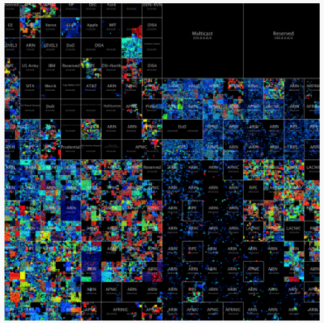
Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



Threat Intelligence Map

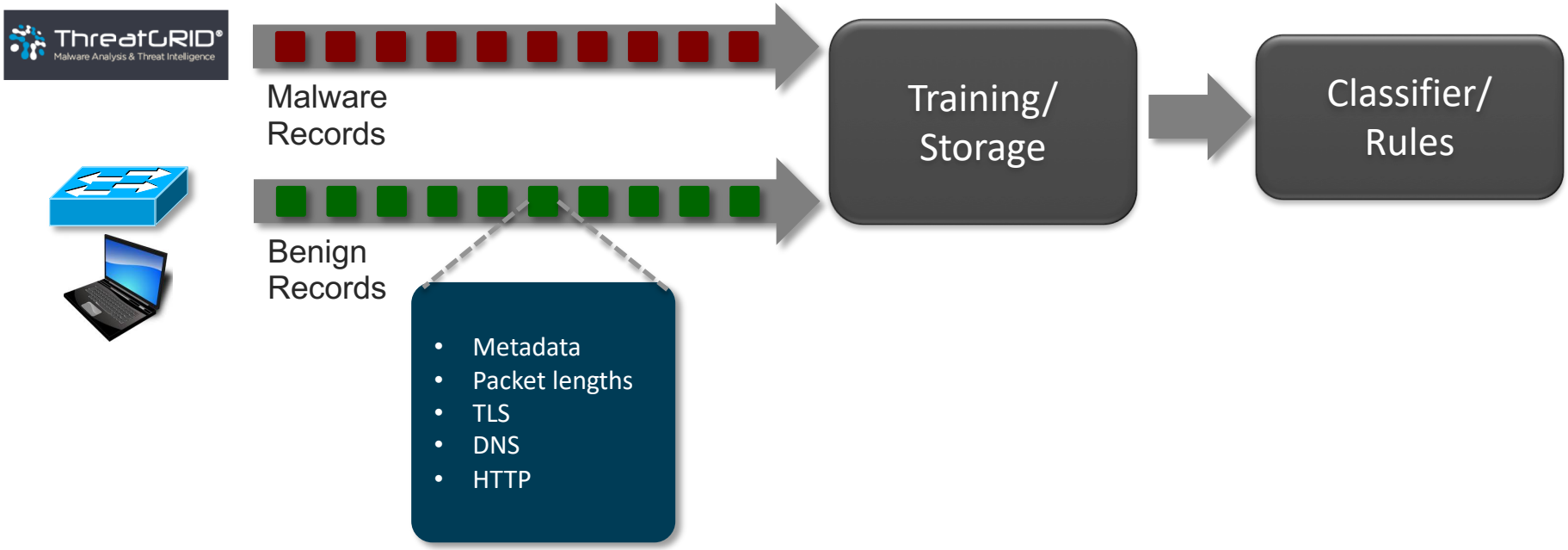
Who’s who of the Internet’s dark side



Broad behavioral information about the servers on the Internet.

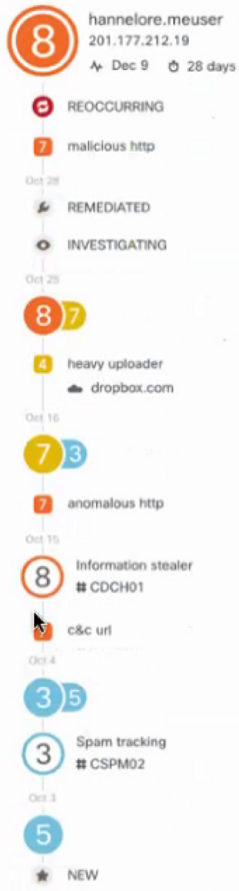
Adatgyűjtés

API, több milliárd flow



https://github.com/cisco/joy

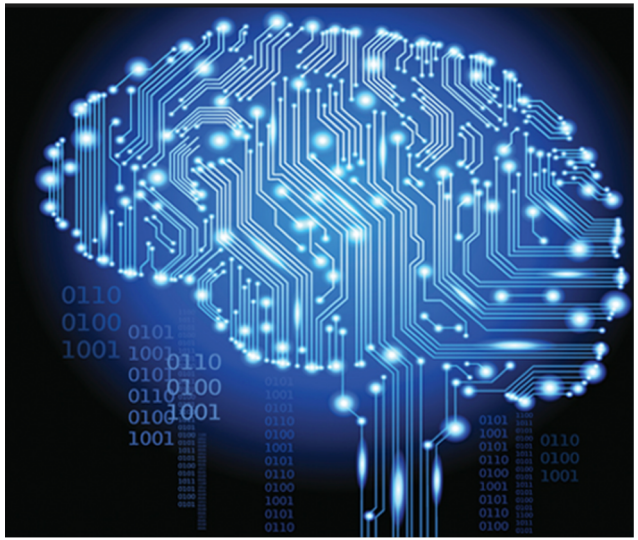
Cognitive Threat Analytics



FTP (uncla...	138B	< 0.01	138B		0B	
ICMP	992B	< 0.01	890B		102B	
Undefined...	549.07KB	< 0.01	548.67KB		408B	
Undefined...	277.39MB	< 0.01	235.45MB		41.94MB	
HTTP (uncl...	620B	< 0.01	144B		476B	
FTP (uncla...	138B	< 0.01	138B		0B	
ICMP	992B	< 0.01	890B		102B	
Undefined...	549.07KB	< 0.01	548.67KB		408B	
Undefined...	277.39MB	< 0.01	235.45MB		41.94MB	
HTTP (uncl...	620B	< 0.01	144B		476B	
FTP (uncla...	138B	< 0.01	138B		0B	
ICMP	992B	< 0.01	890B		102B	

Az MI segíthet

- A kiberbűnözők nem fognak morális kérdést csinálni az MI-ből
- Csak ”emberi erőforrással” nem lehet lépést tartani a nagyszámú malware áradattal
- MI-val hatékonyabb felderítés, megelőzés lehetséges
- malware file felismerés, DNS forgalom,
- titkosított forgalomban,
- HTTP logok, NetFlow információk feldolgozása
- Új megközelítéseket is adhat (DeepMind go példa)



Köszönöm