KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

10 Detekcia a prevencia prienikov

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Detekcia a prevencia prienikov

- detekcia a prevencia prienikov
- pasce na útočníkov
- prístupy k analýze údajov

Detekcia a prevencia prienikov

- **Prienik** = neoprávnená aktivita ohrozujúca systém alebo sieť
- **IDS (Intrusion Detection System)**
  - deteguje a upozorňuje
- IPS (Intrusion Prevention System)
  - deteguje a aktívne blokuje
- dopĺňajú firewall o hlbšiu analýzu prevádzky
- kľúčový prvok viacvrstvovej obrany

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Systémy detekcie/prevencie narušenia (I.)

- **Systém detekcie narušenia (Intrusion detection system, IDS):**
  - zariadenie alebo aplikácia, ktorá analyzuje celé pakety, hlavičky aj užitočné zaťaženie hľadajúc známe udalosti.
  - po zistení známej udalosti sa vygeneruje správa o udalosti.

- **Systém prevencie narušenia (Intrusion prevention system, IPS):**
  - zariadenie alebo aplikácia, ktorá analyzuje celé pakety, hlavičky aj užitočné zaťaženie hľadajúc známe udalosti.
  - po zistení známej udalosti sa vykoná akcia

- **Možné akcie:**
  - zahodenie packetu, zastavenie komunikácie
  - reštartnutie komunikácie
  - ...

Systémy detekcie/prevencie narušenia (II.)

- **Podľa spôsobu detekcie**
  - detekcia signatúr (signature dection)
  - detekcia anomálii (anomaly detection)
  - hybridná detekcia (Hybrid detection)

- **Podľa umiestnenia**
  - hostiteľský detekčný systém
  - sieťový detekčný systém

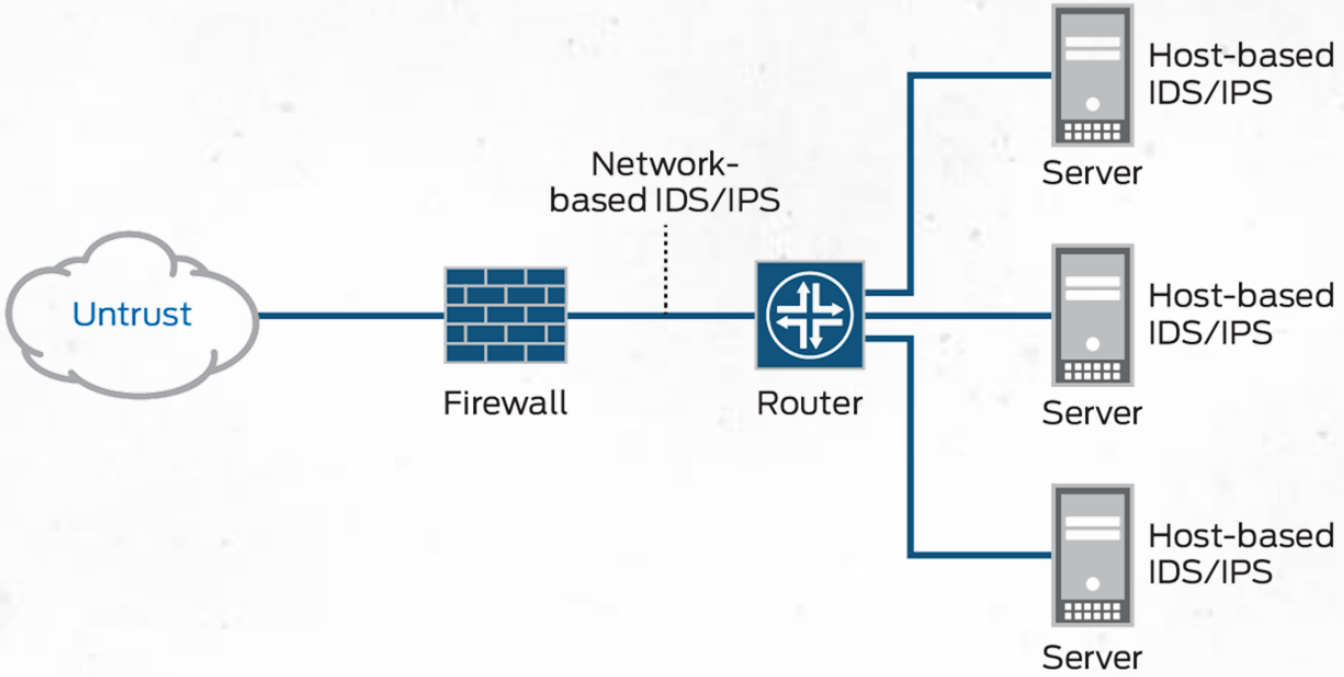
NIDS a HIDS (I.)

- **NIDS (sieťový)**
  - analyzuje sieťovú prevádzku na senzoroch
  - pohľad na celú sieť, nevidí do šifrovanej prevádzky
- **HIDS (hostiteľský)**
  - sleduje aktivitu na konkrétnom systéme
  - detail o systéme (súbory, procesy, logy)

- najlepší výsledok dáva ich kombinácia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

NIDS a HIDS (II.)



Zdroj: https://gupta-bless.medium.com/learning-more-about-ips-and-ids-ef6d859c2ab3

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prístupy k detekcii

- **Signatúrna detekcia**
  - porovnanie so známymi vzormi útokov
  - spoľahlivá na známe hrozby, zlyháva pri nových
- **Anomálna detekcia**
  - odchýlky od normálneho správania
  - odhalí aj nové útoky, ale viac falošných poplachov
- **Heuristická a behaviorálna analýza**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prístupy k analýze údajov

- štatistická analýza prevádzky a profilov správania
- strojové učenie a detekcia anomálií
- korelácia udalostí z viacerých zdrojov
- Threat intelligence - kontext aktuálnych kybernetických hrozieb
- spätná (forenzná) analýza zaznamenaných dát

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

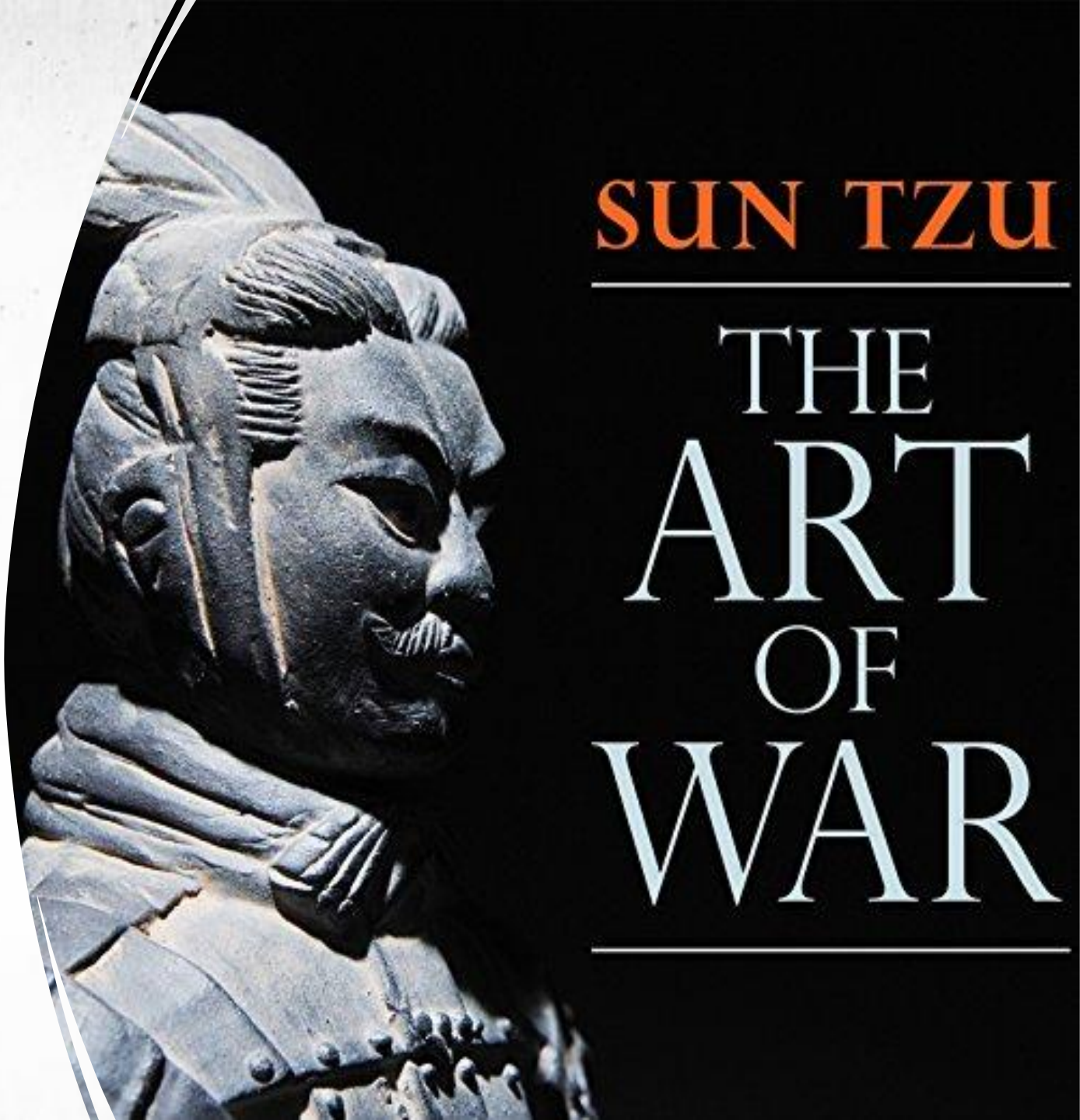
Obmedzenia IDS/IPS

- šifrovaná prevádzka znižuje viditeľnosť
- falošné poplachy zaťažujú analytikov
- potreba pravidelnej aktualizácie signatúr a profilov
- vysoká prevádzka môže systém preťažiť
- pokročilí útočníci sa snažia detekciu obísť (evasion)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

„Ak poznáš nepriateľa
i seba samého, nebudeš porazený.
Ak nepoznáš nepriateľa, ale
poznáš sám seba, máš 50% šancu
na víťazstvo. Ak nepoznáš sám
seba, ani nepriateľa, prehráš.“

- Sun Tzu



Zdroj: Zdroj: https://www.amazon.com/The-Art-of-War-Sun-Tzu-audiobook/dp/B01MQSRAMM/

- **obrana aj útok**
- **nevyhnutnosť pre prežitie**
- **rôzne formy**

Zdroj: https://www.linkedin.com/pulse/video-deception-nature-martin-stevens/
Tricky: The butterfly Kallima inachus resembles a dead leaf. Swallowtail Garden Seeds/flickr, CC BY

Pasce na útočníkov (I.)

„Plánované opatrenia podniknuté
s cieľom uviesť útočníkov do omylu
a prinútiť ich tak prijať (alebo neprijať) konkrétne akcie, ktoré pomáhajú obrane
v kybernetickej bezpečnosti.“

- JAMES J. YUILL

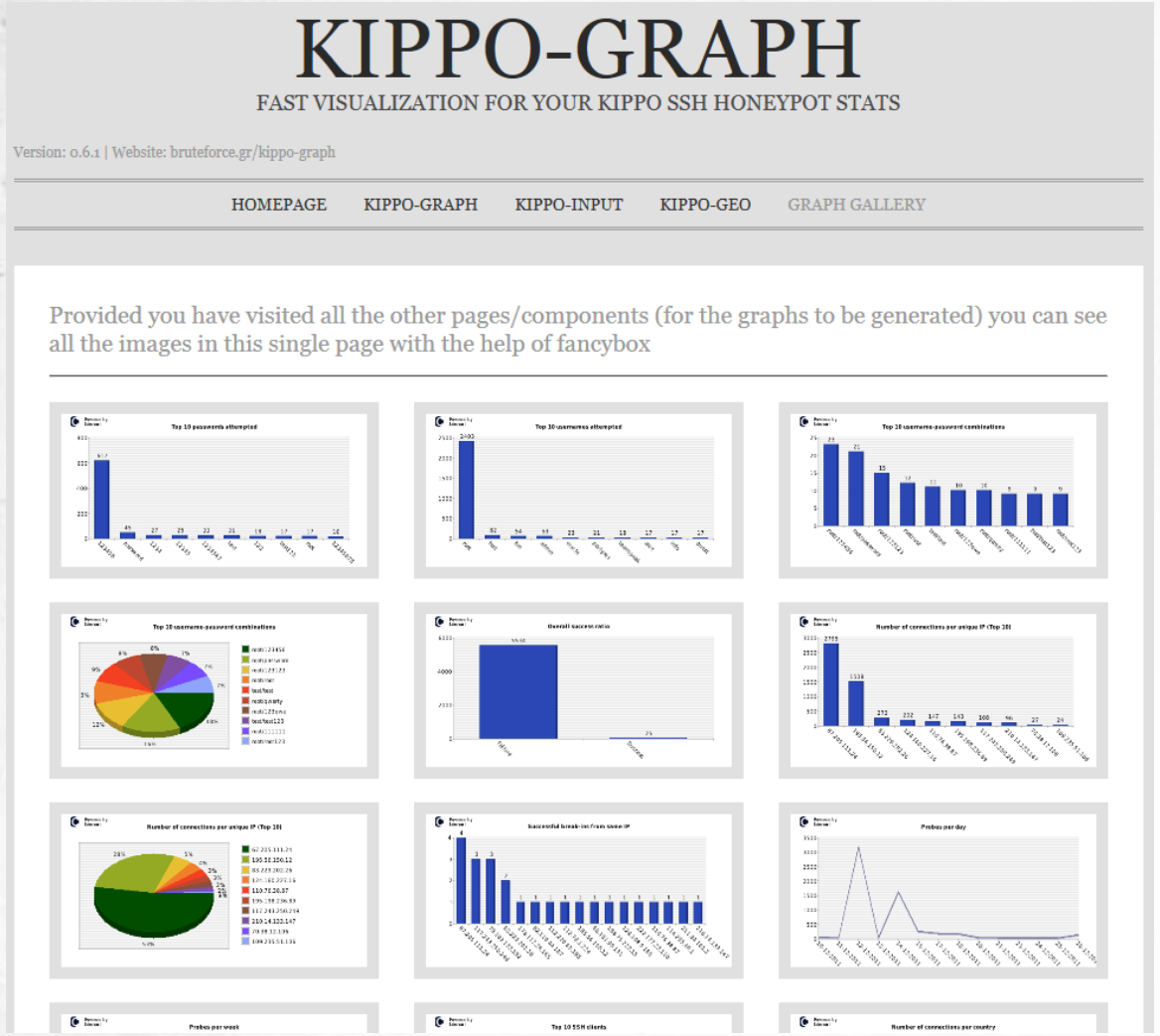
Zdroj: https://medium.com/dataseries/what-really-is-cyber-deception-e60dd33e9e41

Honeypot - zdroj, ktorého hodnota spočíva v sledovaní, útoku alebo kompromitácii!

- Lance Spitzner

Zdroj: https://unsplash.com/photos/Uw15zjNj8ao

Pasce na útočníkov (III.)



Zdroj: https://pixabay.com/sk/photos/mucholapka-venu%c5%a1a-m%c3%a4so%c5%berav%c3%bd-rastlina-1531345/, https://pixabay.com/sk/photos/nepenthes-4791063/

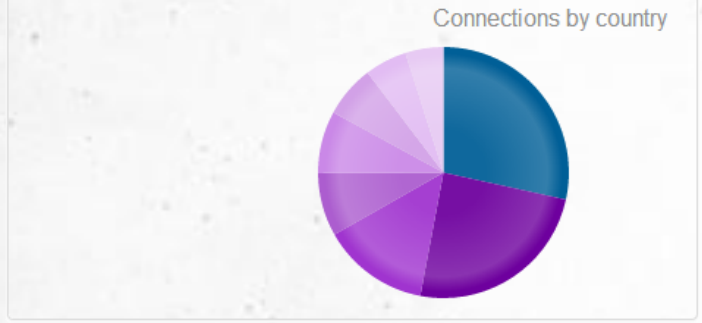
Pasce na útočníkov (IV.)

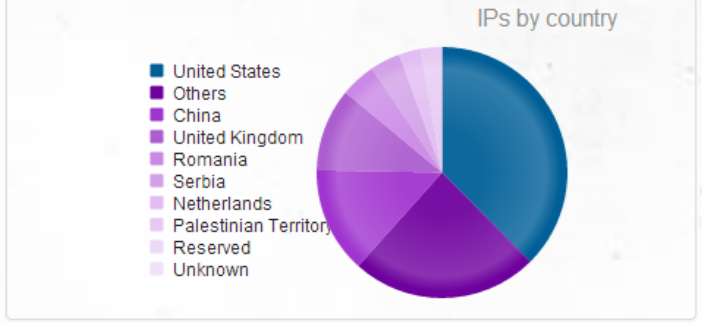
- **honeypot**
  - návnada imitujúca reálny systém alebo službu
  - žiadna legitímna prevádzka → každý prístup je podozrivý
  - odvádza pozornosť útočníka od skutočných systémov
  - zbiera informácie o technikách a nástrojoch útočníka
- **honeynet**
  - celá sieť návnad pre rozsiahlejší zber

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

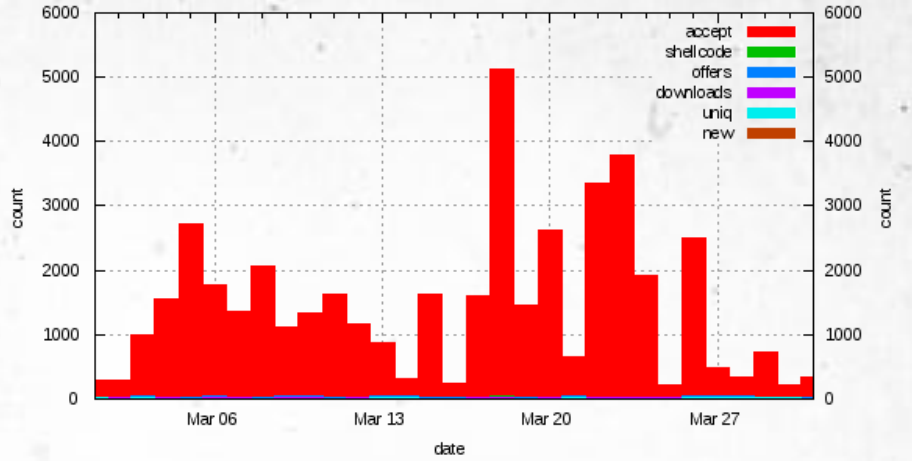
Pasce na útočníkov (V.)

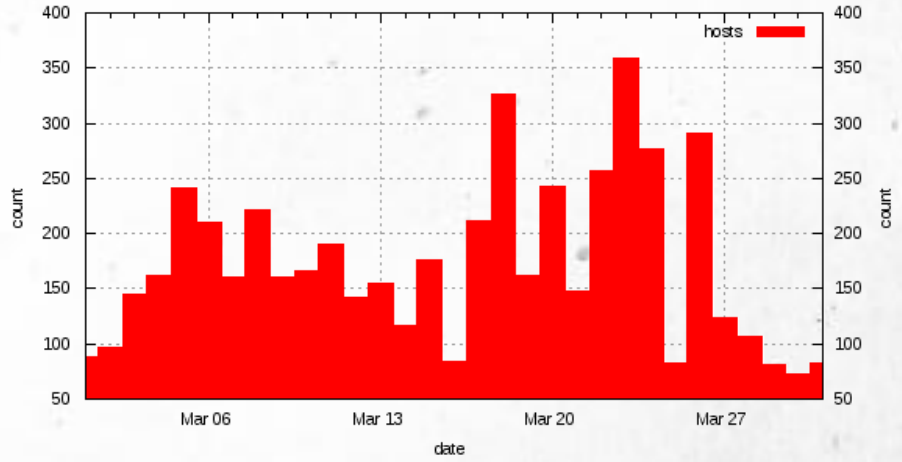
11,612	1,805	269	316	22	22
Connections	IPs	URLs	Downloads	Malware Analized	Malware Known



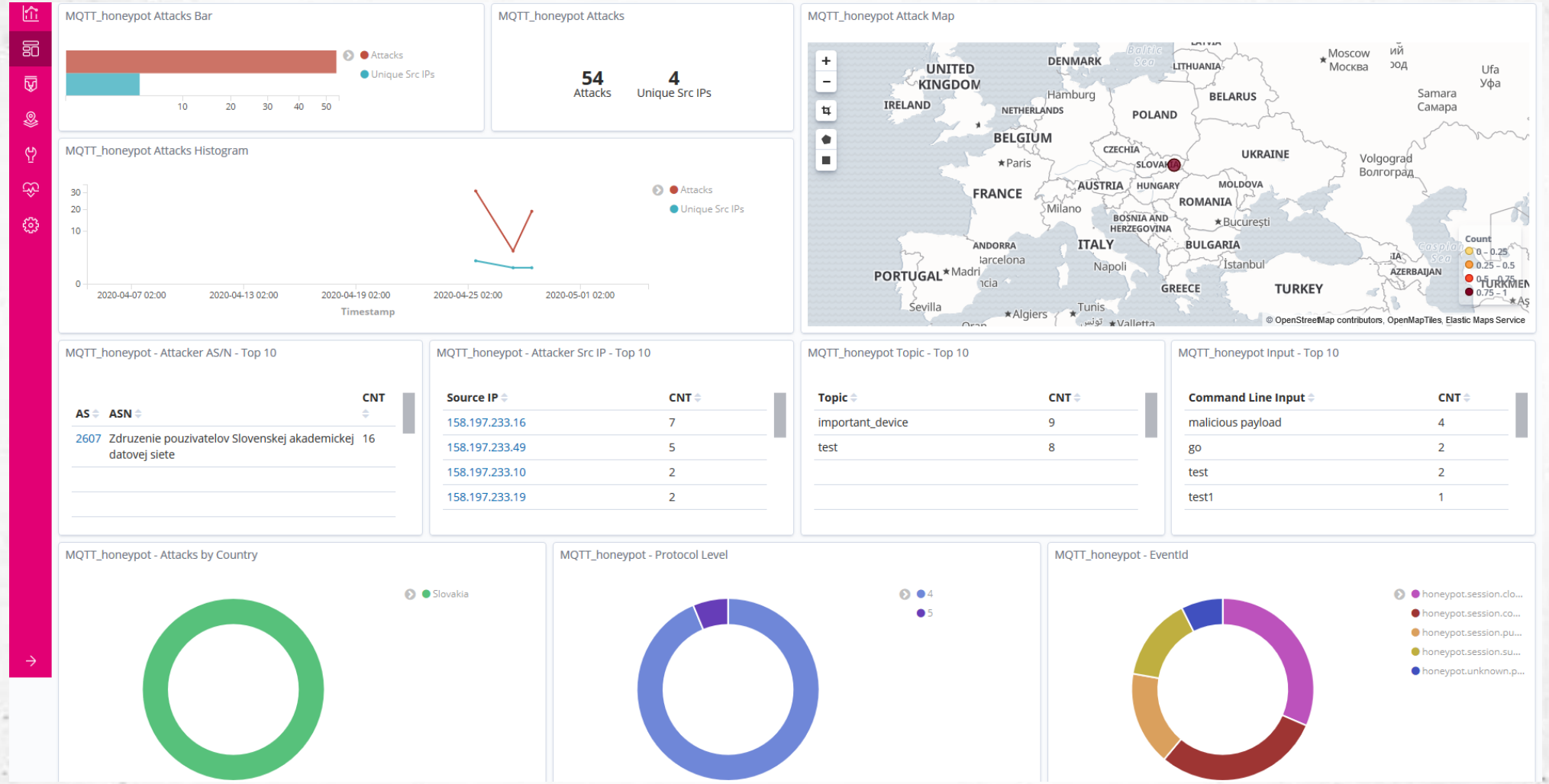



```
mysql> SELECT * FROM auth;
+----+--------------------------------------+---------+----------+----------+---------------------+
| id | session                              | success | username | password | timestamp           |
+----+--------------------------------------+---------+----------+----------+---------------------+
|  1 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | 1234     | 2013-04-28 00:31:08 |
|  2 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | root     | 2013-04-28 00:31:11 |
|  3 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | toor     | 2013-04-28 00:31:17 |
|  4 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | hello123 | 2013-04-28 00:31:20 |
|  5 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | root     | 2013-04-28 00:31:23 |
|  6 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | kippo    | 2013-04-28 00:31:27 |
|  7 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | yes      | 2013-04-28 00:31:30 |
|  8 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | no       | 2013-04-28 00:31:31 |
|  9 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | what     | 2013-04-28 00:31:33 |
| 10 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | paswrod  | 2013-04-28 00:31:36 |
| 11 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | password | 2013-04-28 00:31:37 |
| 12 | e4afcb8aaf9a11e2ad5f000c29cac3fb |       0 | root     | pass     | 2013-04-28 00:31:38 |
| 13 | 3ab48b88af9b11e2ad5f000c29cac3fb |       0 | admin    | admin    | 2013-04-28 00:33:26 |
+----+--------------------------------------+---------+----------+----------+---------------------+
```





Pasce na útočníkov (VI.)



Pasce na útočníkov (VII.)

Výhody

- cenné údaje
- 99% údajov od útočníkov
- veľa implementácií
- minimálne hardvérové nároky

Nevýhody

- obmedzené zorné pole
- možnosť detekcie
- zodpovednosť za zneužitie

Zdroj: Sokol, P., Míšek, J., & Husák, M. (2017). Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security*, *2017* (1), 1-9.
Sokol, P., & Andrejko, M. (2015). Deploying honeypots and honeynets: Issues of liability. In *International Conference on Computer Networks* (pp. 92-101). Springer.

Typy pascí na útočníkov (I.)

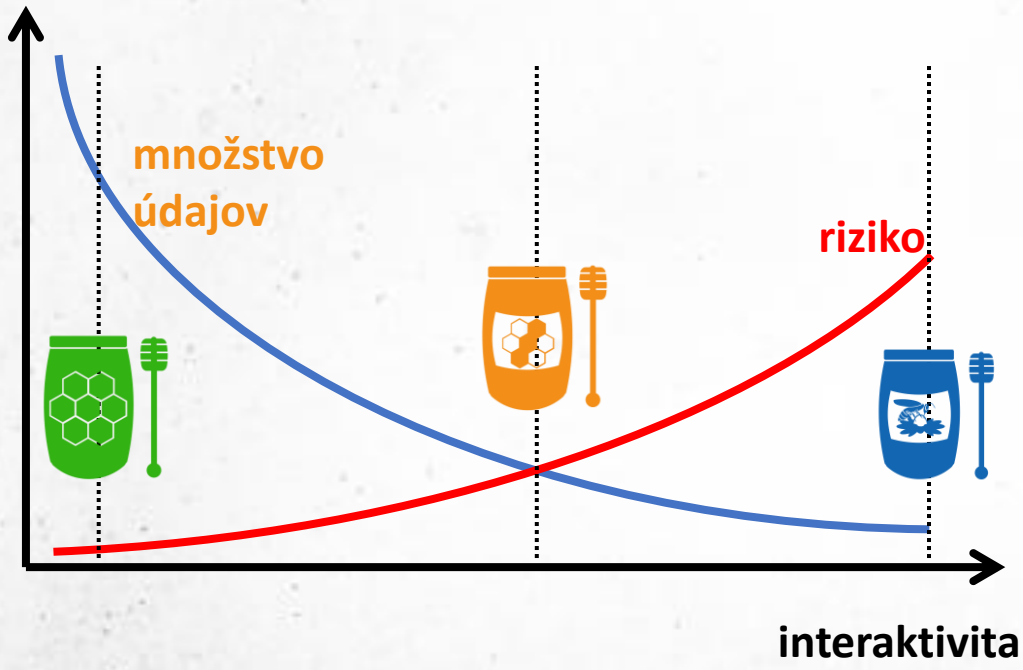
- **Low-interaction**
  - emuluje len odpovede na sieťové požiadavky, nízke riziko
- **Medium-interaction**
  - emuluje len vybrané služby, stredné riziko
- **High-interaction**
  - reálny systém, viac údajov o útoku, vysoké riziko
- **produkčné honeypoty** - ochrana a včasné varovanie
- **výskumné honeypoty** - štúdium správania sa útočníkov

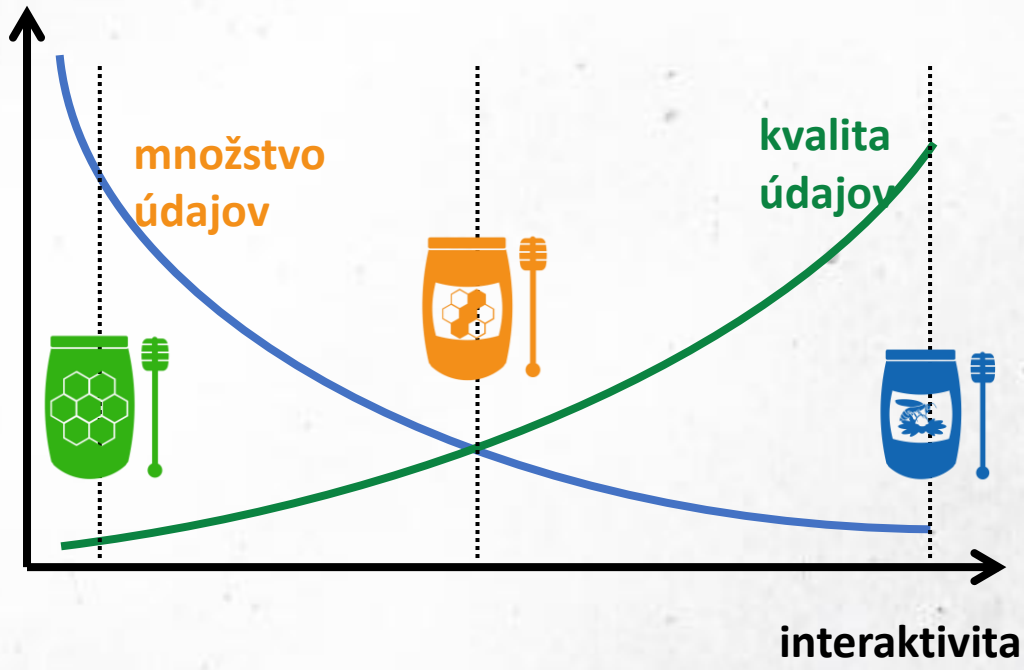
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Typy pascí na útočníkov (II.)

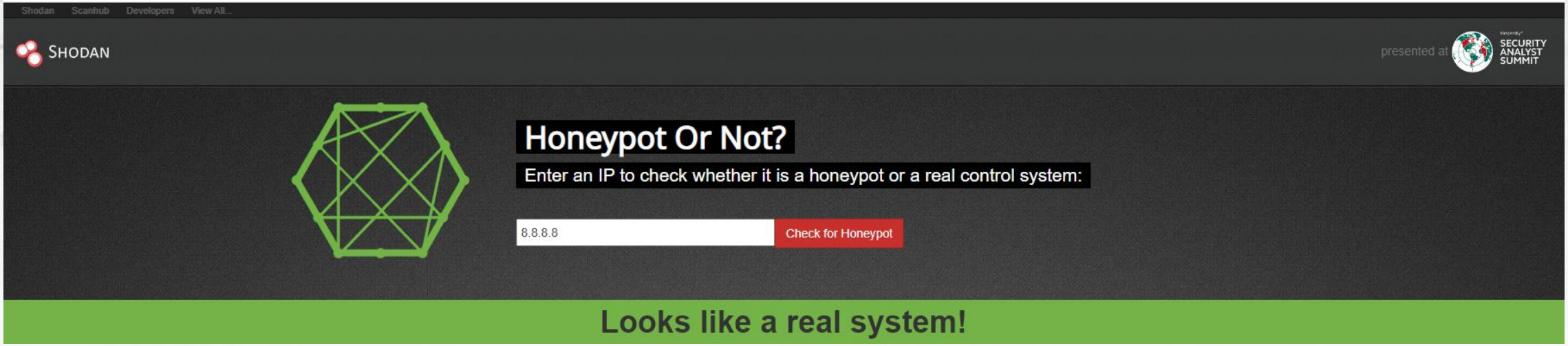
- delenie honeypotov podľa interakcie s útočníkom

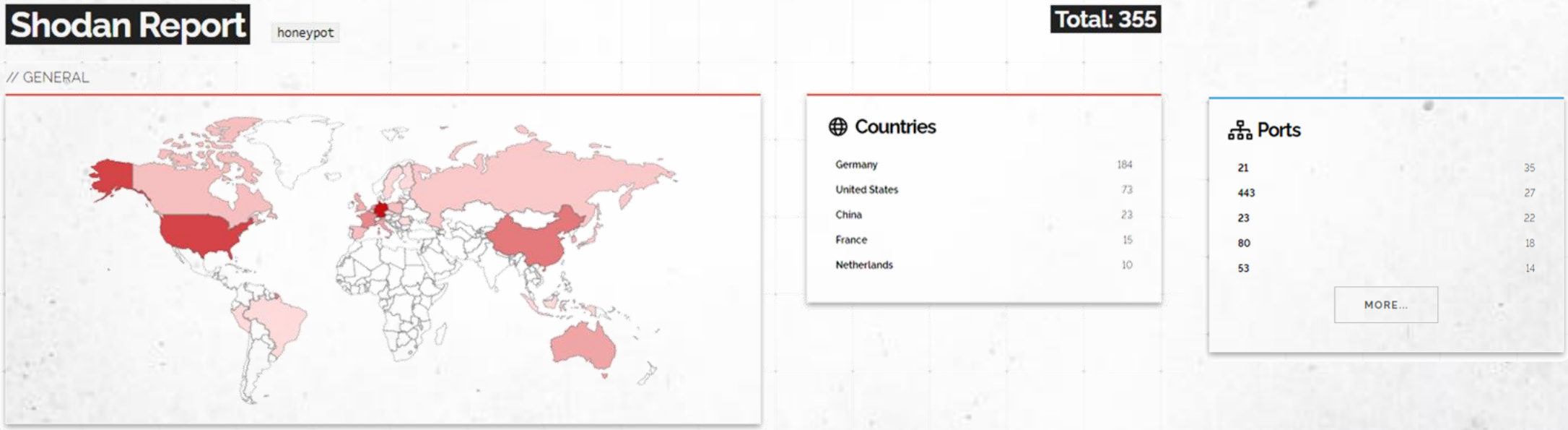
nízka interakcia **stredná interakcia** **vysoká interakcia**





Detekcia pascí na útočníkov





Vývoj podvodných technológií

1998
Honeypot

2000
Honeynet

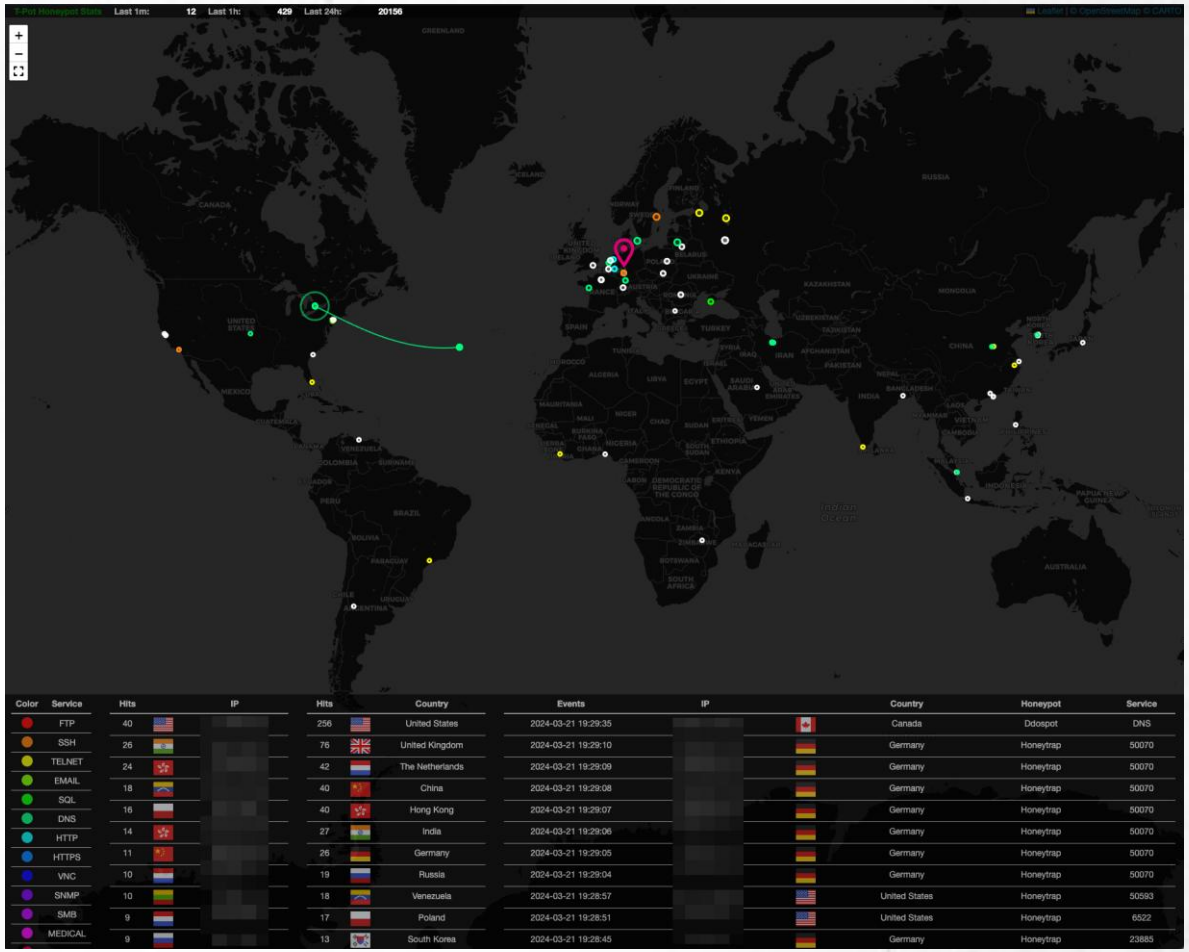
2003
Honeytoken

2012
Honeypot 2.0

2016
Inteligentné platformy

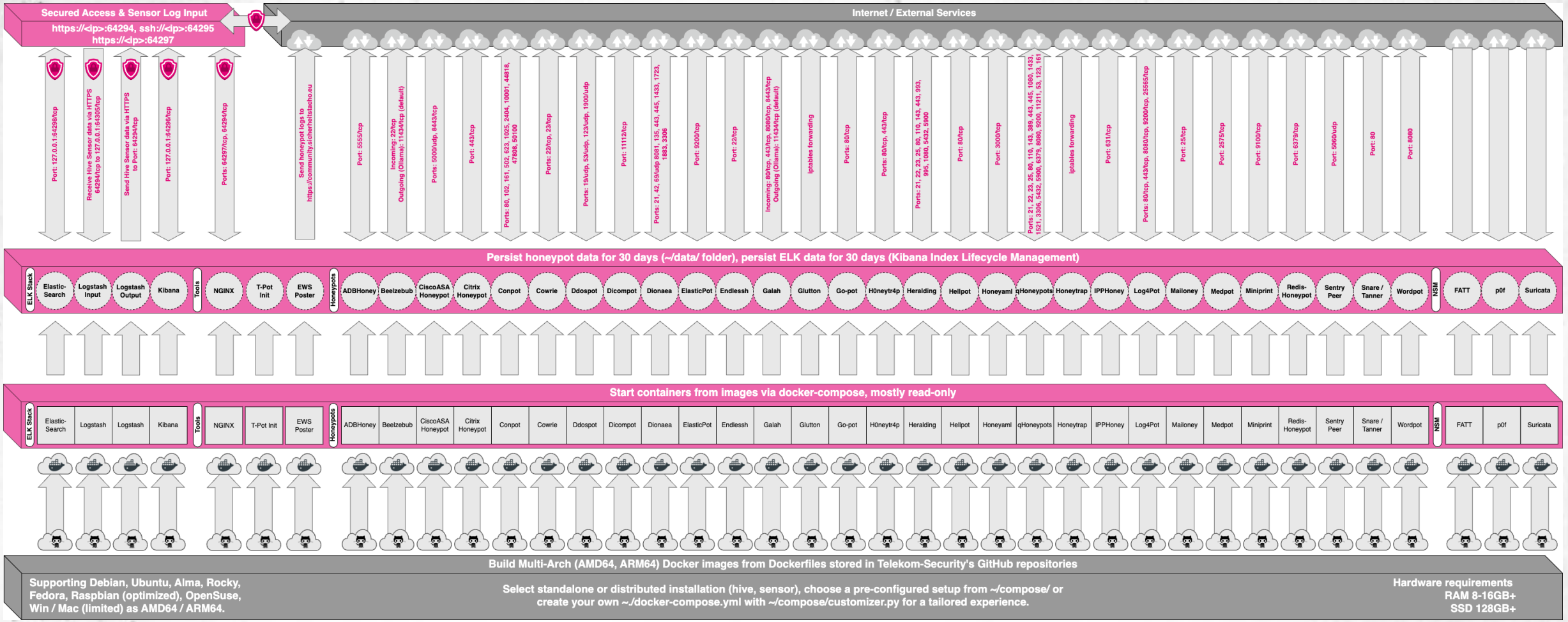
Zdroj: https://www.provehonetworks.com.au/deception-technologies/

T-POT (I.)



Zdroj: https://github.com/telekom-security/tpotce

T-POT (II.)



Zdroj: https://github.com/telekom-security/tpotce

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť