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

12 Sieťové situačné povedomie

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

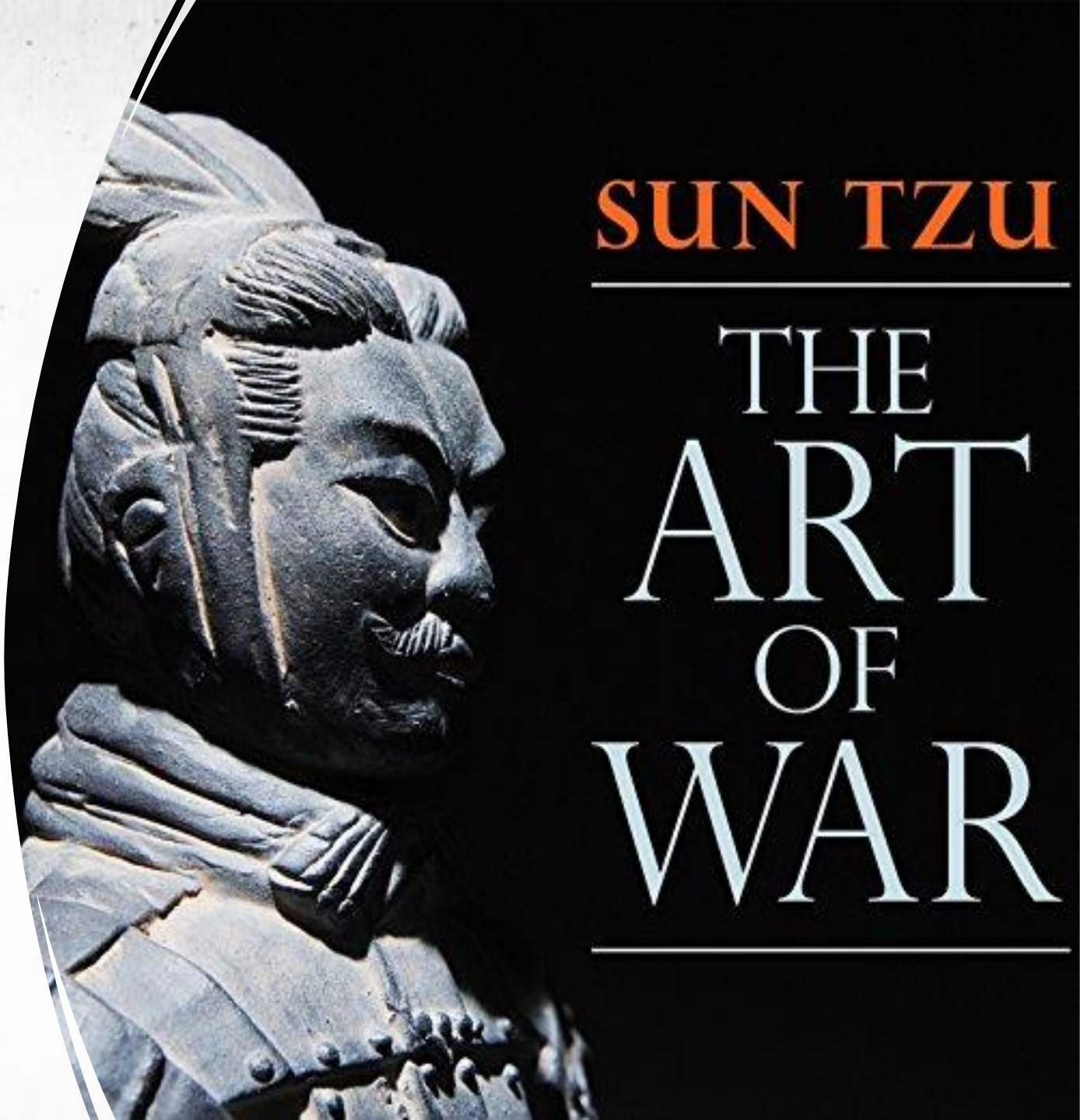
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťové situačné povedomie

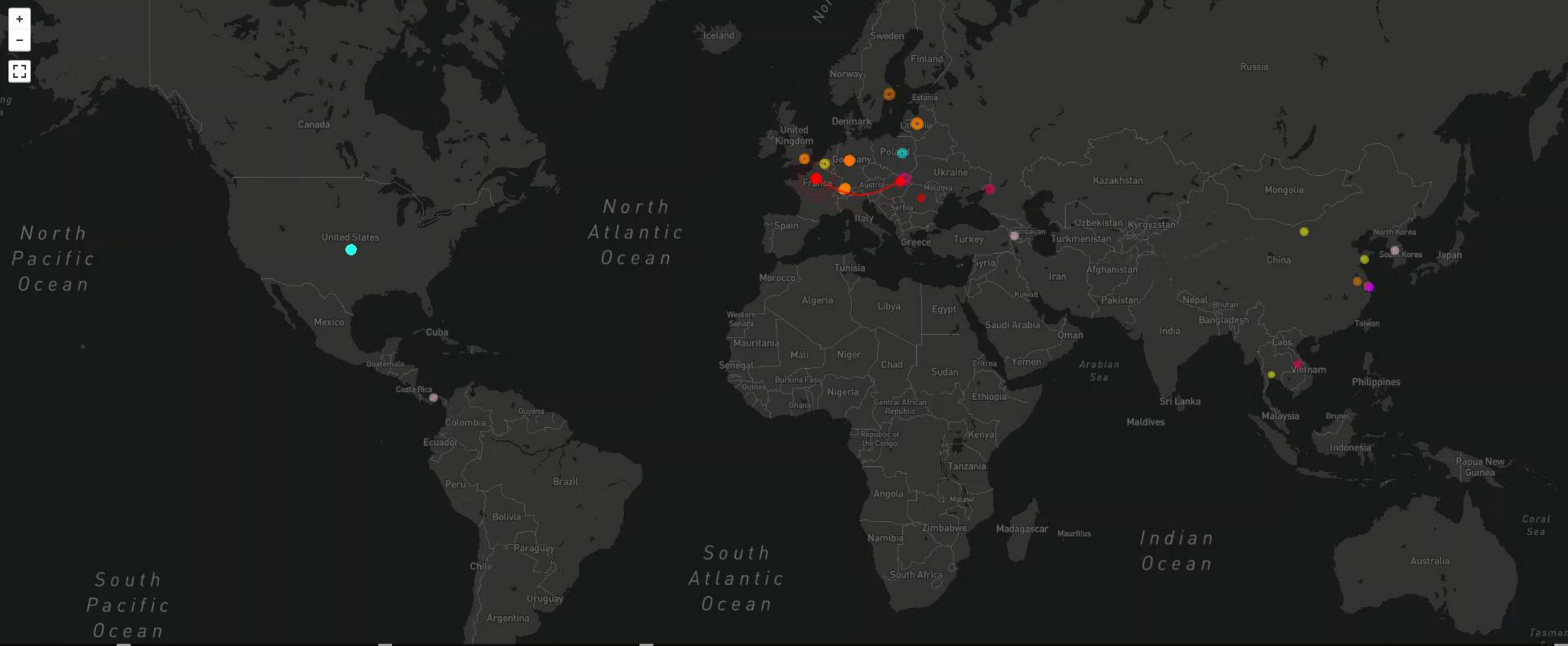
- analýza situačného povedomia
- predikcia situačného povedomia

„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/



Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS
	HTTP

Qtd	IP
11931	51.75.241.220
3074	92.46.160.122
109	89.163.204.36
51	80.254.123.149
46	165.232.180.32
35	179.43.142.180
26	112.240.202.32

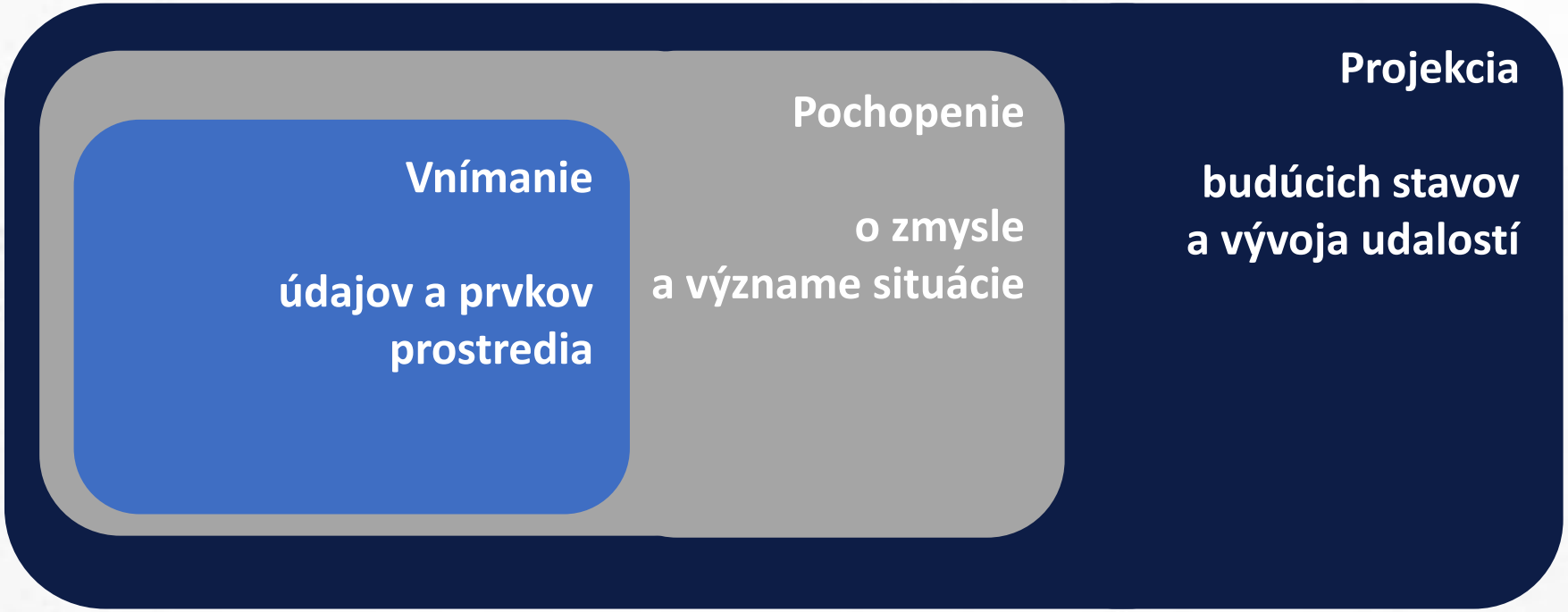
Qtd	Country
11940	France
3074	Kazakhstan
167	United States
166	China
134	Germany
99	Russia
84	Switzerland

Timestamp	IP	Country	Honeypot	Service
2022-04-28 06:05:34	51.75.241.220	France	Sentrypeer	SIP
2022-04-28 06:05:33	51.75.241.220	France	Sentrypeer	SIP
2022-04-28 06:05:31	51.75.241.220	France	Sentrypeer	SIP
2022-04-28 06:05:30	51.75.241.220	France	Sentrypeer	SIP
2022-04-28 06:05:29	51.75.241.220	France	Sentrypeer	SIP
2022-04-28 06:05:28	51.75.241.220	France	Sentrypeer	SIP
2022-04-28 06:05:26	51.75.241.220	France	Sentrypeer	SIP

Sieťové situačné povedomie (II.)

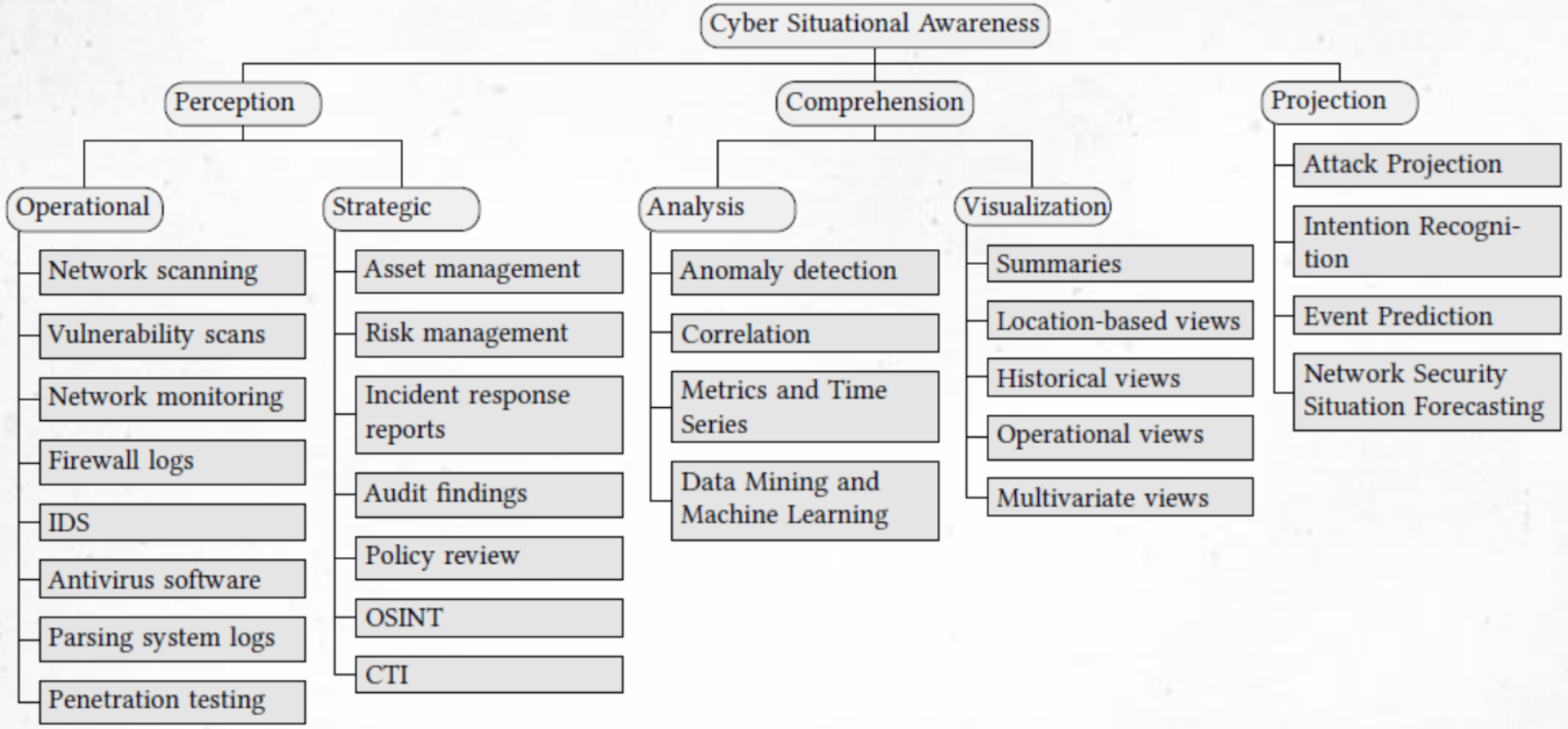
Sieťové situačné povedomie (III.)

- monitorovanie kybernetických systémov, pochopenie kybernetickej bezpečnostnej situácie reprezentovanej modelovaním kybernetických hrozieb alebo súvisiacimi bezpečnostnými výstrahami a predpovedanie zmien v kybernetickej bezpečnostnej situácii (Husák, 2020).



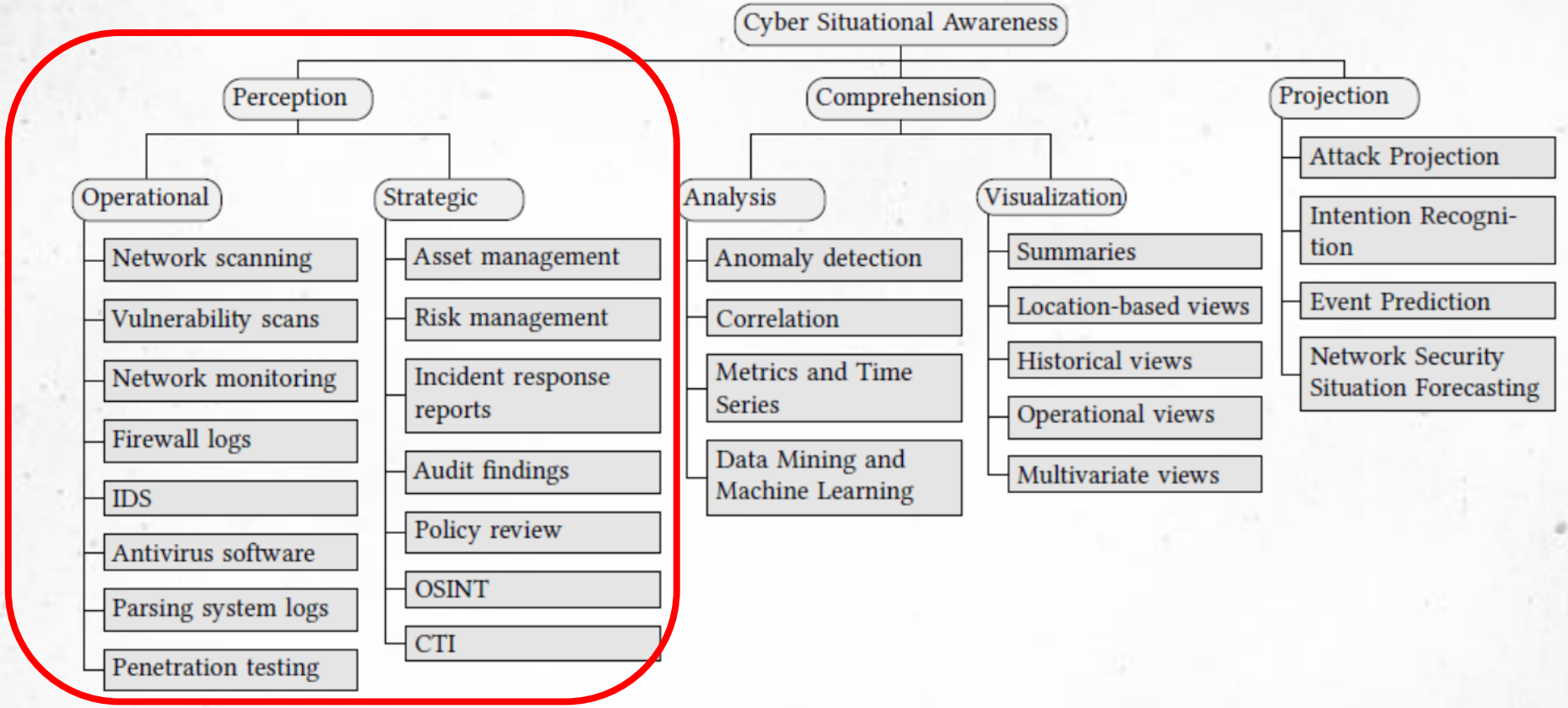
Zdroj: Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

Sieťové situačné povedomie (IV.)



Zdroj: Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

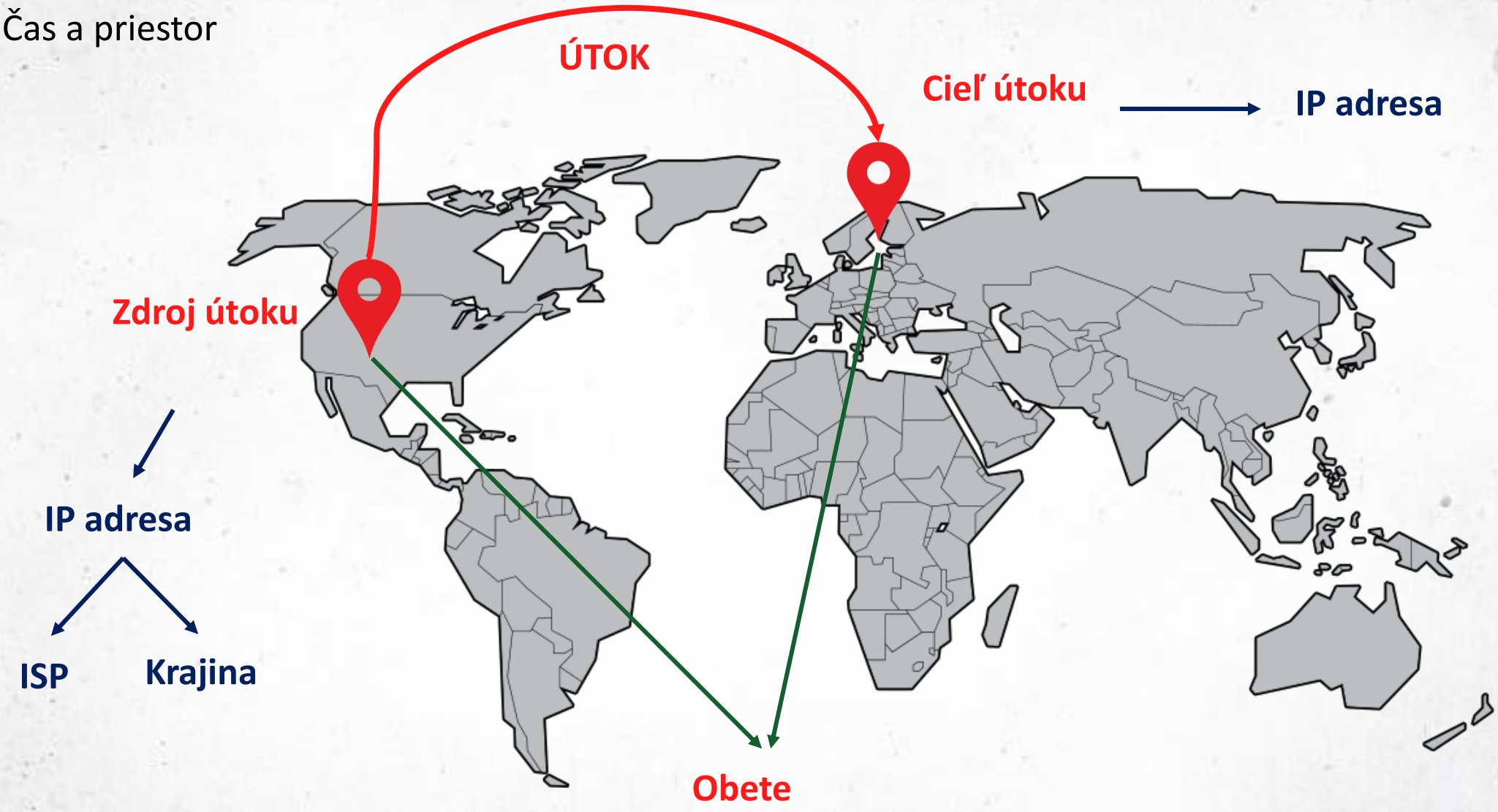
Vnímanie (I.)



Zdroj: Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

Vnímanie (II.)

- Čas a priestor



Vnímanie (III.)

- **Bezpečnostné údaje**


```
{
 "Format": "IDEA0",
 "ID": "4390fc3f-c753-4a3e-bc83-1b44f24baf75",
 "CreateTime": "2019-06-03T10:00:02Z",
 "DetectTime": "2019-06-03T10:00:07Z",
 "EventTime": "2019-06-03T07:36:00Z",
 "Category": ["Fraud.Phishing"],
 "Ref": ["cve:CVE-1234-5678"],
 "Confidence": 1,
 "Note": "Synthetic example",
 "ConnCount": 20,
```


Čas

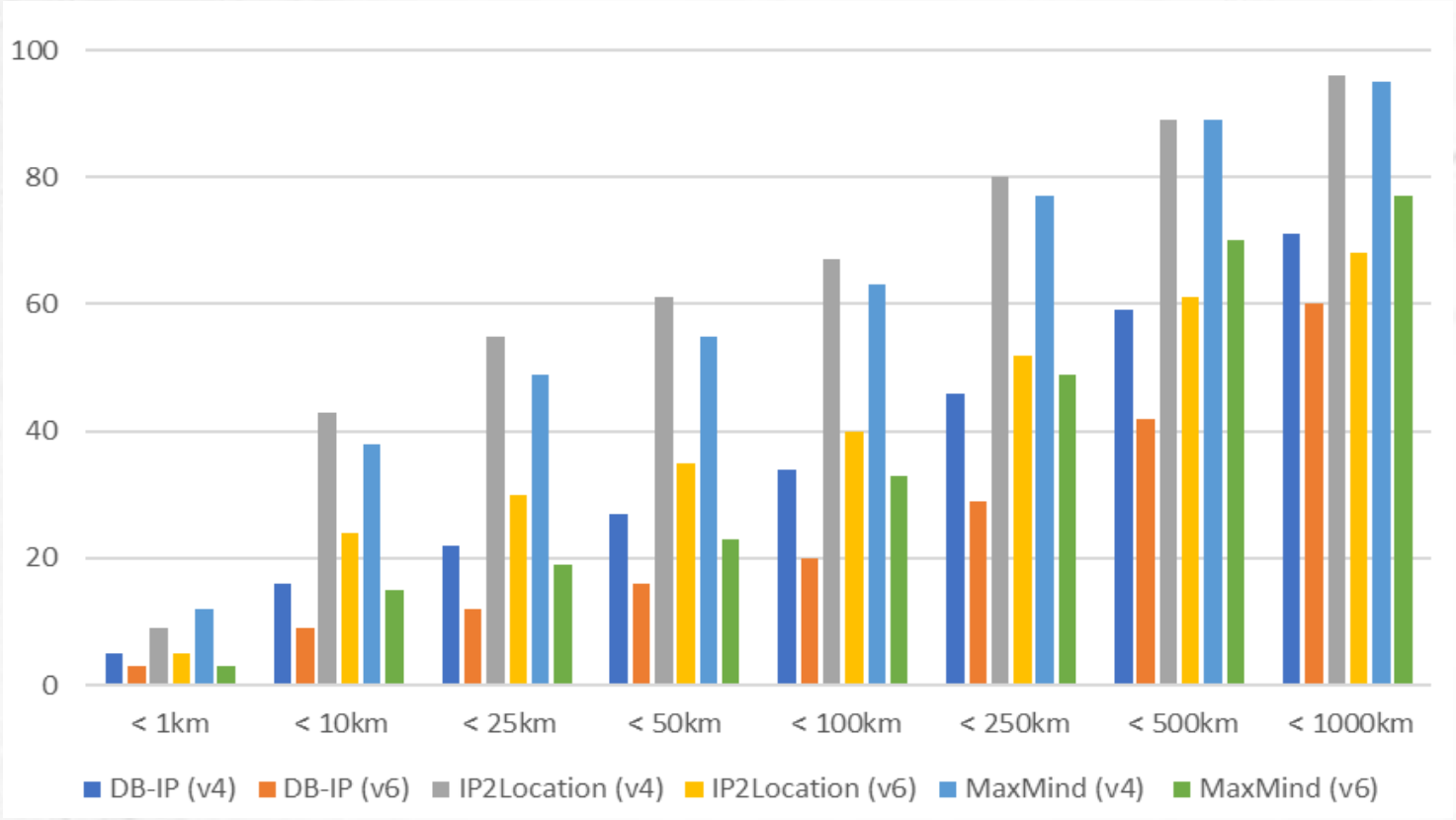
IP adresa

Geolokácia


```
"Zdroj": [
  {
    "Type": ["Phishing"],
    "IP4": ["192.168.0.10/25"],
    "Hostname": ["example.com"],
    "URL": ["http://example.com/cgi-bin/killemall"],
    "Proto": ["tcp", "http"],
  }
], ...
"Node": [
  {
    "Name": "cz.cesnet.kippo-honey",
    "Type": ["Protocol", "Honeypot"],
    "SW": ["Kippo"],
    "AggrWin": "00:05:00"
  }]}
```

Vnímanie (IV.)

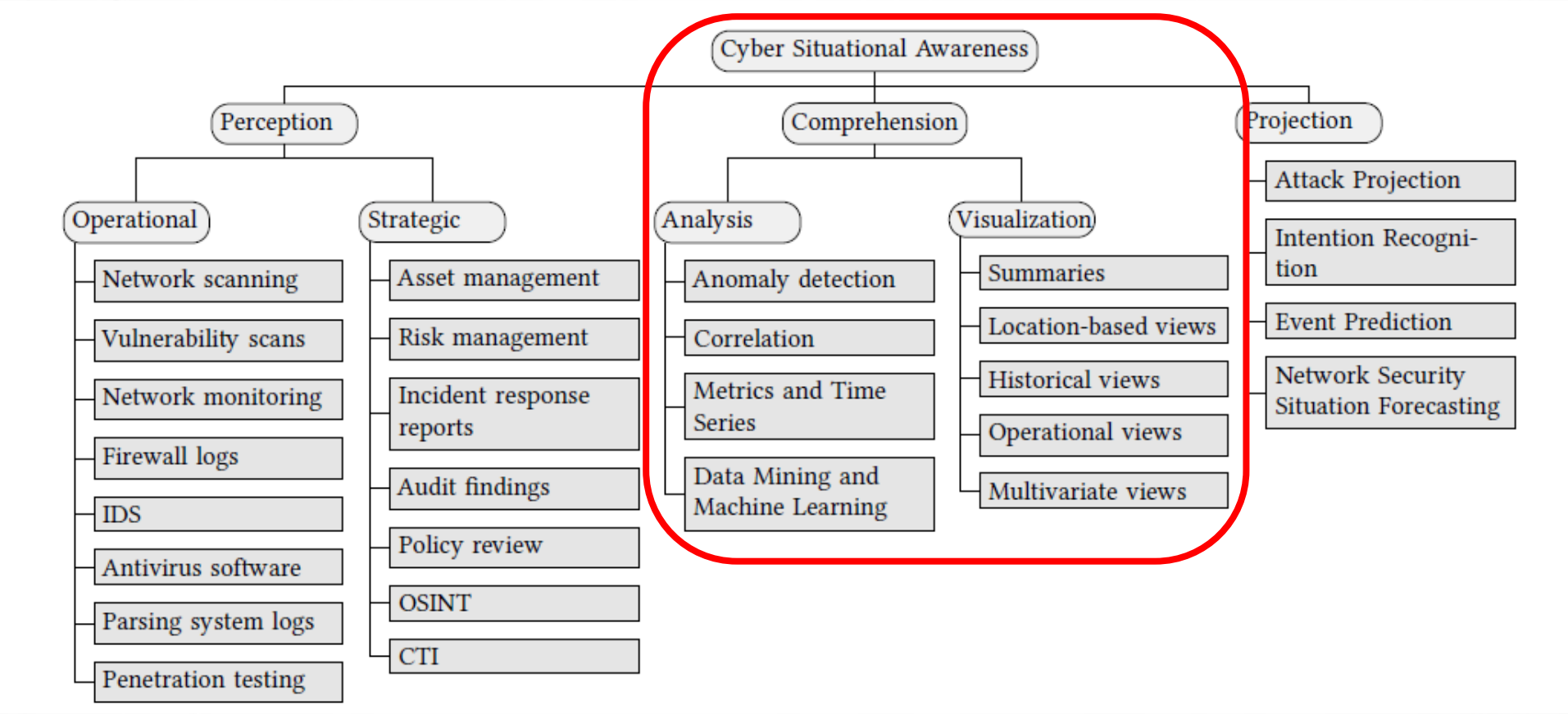
- **Geolokácia**




```
{
    "query": "158.197.16.80",
    "status": "success",
    "continent": "Europe",
    "continentCode": "EU",
    "country": "Slovakia",
    "countryCode": "SK",
    "region": "KI",
    "regionName": "Kosice",
    "city": "Košice",
    "district": "Kosice",
    "zip": "040 12",
    "lat": 48.7192,
    "lon": 21.2512,
    "timezone": "Europe/Bratislava",
    "offset": 3600,
    "currency": "EUR",
    "isp": "Zdruzenie pouzivatelov Slovenskej akademickej datovej siete",
    "org": "P. J. Safarik University in Kosice",
    "as": "AS2607 Zdruzenie pouzivatelov Slovenskej akademickej datovej siete",
    "asname": "SANET",
    "mobile": false,
    "proxy": false,
    "hosting": false
}
```

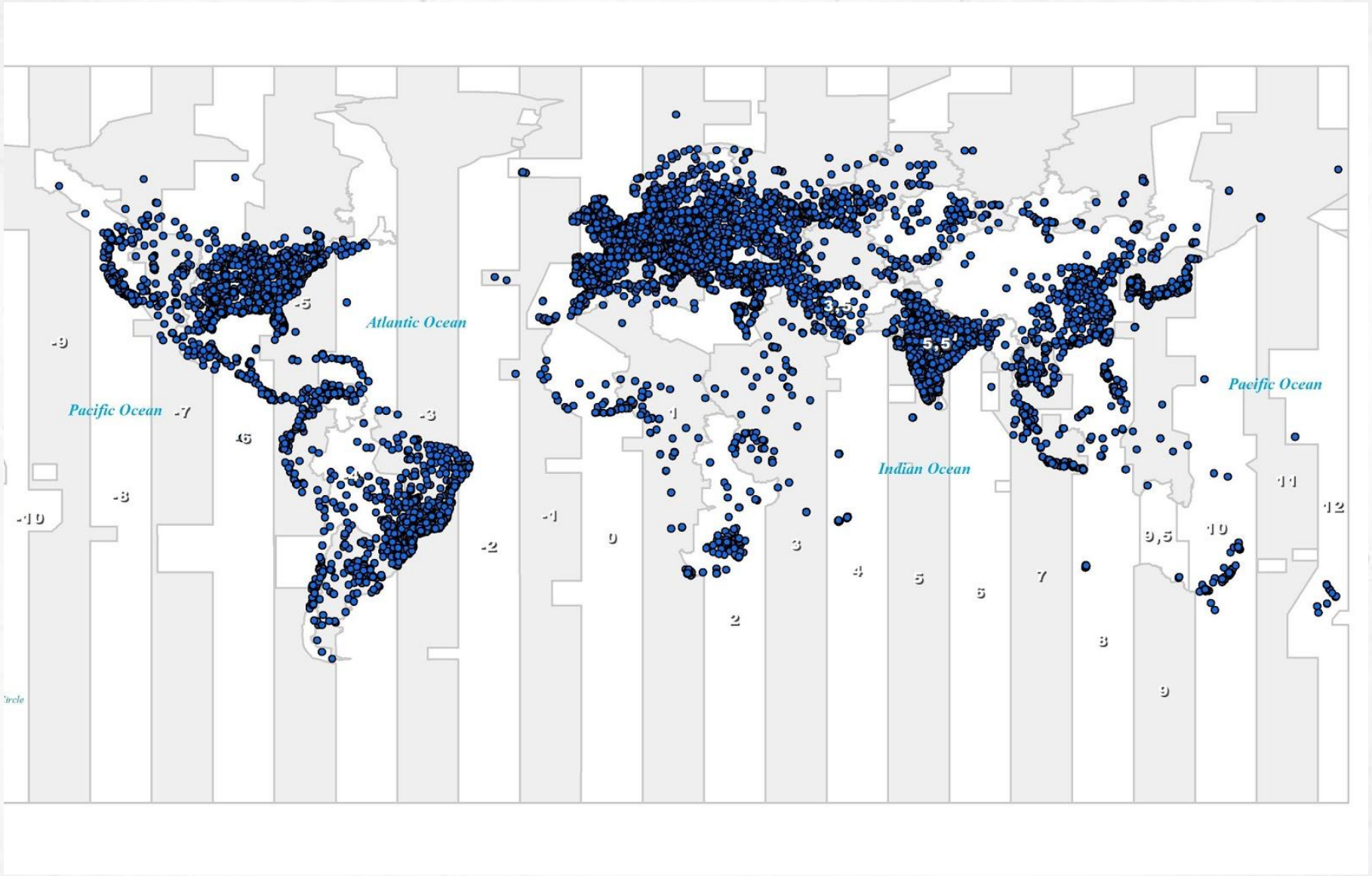

Zdroj: KESTER, Jan-Jelle. Comparing the Accuracy of IPv4 and IPv6 Geolocation Databases. Methodology, 2016, 10.11: 12-17.

Pochopenie (I.)



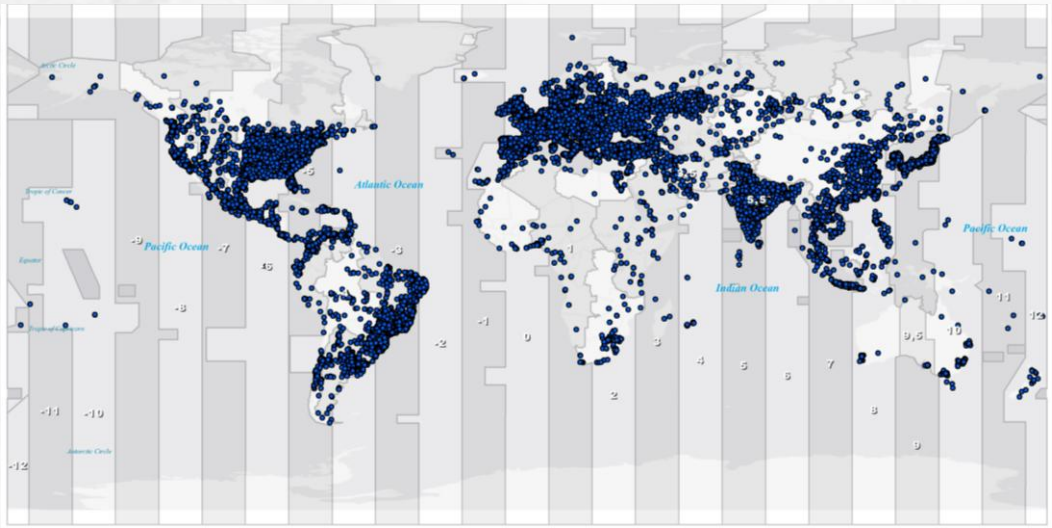
Zdroj: Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

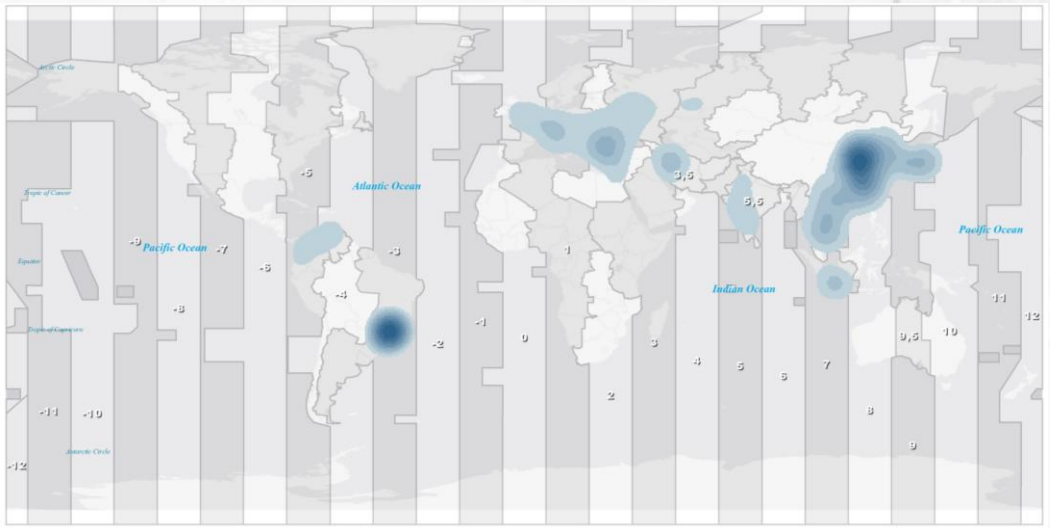
Pochopenie (II.)

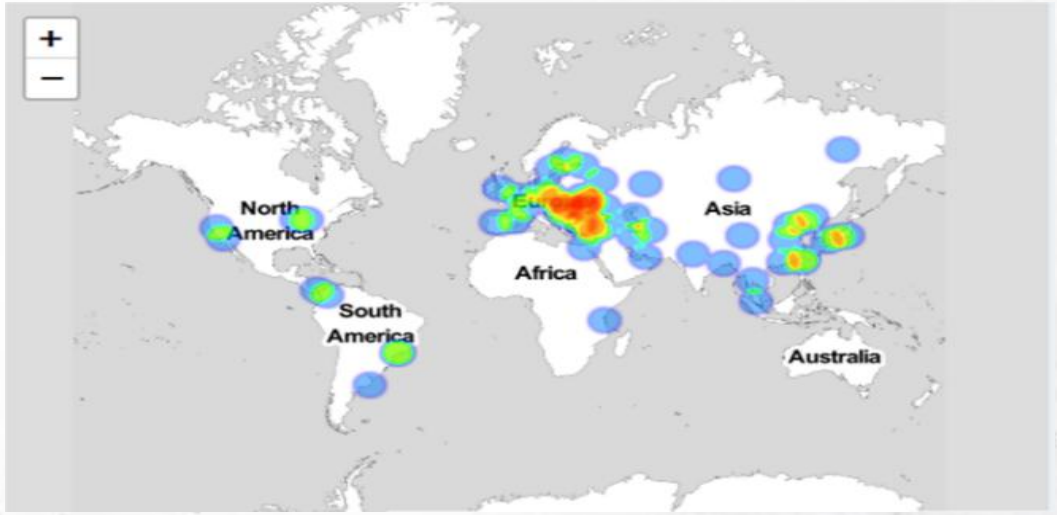


Pochopenie (III.)

- **Priestorové aspekty**



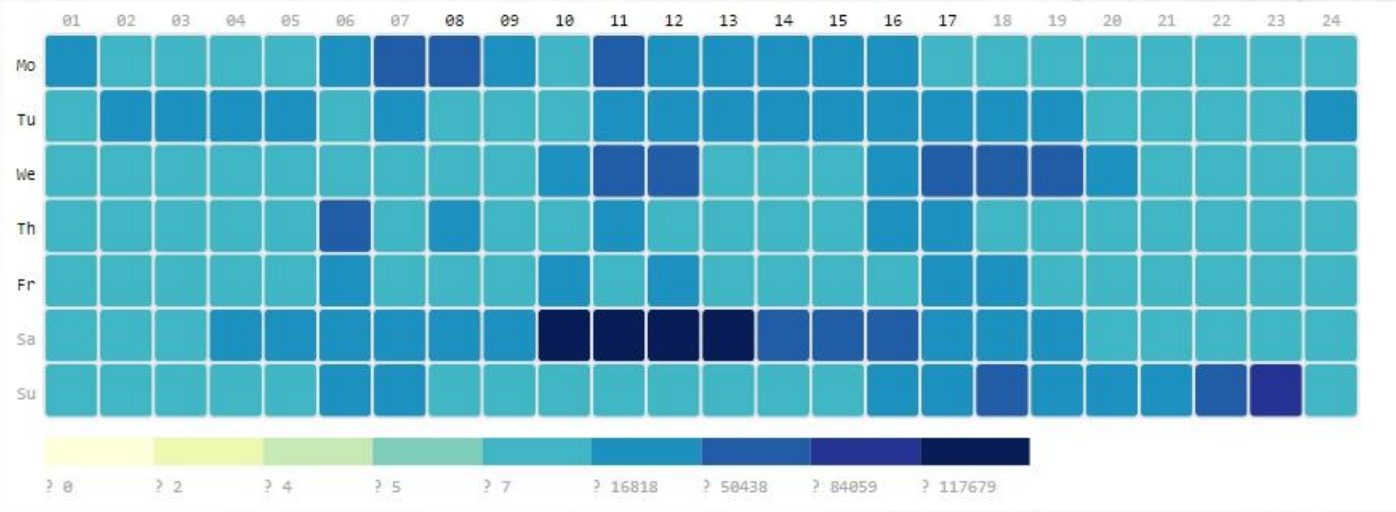




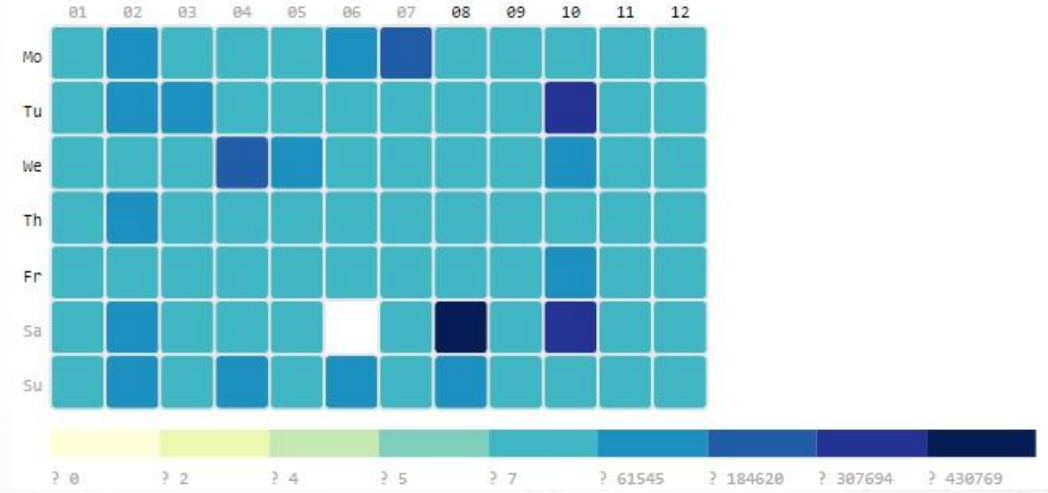
Pochopenie (IV.)

- **Časové aspekty**

Deň v týždni a hodiny

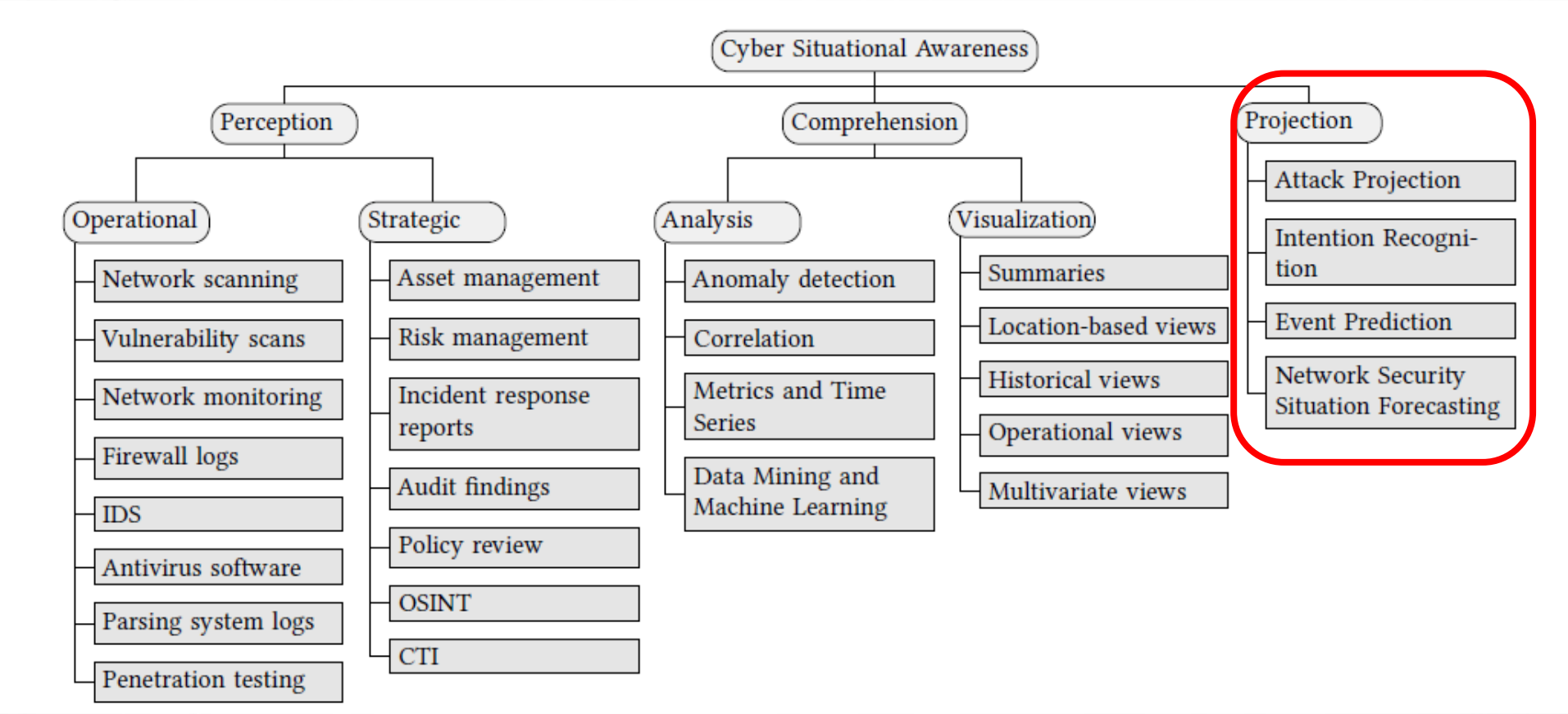


Deň v týždni a mesiace



Zdroj: Sokol P, Kleinová L, Husák M. Study of attack using honeypots and honeynets lessons learned from time-oriented visualization. InIEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON) 2015 Sep 8 (pp. 1-6). IEEE.

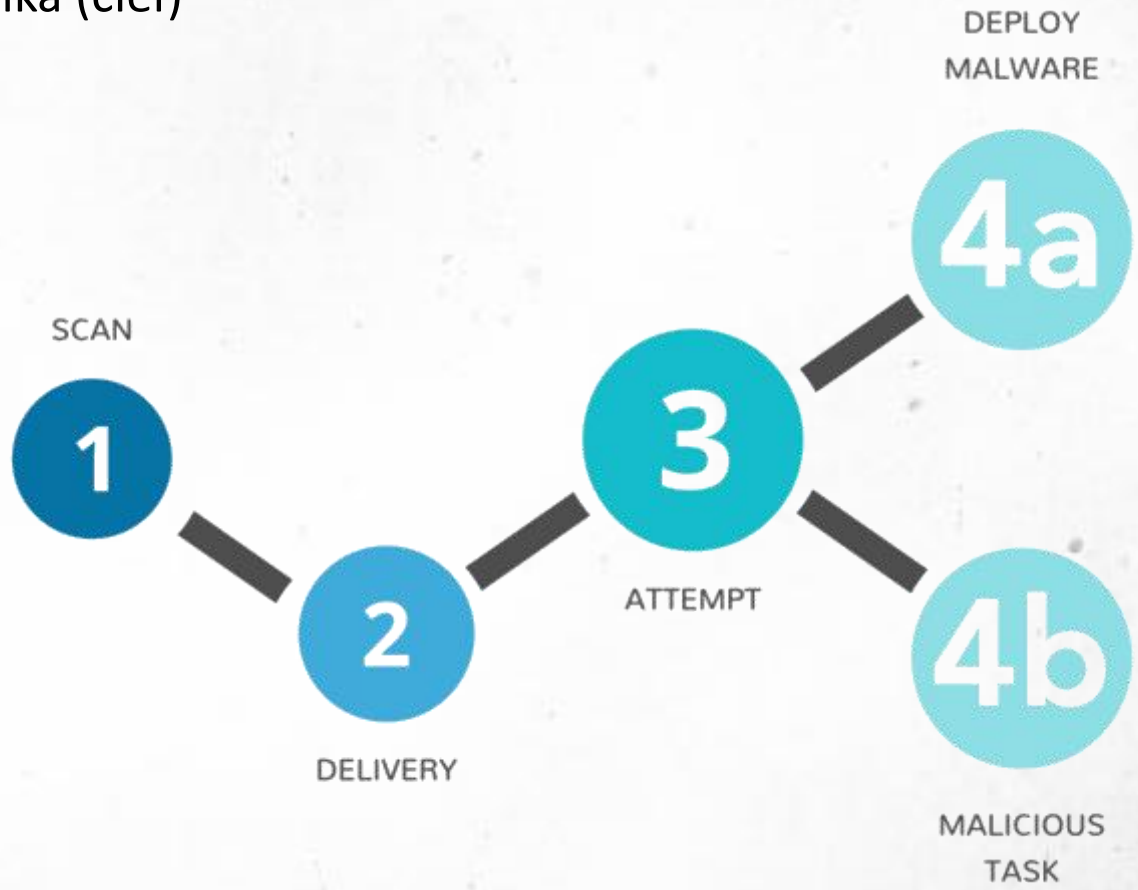
Projekcia (I.)



Zdroj: Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

Projekcia (II.)

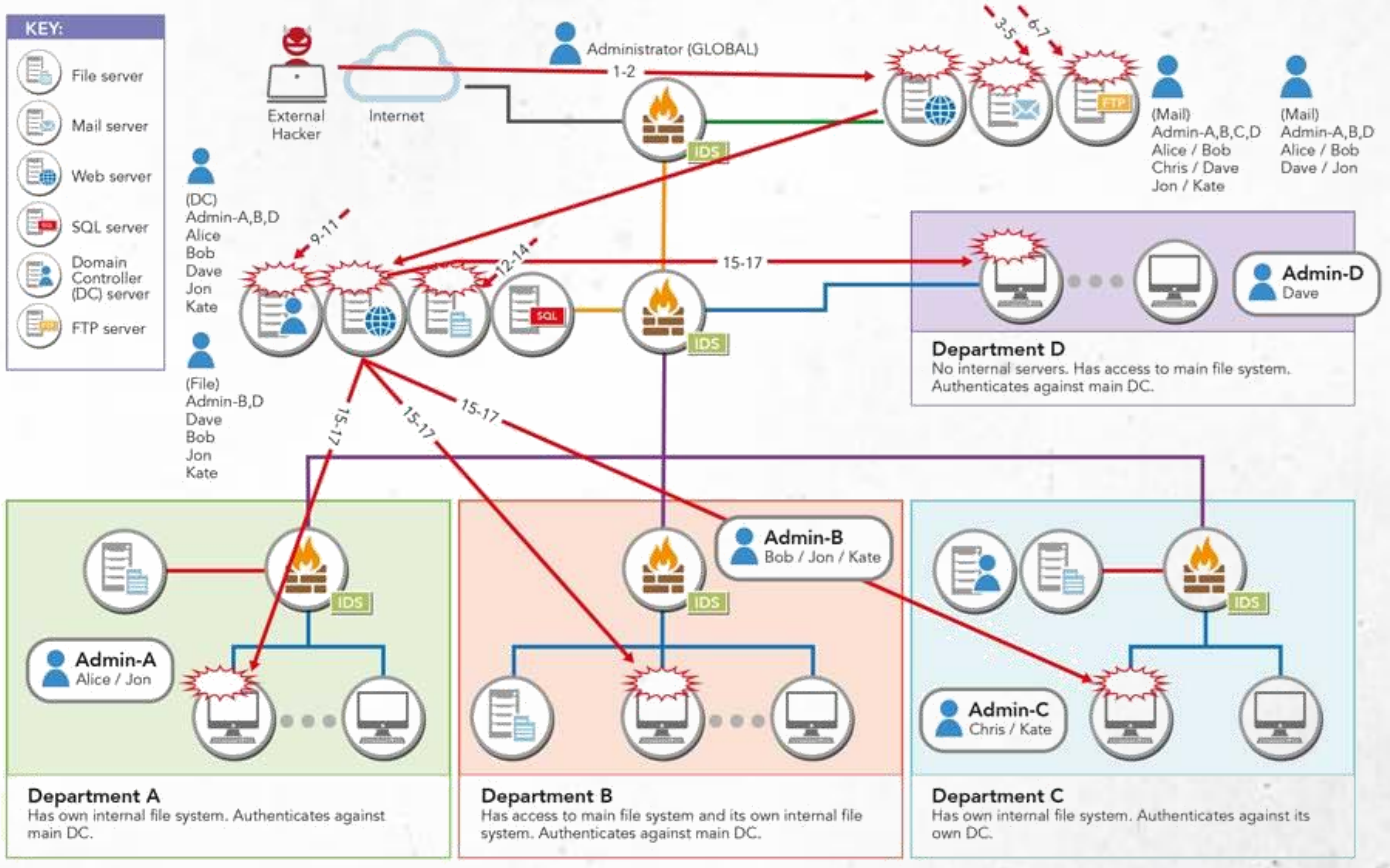
- **projekcia útoku**
- ďalší krok útočníka / posledný krok útočníka (cieľ)
- detekcia v rannom štádiu
- etapy útokov



Zdroj: Pivarníková M, Sokol P, Bajtoš T. Early-Stage Detection of Cyber Attacks. Information. 2020 Dec;11(12):560

Projekcia (III.)

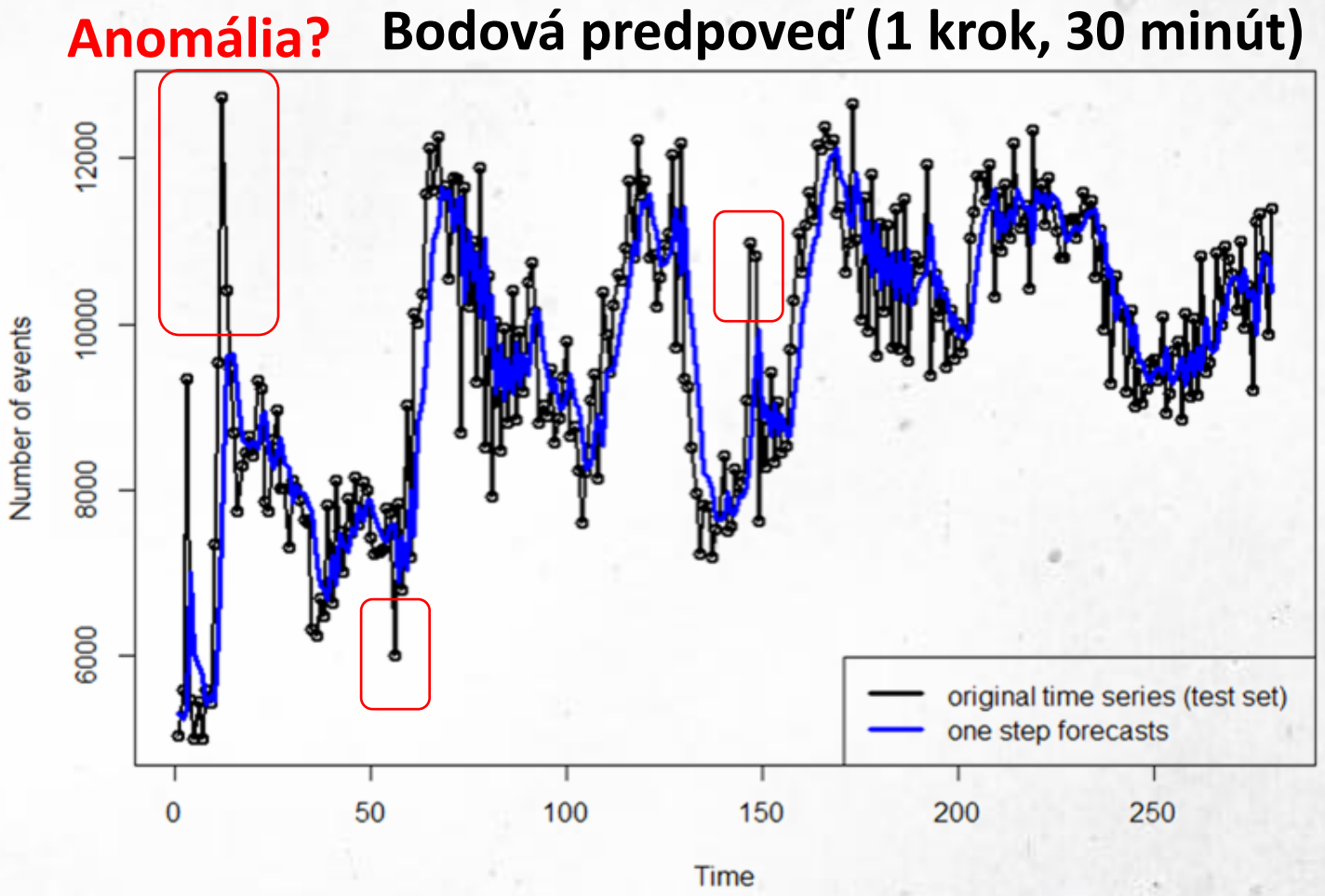
- **predikcia útoku**
- výstup – odhadovaná pravdepodobnosť, že sa sieťová entita bude v danom časovom rozsahu správať zlomyseľne



Zdroj: https://researchfeatures.com/cybersecurity-threats-can-we-predict-them/

Projekcia (IV.)

- **predpovedanie (forecasting)**
- všeobecnejšie údaje
- výstup - Počet upozornení na akcie agentov hrozby (útočníka).
- skutočné hodnoty sa líšia od predpokladaných hodnôt



Zdroj: Pekarčík P, Gajdoš A, Sokol P. Forecasting security alerts based on time series. InInternational Conference on Hybrid Artificial Intelligence Systems 2020 Nov 11 (pp. 546-557). Springer, Cham.

Projekcia (V.)

- **výhody**
  - veľmi vysoká presnosť
  - žiadne problémy s profilovaním
- **nevýhody**
  - nie príliš podrobná predpoveď
  - možné problémy s niektorými typmi údajov.

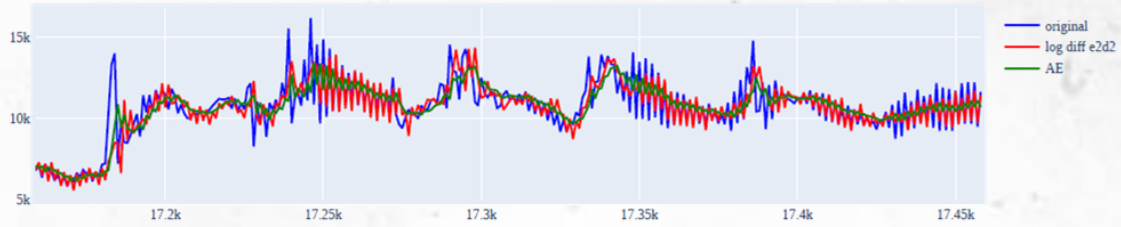


Fig. 1. 1-step forecasting for Port 445 time series based on e2d2 network with log diff scaling and combination of ARIMA and Exponential smoothing.

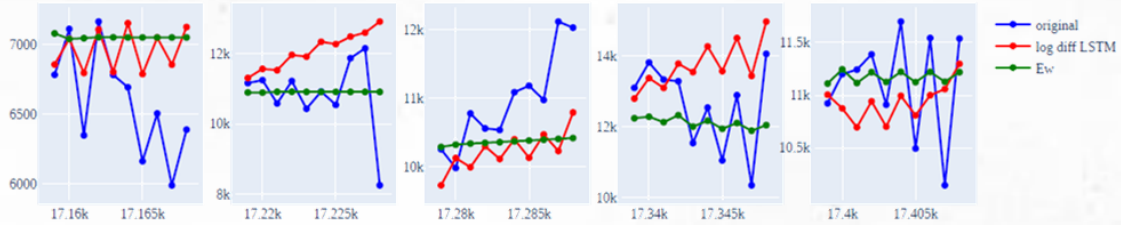


Fig. 2. 10-steps forecasting for Port 445 time series based on LSTM network with log diff scaling and combination of Exponential smoothing with rolling window.

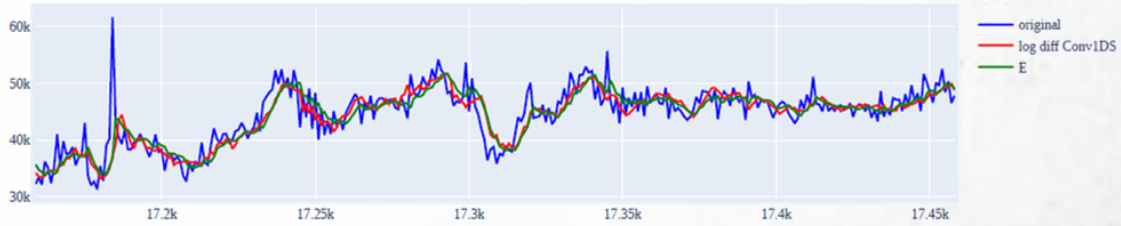


Fig. 3. 1-step forecasting for Count of all alerts time series based on Conv1DS network with log diff scaling and Exponential smoothing.

Zdroj: Sokol, P., Staňa, R., Gajdoš, A. and Pekarčík, P., 2022. Network security situation awareness forecasting based on statistical approach and neural networks. *Logic Journal of the IGPL*., Husák M, Bartoš V, Sokol P, Gajdoš A. Predictive methods in cyber defense: Current experience and research challenges. Future Generation Computer Systems. 2021 Feb 1;115:517-30,

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